Description of document:	General Services Administration (GSA) White Papers produced by the GSA Emerging Technology Division 2021.pdf
Requested date:	22-August-2021
Release date:	31-August-2022
Posted date:	02-September-2022
Source of document:	U.S. General Services Administration FOIA Requester Service Center (LG) 1800 F Street, NW, 7308 Washington, DC 20405-0001 Fax: 202-501-2727 FOIAonline

Office of the General Counsel
FOIA Requester Service Center

August 31, 2022

This letter is in response to your U.S. General Services Administration (GSA) Freedom of Information Act (FOIA) request number (GSA-2021-001545), submitted on August 22, 2021, in which you requested the following:

> “A copy of each white paper, report, study or memorandum (or comparable document) produced during FY2021 by the Emerging Technology Division of the Office of Information Integrity and Access of the GSA Office of Governmentwide Policy. I also request a copy of the listing of topics that have been evaluated, and a copy of the listing of reports/studies/etc. produced to date.”

Enclosed please find the documents responsive to your request.

In processing your request GSA withheld draft and/or unpublished copies of white papers, reports, memoranda, and decisions papers, as these reflect the agency’s deliberative process, are considered pre-decisional in nature, and/or attorney-client privileged communications and as a result have been redacted pursuant to FOIA, 5 U.S.C. § 552(b)(5).

As we have redacted information referenced in the above paragraph(s) with the aforementioned FOIA exemption, this technically constitutes a partial denial of your FOIA request. You have the right to appeal the denial of the information being withheld. You may submit an appeal online at the following link (https://www.foiaonline.gov/foiaonline/action/public/home) or in writing to the following address:

U.S. General Services Administration
FOIA Requester Service Center (LG)
1800 F Street, NW
Washington, DC 20405

Your appeal must be postmarked or electronically transmitted within 90 days of the date of the response to your request. In addition, your appeal must contain a brief statement of the reasons why the requested information should be released. Please enclose a copy of your initial request and this denial. Both the appeal letter and envelope or online appeal submission should be prominently marked, “Freedom of Information Act Appeal.”

This completes our action on this FOIA request. Should you have any questions, please contact Shawn Watson at (202) 368-0854 or by email at shawn.watson@gsa.gov. You may also contact the GSA FOIA Public Liaison, David Eby at (202) 213-2745 or by email at david.eby@gsa.gov for any additional assistance.

Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, email at ogis@nara.gov; telephone at (202) 741-5770; toll free at (877) 684-6448; or facsimile at (202) 741-5769.

Sincerely,

Duane Fulton

Duane Fulton
Lead Government Information Specialist
Office of the General Counsel
General Services Administration

Enclosure(s)

Utilizing Communication Platforms to Promote Interagency Collaboration

Executive Summary

This memo informs agencies that there is no need for Memorandums of Understanding (MOUs) and Interconnection Security Agreements (ISAs) for interagency Microsoft (MS) Teams (Teams) Federation. Further, this memo calls for a shared federal domain whitelist to facilitate interagency Teams collaboration, as well as the establishment of guest access procedures across agencies. It also provides cybersecurity best practices for Teams federation.

MS Teams Federation Assessment

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47 requires that agencies negotiate individual MOUs and ISAs in order to interconnect IT systems. This memo assesses Microsoft Teams in the context of NIST SP 800-47 and finds that Teams collaboration does not fit NIST's definition of an "interconnected system," rendering MOUs and ISAs unnecessary. Appendices A and B contain technical details substantiating these findings.

The applicable rule is Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource.[1] A-130 specifies that while addressing non-Federal entities in Appendix 1 that system owners must develop a MOU and ISA when interconnecting IT systems. NIST publication SP 800-47 addresses interconnected IT systems.

However, a broad reading of SP 800-47 suggests that Teams external access does not constitute an interconnected system; instead, email serves as a better analogue for the manner in which Teams functions.

There are three justifications for this reasoning:

1. SP 800-47 specifically addresses interconnected systems. Both the current revision of SP 800-47 and the draft revision currently being circulated state that an interconnected system is one that shares a direct connection. The examples of a

[1] https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

"direct connection" NIST offers include a dedicated circuit (dial up, T Carrier, synchronous optical network, etc.) or VPN.[2]

Teams external access does not rely on a direct connection. Instead, Teams functions like email -- traffic is sent between the edge services based on Domain Name System (DNS) server lookups of the recipient and destination domains.

2. Because Teams functions more like email (see appendices A and B), the relays (Azure Active Directory or AAD) from one agency to another are obtained from Cloud Service Providers (CSPs) and authorized by the Federal Risk and Authorization Management Program (FedRAMP) under either a Joint Authorization Board (JAB) Authority to Operate (ATO) or an agency ATO. AAD is part of the JAB authorizations for both Microsoft - Azure Commercial Cloud and Microsoft - Azure Government (includes Dynamics 365). OMB A-130 Appendix I appears to regulate interconnections between federal agencies and non-federal entities.

3. While agencies are frequently referred to as independent entities, all agencies share a standard and highly controlled means of adopting technologies both on-premise to an agency (Federal Information Security Modernization Act [FISMA]) and within the cloud (FedRAMP). Since the components that provide Teams functionality (i.e., AAD) are already authorized as part of Teams authorization, further agreements (MOU/ISAs) between agencies are unnecessary, especially in the absence of a direct connection.

In conclusion, Teams has built-in functionality to permit Teams users to communicate across agencies. Teams uses AAD to facilitate this functionality. AAD does not constitute an interconnection given the examples of interconnection contained in NIST SP 800-47; instead, it resembles the DNS servers used in email systems. The Teams product is FedRAMP-authorized, meaning its external access features were as well.

Collaboration between employees in different agencies that use the same FedRAMP-authorized software, should not be subject to additional agreements to use features that the product has in its FedRAMP-authorized configuration. **Thus, when establishing federation between agencies using Microsoft Teams, an agency-to-agency MOU/ISA is not required.**

[2] http://what-when-how.com/data-communications-and-networking/dedicated-circuit-networks-data-communications-and-networking/

Direction to Agencies

This memorandum directs agencies thusly:

1. OMB shall maintain a list of federal domains for federation on OMB MAX. Within 60 days of the issuance of this memo, Chief Information Officers (CIOs) of agencies which have instances of Teams shall submit their permitted domains to OMB for inclusion on the list.
2. Within 60 days of OMB publishing the list of domains in part (1), agencies shall enable Teams federation using a whitelist model that incorporates the OMB list of permitted domains. The Office of the Federal Chief Information Officer (OFCIO) may grant exceptions based on written requests from agencies.
3. Agencies shall ensure that interagency network traffic meets the following minimum cybersecurity requirements:
    a. Isolation of Teams Federation from sensitive business processes, to the extent practical;
    b. Robust scanning of traffic within the Teams communications channels at least equivalent to email scanning for phishing and malware;
    c. User logging within Teams, or equivalent functionality from other software if the agency's Teams instance does not support logging;
    d. Advanced reporting to periodically monitor Teams channels to support ongoing Teams channels access monitoring and auditing;
    e. Periodic reviews of Teams channels to archive inactive channels, and to remove external users and guest users who no longer need access;
    f. Training for users, including on Teams federation functions and the minimum annual Cybersecurity training.
    g. Each agency shall enforce the following:
        - Least Privilege: Only authorizing access to the minimal amount required for an approved or required function; and
        - Role-Based Access: Implement role-based access controls to perform certain operations ('permissions') as approved.
        - When participants access a Teams channel, agencies will present participants tenants with agency rules of behavior.
4. Within 180 days of the issuance of this memo, agencies with instances of Teams shall ensure that they have a process to grant Teams guest access to users external to the agency. Agencies may set clearance and vetting processes for guest access at their own discretion, so long as a process to grant access exists.
5. Federated teams tenants are advised to implement automatic security patching in their Microsoft Teams instances, or otherwise to apply software updates to their instances as frequently as possible.
6. Individual agencies shall retain their own record-keeping requirements.

Appendix A: Email Description

Synopsis

An email is sent via an email client, either web based or locally installed. The email client is connected to the sender's email account. When addressing an email, the sender selects the recipient from a directory or enters the recipient's email address. The information after the "@" symbol is the domain information for the recipients email account. When the email is sent, the sender's email server routes the email via internet to a Domain Name System (DNS) server. The DNS server "looks up" the recipient's email server IP address to route the email to that server. The email is then delivered to that server and ultimately into the recipient's email inbox.

NIST Special Publication 800-45, revision 2,[3] provides guidance on securing electronic mail and section 2 of the guidance provides a detailed description on how email functions. Section 2.1 Background and section 2.2 Multipurpose Internet Mail Extensions SP 800-45 are extracted and included below:

2.1 Background

An understanding of how email messages are composed, delivered, and stored is helpful in understanding email security. For most email users, once a message is composed and sent, it leaves the computer and magically appears in the intended recipient's inbox. This may seem simple but the handling and delivery of an email message can be as complex as that involving physical mail, with processing and sorting occurring at several intermediary locations before arriving at the final destination.

The [email delivery] process starts with message composition. The most basic mail clients typically ask the user to provide the following: subject line, message content, and intended recipients. When these fields are completed and the user sends the message, the message is transformed into a specific standard format specified by Request for Comments (RFC) 2822, Internet Message Format.

At the most basic level, the two primary [email] message sections are the header and the body. The header section contains the vital information about the message including origination date, sender, recipient(s), delivery path, subject, and format information. The body of the message contains the actual content of the message.

Once the message is translated into an RFC 2822 formatted message, it can be transmitted. Using a network connection, the mail client, referred to as a mail user agent (MUA),

[3] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-45ver2.pdf

connects to a mail transfer agent (MTA) operating on the mail server. After initiating communication, the mail client provides the sender's identity to the server.

Next, using the mail server commands, the client tells the server who the intended recipients are. Although the message contains a list of intended recipients, the mail server does not examine the message for this information. Only after the complete recipient list is sent to the server does the client supply the message. From this point, message delivery is under control of the mail server.

Once the mail server is processing the message, several events occur: recipient server identification, connection establishment, and message transmission. Using Domain Name System (DNS) services, the sender's mail server determines the mail server(s) for the recipient(s). Then, the server opens up a connection(s) to the recipient mail server(s) and sends the message employing a process similar to that used by the originating client. At this point, one of two events could occur. If the sender's and recipient's mailboxes are located on the same mail server, the message is delivered using a local delivery agent (LDA). If the sender's and recipient's mailboxes are located on different mail servers, the send process is repeated from one MTA to another until the message reaches the recipient's mailbox.

When the LDA has control of the message, a number of possible events may occur. Depending on the configuration, the LDA could deliver the message or process the message based on a predefined message filter before delivery (filtering can be based on a number of message properties and is discussed in detail in Section 6.2.2). Once the message is delivered, it is placed in the recipient's mailbox where it is stored until the recipient performs some action on it (e.g., read, delete) using the MUA. Figure 2.1 illustrates the flow of the message through the various mail components discussed previously. This is the general process of sending an email.

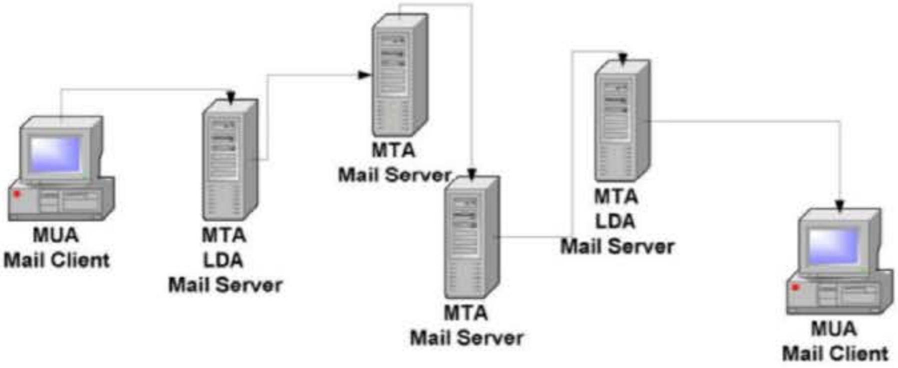


Figure 2.1: Example of Message Flow

2.2 Multipurpose Internet Mail Extensions

RFC 2822 provides a standard for transmitting messages containing textual content; however, it does not address messages that contain attachments, such as a mail message with a word processing document or photo included. Making use of the headers in an RFC 2822 message, the Multipurpose Internet Mail Extensions (MIME) provide almost endless possibilities to describe the structure of rich message content. MIME uses the convention of content-type/subtype pairs to specify the native representation or encoding of associated data. Examples of content types include the following:

- Audio – for transmitting audio or voice data.
- Application – used to transmit application data or binary data.
- Image – for transmitting still image (picture) data.
- Message – for encapsulating another mail message.
- Multipart – used to combine several message body parts, possibly of differing types of data, into a single message.
- Text – used to represent textual information in a number of character sets and formatted text description languages in a standardized manner.
- Video – for transmitting video or moving image data, possibly with audio as part of the composite video data format.

The current MIME standards include five parts: RFCs 2045, 2046, 2047, 4289 (which replaced 2048), and 2049 (see Appendix B). They address message body format, media types, non-American Standard Code for Information Interchange (non-ASCII) message header extensions, registration procedures, and conformance criteria, respectively. With this added functionality, email features such as message attachments and inline hypertext markup language (HTML) are possible. Although MIME extensions allow for binary message content, such content is incorporated into an RFC 2822 message using Base64 encoding, which provides a textual representation of binary data.

Appendix B: Teams Description

Microsoft Teams

Teams is a collaboration software as a service (SaaS) tool that includes chat, video conferencing, telephony, and file sharing. Teams is built on Microsoft 365 groups that leverages identities stored in the Azure Active Directory (AAD). AAD integrates with on-premise active directory (AD) and if **Teams Federation** is turned on, the software permits users in one domain to use Teams features with users in another domain (e.g. sending chats and calling). Microsoft Teams is part of the FedRAMP Agency Authorization (75 agencies) for Office 365 Multi-Tenant and Supporting Services - Moderate, [4] authorized since 2014. Further, Azure Active Directory is Joint Authorization Board (JAB) authorized for both the Microsoft - Azure Commercial Cloud and Microsoft - Azure Government (includes Dynamics 365) JAB authorizations.

Microsoft Teams Federation

Federation is Microsoft's term for a collection of domains that have established trust in the Microsoft Teams environment. Federation allows users in other tenant domains to find, call, chat, and set up meetings with other Teams users. External users have no access to group chats or team resources. Federation can connect Microsoft Teams to other organizations using Teams or Skype for Business on premises.

Federation functionality is analogous to email between domains, with the exception that a user can look up the recipient in any domain to which the Teams tenant is permitted through federation and Teams administration. Federation is not a new function in Microsoft Unified Communications products. It has been used widely since 2007 to connect organizations and functions similarly to sending an email message or making a phone call from one organization to another.

Microsoft Teams Federation Functions

Enabling external access in Teams permits users to:

- Chat with someone in another organization
- Call someone in another organization
- See if someone from another organization is available for call or chat
- Search for users across external organizations
- Identify as an external party
- Display presence

[4] https://marketplace.fedramp.gov/#!/product/office-365-multi-tenant--supporting-services?sort=productName

- Invite and be invited to a meeting directly

External access also permits agencies to record messages, maintain phone call records, and align Teams use with agency policies for various data loss prevention requirements. Using external access by an agency requires additional restrictions in order to meet privacy and records requirements, including:

- Users cannot share files
- Users cannot access Teams resources
- Users cannot be added to a group chat
- Additional users cannot be added to a chat with an external user
- Out of office message is not shown

These restrictions are best implemented through provisioning, Teams configuration, and end-user agreements.

Difference between how Teams finds a person and how an e-mail is routed

While email relies on specific internal and external Mail Transfer Agent (MTA) servers, Teams uses the active directory to lookup users inside the tenant domain and Azure Active Directory (AAD) to lookup users outside the chat initiator's tenant domain. If the recipient does not have Teams, a chat can still be initiated, but the initiator cannot see their status. For chat, the recipient only needs a connection to the internet and a modern web browser and a way to receive the link to the chat (email).[5]

The similarity in function of the two are within the DNS server for email and Azure AD for Teams functionality. These two components do not function as a direct connection within the context of an interconnected system, but as relays to pass information via the sender and recipient servers.

External access in Teams

By default, external access (federation) is turned on in Teams,[6] which means that the organization can communicate with all external domains. If block domains are added, all other domains will be allowed; and if allowed domains are added, all other domains will be blocked. There are three scenarios for setting up external access in the Teams admin center:

[5] https://docs.microsoft.com/en-us/microsoftteams/teams-architecture-solutions-posters#teams-as-part-of-microsoft-365

[6] https://docs.microsoft.com/en-us/microsoftteams/manage-external-access

Appendix B: Teams Description

1. **Open federation:** This is the default setting in Teams, and if enabled, lets users in an organization find, call, chat, and set up meetings with users external to that organization in any domain. In this scenario, users can communicate with all external domains that are running Teams or Skype for Business AND are using open federation OR have added the domain to their allow list.
2. **Allow specific domains:** By adding domains to an Allow list, administrators limit external access to only the allowed domains. Once an administrator sets up a list of allowed domains, all other domains are blocked. To allow specific domains, click Add a domain, add the domain name, click Action to take on this domain, and then select Allowed.
3. **Block specific domains:** By adding domains to a Block list, administrators permit users to communicate with all external domains except those that are blocked. To block specific domains, click Add a domain, add the domain name, click Action to take on this domain, and then select Blocked. Once administrators set up a list of blocked domains, all other domains will be allowed.

Number two and three above constitute a **closed federation.** The preferred method for establishing agency-to-agency connections for the purpose of using the Teams chat feature is through **allowing specific domains**, thereby blocking all unnamed domains.

When external access is permitted in a Teams instance, the chat initiator looks up the chat recipient within permitted domains. The chat initiator will be able to see their status, initiate audio or audio/video chat, send text messages, and if telephony is enabled, make a telephone call using the keypad icon.

Conversely, Teams also permit guest access. Guest access differs from federation in that a "guest" is authorized within a particular instance of Teams and will have full access to all agency Teams resources within the guest access permissions. In other words, a guest has access credentials into the agency's Teams environment. Such access should be treated like any other access into an agency's information systems.

Federation of non-Microsoft products

Another major provider of workspace platforms in the government is Google. Google has the capability to permit collaboration across domains. It is implemented in a different manner than Microsoft in that Google partnered with a 3rd party provider called Federated Directory. However, Federated Directory is a provider located outside the United States (Netherlands) and is not part of the authorization associated with the Google Workplace FedRAMP JAB approval for Google Workplace. There are also other options to federate Google workplace and even federate between Google Workplace and other collaboration tools.

Appendix B: Teams Description

It is also feasible to federate between collaboration platforms (Office 365 and Google Workplace), but that mechanism would have to be further developed through third party integration.

FedRAMP Authorized Collaboration Tools

To increase interagency collaboration, all agencies should whitelist collaboration tools that: 1) are FedRAMP authorized, 2) do not require an account for guest access, and 3) are accessible on a web browser (i.e., no downloads required). The following is a list of the current collaboration tools that meet these requirements:

- □ **Adobe Connect** (Video Conferencing)
  Guest access allows: video conference*
  FedRAMP* Moderate *Authorization by: *Joint Authorization Board (JAB)*

- □ **Adobe Document Cloud** (File Sharing)
  Guest access allows: download files, comment on PDFs, fill and eSign PDFs
  FedRAMP Li-SaaS Authorization by: *United States Agency for Global Media*

- □ **Amazon Chime** **(**Video Conferencing)
  Guest access allows: video conference*
  FedRAMP* Moderate *Authorization by: *JAB only for the AWS US East/West Regions (not GovCloud)*

- □ **Amazon WorkDocs** **(**File Sharing)
  Guest access allows: view-only for documents
  FedRAMP* Moderate *Authorization by: *JAB*

- □ **Google Workspace** (File Sharing, Document Collaboration)
  Guest access allows:** downloading/uploading/preview files in Google Drive, editing/commenting in Google, Docs, Sheets, Slides, Drawings, Forms; no pin sharing required to fill out and submit Google Forms
  FedRAMP Moderate Authorization by: *General Services Administration for Google Workspace (FedRAMP high authorization in progress by JAB)*

- □ **Google Meet** (Video Conferencing)
  Guest access allows: video conference*
  FedRAMP Moderate Authorization by: *See above for Google Workspace*

- □ **Microsoft 365** (File Sharing, Document Collaboration)
  Guest access allows:** downloading/uploading files in OneDrive, editing and commenting in O365 tools: Microsoft Word, Excel, and PowerPoint
  FedRAMP Moderate Authorization by: *Department of Health and Human Services for Office 365 Multi-Tenant & Supporting Services also known as Microsoft GCC (FedRAMP high authorization for Microsoft GCC High in progress by DOJ)*

- □ **Microsoft Teams** (Video Conferencing)
  Guest access allows: video conference*, download files (only during video conference)
  FedRAMP Moderate Authorization by: *See above for Microsoft 365*

- □ **Webex for Government** (Video Conferencing)
  Guest access allows: video conference*
  FedRAMP Moderate Authorization by: *Department of Health and Human Services*

- □ **ZoomGov** (Video Conferencing)
  Guest access allows: video conference*
  FedRAMP Moderate Authorization by: *Department of Homeland Security*

* Video conference includes the standard features of screen sharing, text chat, link sharing, and view participants. Additional tool-specific features may be available.

** Guests may require a verification or pin code in addition to a link to access without an account.

Guiding Principles for Edge Computing

April 26, 2021

Office of Information Integrity and Access

General Services Administration
Office of Government-wide Policy

Guiding Principles for Edge Computing

Overview

Edge computing decentralizes the collection, processing, and storage of data, which extends the network boundary while minimizing the impacts of network latency, bandwidth demands, and network costs. Correctly incorporating edge computing into an overall IT strategy reduces cost and increases efficiency. This document provides underlying context and guiding principles for federal agencies considering edge computing as part of their larger IT strategy.

Background

The arrival of new technologies like the Internet of Things (IoT) and 5G advance the possibilities of edge computing. Depending on the use, edge computing (or "edge") puts time-sensitive data processing closer to either the physical data source or end user. In edge, only processed data, as opposed to all raw data, is sent to the cloud or a wide area network for storage and distribution. Combining edge with IoT or 5G enables accelerated decision making because these advances allow for significantly faster processing and data analysis at the source or "edge" of information.

Edge data processing, analysis, and storage capabilities can fit within any network system of data centers or cloud. Regardless of network, the exchange of raw data, processed data, or analysis may use a high-reliability communication pathway or a more cost-effective communication pathway according to mission necessity. In its simplest implementation, the "edge" may be in the device itself, such as IoT in a mobile phone. In a more complex implementation, it may consist of a cluster of microprocessors that integrate and process multiple data feeds.

Business and government already generate large amounts of data that need to be distributed and used across networks. The emergence of the IoT has amplified large data collection, storage, and transmission. To help manage this much larger landscape of data, edge computing reduces the amount of bandwidth and processing power required to transfer data between local, wide area, and cloud networks. The benefits of edge include low latency, and time-sensitive data acquisition and processing, which offer a hardware cost advantage. The guidance below outlines how edge computing should be part of a network strategy.

Guiding Principles

It's important to develop short- and long-term strategies for continued adoption and implementation of edge technology. The following are recommendations to help federal agencies harmonize edge computing with their data center and cloud adoption strategies. Agencies should work with the Data Center & Cloud Optimization Initiative Program

Management Office (DCCOI PMO) through the Integrated Data Collection (IDC) process to communicate any substantive changes to their Data Center metrics as a result of edge adoption.

The following steps will help you determine which services should remain at edge locations. Check out the Application Rationalization Playbook for greater detail on how to make these decisions.

A. Evaluate the mixture of cloud and data center service delivery with existing technology to determine if edge is more cost efficient, improves service delivery, creates resiliency, and is not a security threat. Refer to Step 6.3 of The Application Rationalization Playbook for guidance on how to analyze onsite hosting alternatives.

B. Consider how edge computing factors into your application rationalization strategy. Edge computing can be a cost effective, network efficient, and useful technology where there is a need for localized data collection and processing. It's also useful in cases where there isn't a need to transmit and store all data, such as real-time sensor monitoring. Agencies should make determinations to use edge computing for specific applications based on the following four criteria:

1. Latency/Determinism
2. Data/Bandwidth
3. Privacy/Security
4. Limited Autonomy

C. Incorporate edge data into your overall data management to distinguish between relevant and noisy data from edge devices. This will provide more accurate data to inform your long-term data warehousing strategy within an evolving IT architecture.

D. Ensure edge devices are incorporated into the network cybersecurity strategy.

1. Ensure edge devices follow the security and privacy controls outlined in the most recent NIST guidance.
2. Ensure edge devices are optimized for internal operations and network monitoring.

For more information about this guidance, contact the DCCOI PMO at: dccoi@gsa.gov. The Cloud and Infrastructure Community of Practice (CoP) also provides meeting materials and a link to a more detailed knowledge portal. Anyone with a ".gov" or ".mil" email address may access the CoP through the MAX Federal Community.

Interagency Collaboration Analysis and Recommendations

September 2021

U.S. Federal Chief Information Officers Council
U. S. Office of Management and Budget
and
Office of Information Integrity and Access

General Services Administration
Office of Government-wide Policy

Table of Contents

Executive Summary **4**

Background **5**

Methodology **6**

Challenges to Implementing Interagency Collaboration **7**
Policy Compliance 7
Security Policies 7
Records Management Policies 8
Agency Specific Policies 9
Procurement Issues 9

Collaboration Areas **9**
Collaboration Suites 9
Collaboration Suites Used by Federal Agencies 10
Challenges to Interagency Collaboration 10
Collaboration Suite Recommendations 11
Email 12
Email Solutions Used by Federal Agencies 12
Challenges to Government Collaboration 12
Email Recommendations 12
Calendar 13
Calendar Solutions Used by Federal Agencies 13
Challenges to Government Collaboration 13
Calendar Recommendations 14
Video Conferencing 15
Commonly Used Video Conferencing Solutions 16
Challenges to Government Collaboration 16
Video Conferencing Recommendations 17
Text-based Chat 18
Text-Based-Chat Solutions Used by Federal Agencies: 18
Challenges to Government Collaboration 18
Text-based Chat Recommendations 19
Large File Sharing 19
File Sharing Solutions Used by Federal Agencies 20
Challenges to Government Collaboration 20
File Sharing Recommendations 21
Document Collaboration 22
Document Collaboration Solutions Used by Federal Agencies 22

Challenges to Government Collaboration 22
Document Collaboration Recommendations 23
Overall Recommendations for Improving Interagency Collaboration 24
Interagency Collaboration Recommendations - Short Term 24
Interagency Collaboration Recommendations - Long Term 26
Establishing a PMO for Interagency Collaboration 26
Program Governance 27
Program Management 27
Responsibilities of the PMO 28
Appendix A: Slack in the United Kingdom Case Study 30
Appendix B: FedRAMP-Authorized Collaboration Tools 32
Appendix C: Enabling Calendar Sharing and Guest Access for Collaboration 33
Appendix D: In-House Scheduling Solution for MAX.gov 40

Executive Summary

The U.S. Government increasingly relies on collaboration capabilities to achieve its mission. The ability to meet and conference virtually, send text messages, share large files, view external calendars, and collaborate on documents is critical to operations in a modern federal agency and instrumental in a telework-dominant world.

Delivering exceptional customer experience takes an interconnected government. Throughout the pandemic, cross-government collaboration was remarkable. However, it highlighted the need for cross-government collaboration tools. Every department and agency continues working at unprecedented levels of telework -both in volume and scope of activities, and importantly, sustaining performance. End-to-end communications and processes cut horizontally and vertically through multiple levels of government.

To resolve interagency collaboration challenges, the federal government needs to consider both short-term (by end of FY22 Q2) and long-term (by end of FY23 Q2) strategies with a focus on the governance, technical, policy, and procurement aspects of interagency collaboration. Below are the following key short-term recommendations for interagency collaboration, some of which are currently in implementation:

- All agencies should whitelist web client versions of office productivity and collaboration tools that have a FedRAMP authorization and do not require account creation.[1]
- All agencies should identify procedures, appropriate to their mission and security posture, to allow guest access to their collaboration suites.[2]
- All agencies should configure their Exchange and Gmail services to allow person-to-person sharing of calendars (free/busy) across agencies.[3]
- The National Archives and Records Administration (NARA) should update NARA Bulletin 2009-02, conduct a formal assessment, and issue new guidance as needed for virtual meetings and document collaboration in multi-agency environments.
- FedRAMP should incorporate a supply chain risk assessment (SCRA) as part of security controls baseline to ensure that all agencies can leverage FedRAMP authorizations.
- A dedicated office should oversee the Microsoft 365 Teams federation pilot and scale it to include more agencies.

Additionally, one long-term recommendation is to establish a program management office (PMO) at General Services Administration (GSA) to have a centrally-managed office to standardize technology adoption for interagency collaboration, ensure an aligned strategy across the government, and provide a learning environment for this work.

[1] See Appendix B: FedRAMP-Authorized Collaboration Tools for details.
[2] See Appendix C: Enabling Calendar Sharing and Guest Access for Collaboration for details.
[3] ibid.

Background

The Office of Management and Budget (OMB) Memo M-21-25 states that "Agency leaders can leverage issues such as telework, remote work, and flexible work schedules as tools in their broader strategies for talent recruitment and retention, and for advancing diversity, equity, inclusion, and accessibility in the Federal workforce."[4] Modern, cloud-based, collaboration tools can provide for this flexibility and enhance productivity by giving team members the ability to collaborate together from anywhere, in real time. New technologies in collaboration areas, such as email, calendar, video conferencing, text chat, file sharing, document collaboration as well as collaboration suites, which encompass all the collaboration areas mentioned, can be leveraged for more efficient collaboration.

For several years, the Federal Government attempted to find solutions to increase interagency collaboration in an efficient, secure, and cost-effective manner. While previous attempts identified problems and potential solutions, the Federal Government still lacks a cohesive strategy to sustain continued virtual interagency collaboration. This lack of guidance on the best solutions and practices for collaboration tools has resulted in agencies pursuing different paths and acquiring multiple solutions of similar collaboration tools.

Previous Attempts to Address Interagency Collaboration

The Federal Government has long recognized the need for agencies to work together in a secure and efficient manner. Several teams and agencies have attempted to find solutions to this problem, but few had lasting success. More than a decade after the first government-wide collaboration platform was established to address problems with interagency collaboration, many of the same problems still exist. Below is a brief timeline of the most significant efforts:

2007 OMB created the government-wide collaboration platform, MAX.gov, to pass back-and-forth budget information between OMB and agencies during the budgeting process.[5]

2013 GSA's Federal Strategic Sourcing Initiative (FSSI) and the GSA SmartBUY program team up to develop and implement sourcing and management strategies to lower the Federal Government's total cost of ownership of commercial software. However, bid protests and other challenges in establishing this blanket purchase agreement (BPA) sidelined the effort and the procurement vehicle was not established.

2015 A Presidential Innovation Fellow team established a cloud-based platform that allowed for chat and document exchange. Although this project did not gain

[4] https://www.whitehouse.gov/wp-content/uploads/2021/06/M-21-25.pdf
[5] https://www.thegovlab.org/static/files/smarterstate/MAX.pdf

traction, it identified cultural and policy barriers to cross-government collaboration.

2017 GSA TTS, NIST, DHS, OFCIO, USDS, and OSTP created a Tiger Team to improve document collaboration across government.[6] The Tiger Team highly recommended, as a first step, moving to cloud-based email suites. The team also highlighted many of the problems in government with interagency document collaboration, but never finalized results or recommendations from this effort.

A limited outcome from this Tiger Team resulted in an OMB initiative for government-wide adoption of cloud-based email suites. This became one of the Information Technology (IT) Modernization goals of the President's Management Agenda: to improve the proportion of CFO (Chief Financial Officers) Act agency inboxes, hosted by cloud services, from 44% to 84% from FY 2018-2020. However, lack of interest from leadership caused the initiative to dissipate.

2020 A Tiger Team was created after the dramatic expansion of telework due to COVID-19, which further exposed the fragmented nature of interagency collaboration. The team aimed to produce best practice documents and a series of both long-term and short term recommendations. In July 2020, the team suggested four solutions from-short term to long-term: configuration, federation, shared services, and interoperability. The team did not take any further action to implement the proposed solutions.

Ongoing In an ongoing effort, the CIO Council and OMB's Office of the Federal Chief Information Office (OFCIO) piloted a small number of Microsoft-to-Microsoft federation programs between agencies of varying size. The first official federation of Teams was completed in Q1 FY21. An instruction manual was created for Microsoft-to-Microsoft federation and additional agencies are joining the federation pilot.

Ongoing As part of the migration efforts of MAX.gov from OMB to GSA's Technology Transformation Service (TTS), a full analysis of MAX.gov and its features is performed and a new plan is established to better support interagency collaboration beyond passing budget information between OMB and agencies.

Methodology

At the request of the CIO Council, GSA's Emerging Technology Division in coordination with OMB, conducted research on the following collaboration areas: email, calendar, video

[6] Tiger team consists of: GSA's Technology Transformation Service (TTS), National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), OMB Office of the Federal Chief Information Officer (OFCIO), U.S Digital Service (USDS), and the Office of Science and Technology Policy (OSTP).

conferencing, text chat, file sharing, document collaboration as well as collaboration suites, which encompass all the collaboration areas mentioned. The goal was to identify the barriers to interagency collaboration in each area and to provide solutions. In researching barriers, this interagency collaboration team thoroughly reviewed technical capabilities, policy, and procurement barriers. The review of policy focuses on security, records retention, and existing agency policies. The interagency collaboration team then proposed recommendations for each collaboration area and overall short-and long-term recommendations.

Challenges to Implementing Interagency Collaboration

The interagency collaboration team found the technical implementation challenges are minor. Often, technology is more than capable of allowing agencies to work together across agency boundaries; however, agencies do not configure and implement the tools they have for situations requiring interagency collaboration. This issue is often traced to compounding policy or procurement issues. Below are several key policy and procurement challenges preventing the Federal Government from leveraging the benefits of modern collaboration tools for interagency use.

Policy Compliance

There are many commercial tools available to help agencies collaborate with each other. However, the need to comply with both government-wide and agency policies prevent agencies from leveraging many of those tools for interagency collaboration. Agencies must consider security, accessibility, records retention, and other legal requirements when using collaboration tools. The need to comply with various policies sometimes leads an agency to either bar employees from using collaboration tools or to put restrictions on use of the tools rendering them less effective for interagency, or even intra-agency, collaboration.

Security Policies

Cybersecurity and information security are both top priorities in federal information technology acquisitions. Agencies choose products that meet their security needs and configure based on their security needs / interpretations. Agencies must comply with numerous cybersecurity policies, such as the Federal Information Security Management Act (FISMA), the National Institute of Standards and Technology (NIST) Cybersecurity Framework, Trusted Internet Connection (TIC) 3.0, Zero Trust, and OMB Circular A-130 among other policies. Additionally, agencies must ensure that all cloud products have a FedRAMP authorization or meet FedRAMP's baseline security controls.

In addition, some agencies also have additional statutory requirements they must comply with. For example, since fiscal year 2013, annual appropriations legislation requires that before the Departments of Commerce and Justice, the National Aeronautics and Space

Administration, and the National Science Foundation acquire a high impact or moderate impact information system(s), the agencies must perform a SCRA of both the information system and the proposed awardee. Additionally, those agencies must consult with the Federal Bureau of Investigation prior to acquiring the system.[7] Due to each agency's unique risk profile and statutory requirements, different security offices interpret risk and best practices differently across agencies. That is why one agency's Federal Information Processing Standards (FIPS) -199 evaluation may lead them to conclude that an IT system is secure and acceptable to use while another agency's FIPS-199 evaluation results in a different conclusion. To reduce risk, collaboration tools or features may be disabled or configured to prevent interagency collaboration. NIST SP-800-53 Rev. 5 includes a SCRA, and FedRAMP is working to include it into their baseline, but there are additional controls required to meet annual appropriations legislation.

Records Management Policies

Agencies must also consider records management requirements under the Federal Records Act, the Presidential Records Act, and the Freedom of Information Act (FOIA), all of which were enacted prior to the adoption of cloud-based collaboration tools. The most recent direction provided to agencies on how to manage records in a multi-agency environment originates from the National Archives and Records Administration (NARA) Bulletin 2009-02, which does not provide adequate guidance on records creation and maintenance when using video conferencing tools nor document collaboration.[8]

NARA Bulletin 2009-02 "provides guidance on managing records when Federal agencies collaborate in multi-agency environments."[9] The bulletin defines multiagency environments as "collaborative endeavors in which two or more Federal agencies share information to meet common goals," and outlines how agencies should manage records when working in a multi-agency environment including the information that needs to be managed, who is responsible for managing the records, the record management responsibilities. However, the bulletin falls short as it does not address how agencies should manage records that are created using tools such as video conferencing and document collaboration for cross-agency collaboration.

As collaboration efforts grow in size, scope, and complexity, the question of what records are created by collaboration tools, how and what to retain, the ownership of those records, and who is responsible for maintaining them becomes more uncertain. For example, agencies have different interpretations of how records are created when a virtual meeting takes place using a video conferencing tool. Some agencies consider a videorecording of the meeting to be the official record of the meeting. Other agencies consider any videorecording of a meeting to be supplemental to the official record of the meeting. Agencies also differ on whether the different functions used during a video conference

[7] Consolidated Appropriations Act, 2021 (P.L. 116-260)
[8] https://www.archives.gov/records-mgmt/bulletins/2009/2009-02.html
[9] Ibid.

meeting, such as chat or polls, are considered a record. Often, this is at the expense of collaboration features, which may be turned off to prevent accidental creation of records.

Agency Specific Policies

Agencies may have policies in place that prohibit the use of collaboration tools for dated reasons that may no longer be relevant. For example, years' old policies blocking certain domains can prevent agencies from being able to use FedRAMP-authorized tools to work with other agencies. Some agencies block their employees from accessing the Google domain even though Google Workspace has received FedRAMP authorization and is used by other federal agencies, including GSA and NARA. As a result, employees at agencies that block the Google domain cannot join virtual meetings hosted on GoogleMeet.

Agencies may also have unique statutory requirements that prevent them from using cloud-based collaboration tools to work with other agencies. Similar to the requirement in annual appropriations law, that some agencies must consult with the FBI before acquiring certain telecommunications technology, each agency must have policies in place to comply with its statutory requirements. These policies can affect the tools an agency uses, how those tools are configured, and the extent in which an agency can collaborate with another agency.

Procurement Issues

Agencies acquire solutions to fit their immediate needs and establish configurations for those solutions without consideration for using them for interagency collaboration. Without centralized guidance, agencies often acquire different collaboration tools to solve for the same needs. While agencies should avoid vendor lock-in, having too many tools that serve a single purpose can be a waste of resources; especially when tools are not cross-compatible across organizations. GSA tried to develop and implement sourcing and management strategies to lower the Federal Government's total cost of ownership of commercial software using a blanket purchase agreement (BPA), but these efforts were sidelined and the procurement vehicle was not established due to bid protests and other challenges. Similar efforts have resulted in the same outcomes.

Collaboration Areas

Collaboration Suites

A collaboration suite is a collection of cloud computing, productivity, and collaboration tools offered under one suite. For the purposes of this paper, collaboration suites include email, calendaring, text chat, video conferencing, real-time document collaboration, and large file sharing. Collaboration suites are essential to accomplishing work and achieving mission goals. Rather than seeking to acquire collaboration tools individually, agencies procure one collaboration or productivity suite with a variety of tools. Collaboration suites often provide economies of scale and offer interoperable tools and features. For a collaboration solution to be secure for use within the Federal Government, the platform must be FedRAMP-authorized.

Collaboration Suites Used by Federal Agencies

- Microsoft 365
- Google Workspace

Challenges to Interagency Collaboration

Currently, agencies are focused on operating within their collaboration suites and not on configuring collaboration suites to be conducive to interagency collaboration. Due to additional security, identity, policy, and uncertainty risks, many agencies choose to prohibit features that enable collaboration outside their organization (e.g., federation and guest access), or even within the agency (e.g., text chat).

Agencies may also believe that NIST SP-800-47 requires them to negotiate a Memorandum of Understanding/Agreement (MOU/A) with each agency they want to federate with or provide guest access to.[10] NIST SP-800-47 specifically addresses interconnected systems and defines an interconnected system as one that shares a direct connection. The examples of a "direct connection" NIST offers include a dedicated circuit (e.g., dial up, T Carrier, synchronous optical network, etc.) or Virtual Private Network (VPN).[11] However, analysis conducted for the Microsoft 365 Teams federation pilot determined that external access to Microsoft Teams does not rely on a direct connection. Instead, Microsoft Teams functions like email -- traffic is sent between the edge services based on Domain Name System (DNS) server lookups of the recipient and destination domains. Therefore, when establishing federation between agencies using Microsoft Teams and potentially other collaboration suites, an agency-to-agency MOU/ISA is not required.

Microsoft offers three 365 environments to federal agencies: the Government Community Cloud (GCC), Government Community Cloud High (GCC High), and the MS Department of Defense (DoD) Cloud. It is not possible to federate or provide guest access across different 365 environments to meet federal security standards. For the purposes of this paper, references to Microsoft 365 means Microsoft 365, GCC at FedRAMP-(moderate) authorized solution to meet the needs of most federal agencies that do not handle classified information. Additionally, across all cloud environments, Microsoft offers two license versions of 365: G3 and G5. G5 licensing offers additional security tools and other capabilities for the hosting agency. As long as they are in the same environment (i.e., GCC, GCC High, DoD), agencies do not need to use the same license version (i.e., G3, G5) of Microsoft 365 in order to federate with each other.

[10] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-47.pdf

[11] http://what-when-how.com/data-communications-and-networking/dedicated-circuit-networks-data-communications-and-networking/

Agencies using Google Workspaces find it challenging to collaborate with agencies that block the Google domain as a result of outdated policies. By blocking the Google domain, agencies effectively block employees from using Google tools. Agencies first blocked the Google domain out of concern that employees would use included tools to conduct personal business. However, this is both a technical attempt at solving a managerial problem and an antiquated policy. The justification for blocking the Google domain is dated and hinders agencies that use Google Workspace from federating with and providing guest access to agencies that do not use Google Workspace.

True integration between Microsoft 365 and Google Workspace is challenging. While the government has success with Microsoft 365 to Microsoft 365 federation, no such success has been accomplished between Microsoft 365 and Google Workspace. Additionally, federation between agencies using the same Microsoft 365 cloud environment is possible because the cross-domain identity tool, Azure Active Directory, is within the FedRAMP authorization boundary. Federation between two or more agencies using Google Workspace or Google Workspace to Microsoft 365 can be done by setting up security assertion markup language (SAML) between services or tenants, but this solution has not been tested and may not fall under the current FedRAMP authorization. Additionally, there are third party applications, such as federated.directory, which can establish similar integrations.

Collaboration Suite Recommendations

Short term:

1. Agencies should update or establish a policy that would allow employees to grant guest access to their collaboration suite.
2. In addition to CIO Council's continuing the Microsoft 365 federation pilot:
    a. OMB should expand the current Microsoft 365 federation pilot by:
        i. Increasing the number of participating agencies
        ii. Replacing MOU requirements with government-wide registry agreement
    b. GSA should conduct a similar pilot for Google Workspace environments. Google Workspace federation pilot should explore:
        i. Google Workspace to Microsoft 365 integration and calendar interoperability
        ii. Google Workspace to Google Workspace integration and calendar interoperability
        iii. Additional 3rd party options as needed
3. Agencies should use additional collaboration tools (e.g., video conferencing) for interagency collaboration to create necessary redundancies to have fallback options, to prevent vendor lock-in, and provide resiliency to best fit agencies' needs.

Long term:

1. Establish a program management office (PMO) to be a centrally managed office that can standardize the adoption of technology for interagency collaboration, provide technical assistance, address government-wide policy or records challenges, ensure

an aligned strategy on interagency collaboration tools across the government, and work with various offices to establish a contract vehicle offering best in class collaboration tools configured for interagency collaboration. To support use of collaboration suites for interagency collaboration, the PMO should:

a. Ensure that any contracting vehicle for interagency collaboration offers instances of Microsoft 365, Google Workspace, and any other best-in-class collaboration suite that are configured for interagency collaboration.
b. Evaluate whether new collaboration suites are suitable for use in the federal government.
c. Continue on-going efforts to support collaboration suite integration across agencies; including support and scaling of Microsoft 365 Teams federation efforts.

Email

Email is a critical form of communication for all sectors of the workforce and is unique because it is interoperable between vendors. Regardless of the email tool, any agency can send an email to another agency or the private sector with few problems. Unlike other methods to exchange messages such as social media platforms, emails can be exchanged to or by anyone through a variety of mechanisms without the need for individuals to use the same company or platform. At this time email is one of the most effective collaboration tools that the federal government uses, and it is the building block for connecting other services and people.

Email Solutions Used by Federal Agencies

- Microsoft Outlook
- Google Gmail

Challenges to Government Collaboration

Due to the maturity and interoperability of email, there are few challenges to collaboration for the Federal Government in this area. However, there are still issues of important emails getting blocked; such as, when a sending mail server has been accidentally placed on an agency's blacklist rather than on a proper whitelist, or if the DomainKeys Identified Mail (DKIM) signatures are not read properly. For instance, there is a known Microsoft issue of rejecting Google Calendar update emails because only the first DKIM signature is read (i.e., Google) while the second signature is ignored (i.e., the sending agency).

Email Recommendations

Short term:

1. Agencies should ensure fullest use of email that comes with collaboration suite features.
2. Agencies should continue to work with partner organizations to ensure business emails are not blocked.

Long term:

1. Agencies should have a long-term strategy in the event they change email providers to avoid challenges related to transitioning to different versions of the same email provider.

Calendar

Scheduling and tracking meetings are essential parts of any business. To help users track their commitments, many calendar solutions need to integrate with email solutions to offer calendar assistants, automated appointment reminders, automated calendar creation from links or emails, and other reminders. The most useful feature for collaboration is the ability for a user to view another person's availability to determine when the person is free for a meeting rather than sending emails back-and-forth to determine availability. The ability to view and share an individual's calendar with others is an effective means to schedule meetings and is crucial to interagency collaboration.

If the organization enables sharing, then an individual can allow others outside of their organization to view their calendar. An individual can "share" their calendar with others using the same calendar platform (i.e., Microsoft 365 to Microsoft 365 or Google Calendar to Google Calendar[12]), or an individual can "publish" their calendar to the public, produce an Internet Calendar Subscription (ICS) link, and share this link with others using any calendar platform.[13]

There are also scheduling solutions that do not require individuals to share or publish their calendar. One type of solution integrates with users' calendars and suggests dates and times when participants are available to meet. Another type of tool allows each meeting participant to submit the dates and times when they are available, and the tool suggests times when all participants have indicated they are free to meet.

Calendar Solutions Used by Federal Agencies

- Microsoft Calendar
- Google Calendar
- Max.gov

Challenges to Government Collaboration

Federal employees spend countless hours scheduling meetings. 40% of workers waste up to 30 minutes a day just searching for a collaborative space for meetings.[14] The root cause of this problem is the inability for agency employees to share their calendars with individuals outside of their agency, bureau, or department. Sharing calendars with external

[12] https://support.microsoft.com/en-us/office/share-your-calendar-in-outlook-com-0fc1cb48-569d-4d1e-ac20-5a9b3f5e6ff2

[13] https://www.eui.eu/ServicesAndAdmin/ComputingService/EMail/GuideCalendarPublishShareDifference.aspx

[14] https://www.wsj.com/articles/new-office-flashpoint-who-gets-the-conference-room-1413307377

collaborators is restricted at many agencies due to security and privacy concerns. Agencies fear that sharing or publishing calendars will expose their data to malicious actors. Further, agencies are concerned the synchronizing function could lead to increased malware incidents. Additionally, while sharing calendars between different collaboration suites is feasible, the steps required to do so are complicated and it has not yet been done between federal agencies.

Sending and receiving calendar invites and updated notifications still remains a problem between certain agencies. Even if the initial meeting invite is delivered between agencies using different collaboration suites, any updates and cancellations can lag, duplicate the invite, or fail to arrive due to the recipient's mail server blocking the email notification. This causes unnecessary confusion to the invitees.

Calendar Recommendations

Short term:

1. Agencies should ensure calendaring server notifications are not blocked or restricted to ensure accurate and updated meetings.
    a. Whitelist domains between agencies to support meeting and event notifications.
    b. Agencies who have not migrated email systems to the cloud, need to ensure their security certificates are up-to-date and notifications are delivered.
2. Agencies should configure systems to enable:
    a. Calendar sharing[15] (i.e., public view of free/busy schedule). This will allow employees to publish their calendars with those individuals outside of the agency, bureau, or department that utilize the same collaboration suite, to the extent practicable.
        i. NOTE: When sharing between collaboration suites, calendar availability behaves as a snapshot of the calendar and may not reflect updates in real time.

Long term:

1. Agencies shall continue to federate Microsoft Teams, especially focusing on calendar integration.
2. Agencies shall continue to pilot Microsoft Teams to Google Workspace integration for calendar
3. GSA Technology Transformation Service (TTS) should provide a calendar feature on Max.gov that would allow Max.gov users to publish their calendar availability and share their calendars.
    a. See Appendix N[16] for more information.
4. The centralized PMO established to standardize the adoption of technology of interagency collaboration tools should:

[15] See Appendix C: Enabling Calendar Sharing and Guest Access for Collaboration

[16] See Appendix D: Cross Agency Scheduling Solution Tool

a. Regularly evaluate calendar and scheduling tools and determine whether they meet government-wide standards and are suitable for interagency collaboration.
b. Ensure agencies have more than one avenue to share calendars and schedule meetings across agency boundaries.

Video Conferencing

Video conferencing is a live virtual meeting between two or more individuals in different locations. This includes the transmission of audio, video, text, and presentations in real time through the internet. A variety of enterprise and open-source video conferencing platforms continue to push out new features to their products in competition with each other. For the purposes of this paper, the following features are deemed necessary for the use of video conferencing for interagency collaboration:

- **Camera use:** The ability for individuals to show themselves using their camera functionality for more impactful communication and ability to display visual cues.
- **Screen Sharing:** This feature allows individuals to give presentations, display documents and slide decks, and allows for active collaboration with other participants, furthering productivity.
- **Recording:** Recording meetings allows hosts to review meetings and search back for specific information. Host control over recording features is also important to ensure confidentiality and prevent unknown individuals from downloading the recording.
- **Dial-in:** The option for dial-in allows individuals who may not have access to their computer, have unreliable bandwidth, or are otherwise unable to use video conferencing to join a meeting and participate.
- **Web Client Version:** Video conference platforms should also offer the option for participants to join through a web browser rather than downloading the application. This is an especially important feature as some agencies explicitly bar employees to download software or plug-ins onto their computers without permission.
- **No Account Setup to Participate:** Video conference platforms should also offer the option for participants to join without having to create an account. This is important because some agencies do not allow employees to create accounts using their work email address and federal employees cannot use personal email addresses to conduct official business.
- **FedRAMP Authorization:** FedRAMP standardizes the approach to security assessment, authorization, and continuous monitoring of cloud products and services. Federal agencies may only use cloud-based tools that are FedRAMP-authorized.
- **Additional Security and Privacy Features:** In addition to FedRAMP authorization, agencies may request additional security and privacy features to ensure meetings and data are protected. For instance, features that allow meeting hosts to password protect meetings, and create unique URLs, ability to delegate host duties, muting privileges, and removing individuals from meetings.

- **Section 508 Compliance:** Section 508 of the Rehabilitation Act requires federal agencies to make their electronic and information technology accessible to people with disabilities. For video conferencing this means the ability for the tool to provide live captioning, screen reading, keyboard shortcuts, and other features. These features may need to be available during the meeting and after the meeting (e.g., adding captioning to recorded meetings).

Commonly Used Video Conferencing Solutions

Table 1: Commonly Used Video Conferencing Solutions

Platform*	Used in Government	FedRAMP[17] Authorized	Dial-In Option	Live Captioning (508 compliance)
Adobe Connect	Yes	Yes	Yes	Participant captioner or StreamText
AWS Chime	No	Yes	Yes	No
Cisco Webex For Government	Yes	Yes	Yes	No
Google Meet	Yes	Yes	Yes	Speech-to-text AI
Jitsi (Open Source)	No	No	No	No
Microsoft Teams	Yes	Yes	Yes	Microsoft Automatic Speech Recognition (ASR) technology service
Verizon BlueJeans	No	No	Yes	Yes - native 3rd party speech-to-text vendor
ZoomGov	Yes	Yes	Yes	No - only through a 3rd party tool

*All of the tools provide the following features: web client version, secure access control, ability to record meetings, and screen sharing.

Challenges to Government Collaboration

Agencies are not just paying for their standard collaboration suite video conferencing tools, but some are paying for other video conferencing tools as well. While this creates redundancy and resiliency, each additional tool requires IT and procurement offices to support and be knowledgeable about those tools. In addition, several agencies have internal policies preventing individuals from using the video conference tools within their collaboration suites, ultimately paying for unused solutions and wasting financial resources.

[17] https://marketplace.fedramp.gov/#!/products?status=Compliant&sort=productName

This problem is exacerbated when agencies block access to FedRAMP-authorized tools. For example, GSA maintains at least four different video conferencing tools to host virtual meetings because many agencies block access to the Google domain.

Some agencies limit use of specific features or do not use video conferencing due to security issues, records retention and management policies, and the lack of technology in place to host or participate in video conferencing. This results in interagency meetings to be conducted only in-person or via phone.

Video Conferencing Recommendations

Short-term:

1. NARA should issue additional guidance on recording virtual meetings and video conferencing chats. Guidance should explicitly state:
    a. Meeting notes and/or meeting minutes are sufficient for records purposes, even for virtual meetings.
    b. Video conference chats are very similar to the side conversations that take place during in-person meetings and therefore should not be considered a record by default.
    c. Other virtual meeting participation features, such as polls, whiteboard, reactions or hands-up features should be treated the same as in-person conversations and not be considered a record by default.
    d. Recording a virtual meeting does not necessarily make it a record.
2. Agencies should whitelist tools and allow their employees to join via web browser meetings hosted on FedRAMP-authorized video conference tools that do not require an account creation.
3. Agencies should issue clear policy on the use of video conference tools for interagency collaboration. Policies should include:
    a. Employee responsibilities when participating in a video conference, versus hosting a video conference, including the retention of any records, any restrictions on use of the video conference platform’s features such as chat, screen sharing, and polling.
    b. A default policy that cameras should be turned on and detail situations where the use of the camera function is not allowed and/or when an employee should use the dial-in function.
        i. Agencies and offices that currently do not allow employees to use the camera to participate in video conferences should evaluate mitigating solutions, such as using preset or blurred backgrounds.

Long-term:

1. The centralized PMO established to standardize the adoption of technology of interagency collaboration tools should:

a. Regularly evaluate video conferencing tools and determine whether they meet government-wide standards and are suitable for interagency collaboration.
b. Work with CIO Council and other appropriate agencies to reduce the overall number of video conference tools used for interagency collaboration.

Text-based Chat

Also known as “instant messaging” or a “messaging” application, text-based chat is the ability to transmit text between individuals or groups of individuals in real time over the internet or other types of networks. Recently, text-based chats have become a key component of a project’s workflow. These applications are used to quickly relay information, get a response to a question, or pass along useful information in a format that is seen as less formal than sending an email. Messaging applications are taking the place of some in-person interactions and emails, and have shown to improve productivity. McKinsey Global Institute estimates that using tools like instant messaging can raise worker productivity by 20-25%.[18]

Text-Based-Chat Solutions Used by Federal Agencies:

- Google Chat
- Microsoft Teams
- Slack
- Cisco Jabber

Challenges to Government Collaboration

While individual agencies have adopted text-based chat applications for internal use, the Federal Government as a whole does not view chat applications as a key component of collaboration. Some agencies even disable the chat feature or do not configure their collaboration suites to allow their employees to use the chat tool to chat with others inside or outside of the agency.

Skepticism of chat platforms may be due to a belief that employees would use them for personal business which distracts them from performing their duties. However, the same criticism could be used for telephones or emails, neither of which face the same skepticism. As more employees own their own smartphones with access to various chat and social media platforms, and can use cellular data to chat, text, or conduct personal business, the concern that employees would use government-furnished equipment to text or chat does not align with current day practices.

Agencies also need better guidance on how to manage any records that come from a conversation over text based chat. To address this issue, some agencies direct their

[18] https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-social-economy

employees to document any record created over chat by taking a screenshot or emailing the substance of the conversation to create a record. Other agencies consider all chats, regardless of content, to be a record that must be saved and managed. Doing so takes more data storage and leads to unnecessary storage costs. In addition, this often discourages employees to use text based-chat in its intended way, leading employees to continue to rely on email for written interagency communication, which is not as efficient for quick replies as text messaging.

Text-based Chat Recommendations

Short-term:

1. Agencies should re-evaluate policies and, if needed, change policies to allow employees to use authorized chat tools.
2. Agencies should configure guest access within their collaboration suites to allow same collaboration suite users from other agencies to communicate using text-based chat.

Long term:

1. The centralized PMO established to standardize the adoption of technology of interagency collaboration tools should:
   a. Explore text-based chat solutions that can be implemented government-wide[19]

Large File Sharing

During the course of normal operations and especially during collaboration with other agencies or organizations, documents, data, and other materials need to be shared. Often, this data needs to be shared in a secure manner, especially if it contains personally identifiable information (PII), protected health information (PHI), controlled unclassified information (CUI), For Official Use Only (FOUO), or other sensitive information. One of the easiest ways to share such information is email, but this may not be possible if additional security on the data is required. Additionally, sharing large files is not possible through email due to size limitations (e.g., administrator set limitations for Microsoft Outlook and 25MB limit for Gmail). Alternative solutions are required for secure and large file sharing, either as a standalone product or part of an existing collaboration suite. These solutions need to offer the ability to share and receive large files securely (e.g., password protections, classification labeling, access controls, etc.), as well as scan for viruses before files are downloaded inside a network.

More recently, file sharing is quickly expanding beyond just sharing a file and is often embedded in a workstream. An effective file sharing solution needs to provide more than

[19] One example of this is Slack use in the UK. See Appendix A: Slack in the United Kingdom Case Study

the ability to share and should offer abilities to tie that file and actions around it to the business workstream. The Federal Government recognized the need for secure file sharing early, establishing Max.gov in 2007 to facilitate the sharing of budget information between OMB and agencies; this includes both sharing of files and the related workstream to get budgets approved. Max.gov expanded its capabilities to allow interagency teams to share files and collaborate by setting up a community page.

File Sharing Solutions Used by Federal Agencies

- MAX Drive
- Department of Defense Secure Access File Exchange (SAFE)
- Huddle
- Box
- Google Drive
- Microsoft OneDrive

Challenges to Government Collaboration

There are many file sharing options already available to the Federal workforce. In addition to stand alone tools, collaboration suites (i.e., Google Workspace and Microsoft 365) offer a rich set of functionalities in addition to file exchange. Collaboration suites are now net-native that allow users to collaboratively edit and share documents, spreadsheets, and presentations in a web browser. These functions can be enabled to be shared with users outside the organization (i.e., guest access). Unfortunately, many agencies choose to lock down these features due to security concerns.

In 2020, GSA's 10x team[20] researched whether there was a need for a custom file sharing solution to improve file sharing between and outside agencies. The 10x team identified individual IT policy constraints, challenges with identity management, information sensitivity, and storage / licensing costs as the largest challenges to building such a file sharing solution, but ultimately decided not to proceed because the true obstacles were based in agency policies rather than the lack of available technologies.

The biggest challenges are individuals knowing what to share, when, and with whom, which can be a delicate balance between openness and security. Federal IT policies result in a tendency to lean towards a more restrictive view on sharing, open sourcing, and collaboration. These restrictive policies often run counter to best practices, but for the case of government information sharing, a little friction may be a good thing. Setting deliberate specific (and often authenticated) recipients of information, building in additional time or approval steps, requiring planning and conversations around sharing between sender and recipient may seem like pain points, but these kinds of behavioral controls ultimately have a protective effect. Friction slows the sharing process down and ensures that the right

[20] The 10x program is part of GSA's Technology Transformation Services and is an incremental investment program to support and develop ideas from Federal employees about how technology can improve the public's experience with the Government.

information is shared with the right people, preventing unintended and potentially problematic disclosures.

On the other hand, the most common use case of large file sharing 10x found was staff sharing files with themselves. This means that IT policies limiting the types of tools that can be installed and used on a Federal Government computer produced a workaround where people routinely move data and other content on and off secure networks introducing potential security vulnerabilities.[21] The limits of current solutions and of IT policies may lead some individuals to rely on workarounds or use solutions that are not FedRAMP-authorized or otherwise approved by their agency.

Another issue discovered was lack of awareness of alternative FedRAMP-authorized file sharing solutions. However, a FedRAMP authorization does not necessarily mean that a federal employee can use that solution to share files. Federal employees also need to know which file sharing method(s) their agency allows them to use as well as the agency's policies for using file sharing tools.

File Sharing Recommendations

Short-term:

1. Agencies should configure their settings to allow guest access to federal employees and contractors and establish access controls to ensure that guests only have access to files or documents when granted.
    a. Agencies should use sensitivity labels to classify and protect documents, limit access to files and internal sites, and other collaborative spaces.
2. Agencies should issue clear policies on large file sharing outside of the agency. Guidance should include:
    a. When and how to provide guest access, including when access should be terminated and any restrictions on providing guest access.
        i. Including which FedRAMP-authorized product(s) are authorized for use within the agency
    b. The proper use of sensitivity labels and other security measures to prevent guests from downloading or copying files, if necessary.
    c. Allowing employees to receive files from other agencies when shared through FedRAMP-authorized tools.

Long-term:

1. Ensure Max.gov continues support of MAX Federal Community.
    a. Including a file sharing feature for federal employees at different agencies to upload and share large files.
2. The centralized PMO established to standardize the adoption of technology of interagency collaboration tools should:

[21] For more information, reach out to GSA's TTS for the 10x: Large File Exchange Phase 2 Report (January 21st, 2021)

a. Regularly evaluate and determine which tools for file sharing meet the technical and security standards established by the interagency board and present those tools for best-in-class determination.
b. Determine configuration settings for best-in-class collaboration suites and file sharing tools to allow for interagency sharing of large files.

Document Collaboration

Document collaboration allows two or more individuals to review, edit, and comment on a document at the same time in real time. In addition to providing a more efficient way to edit documents, document collaboration tools also allow users to have better control over a document's versions. Document collaboration solutions need to have several features to allow users to effectively work together on a single document:

- Allow for users from different organizations to work on a document at the same time and reflect any changes or comments immediately.
- Allow users to "tag" others on a document to assign work to an individual or notify them that something in the document needs their attention.
- Track and identify edits and comments from different users so that each user's edits are clearly distinguished from one another.
- Allow users to insert their edits as a suggestion, rather than directly into the document.
- Possess the ability to track different versions of the document, allow users to view previous versions, and allow users to revert to older versions of the document when needed.

Document Collaboration Solutions Used by Federal Agencies

- Google Workspace
- Microsoft 365

Challenges to Government Collaboration

When acquiring and deploying their collaboration suites, a top priority for agencies is to ensure only authenticated and validated users are able to access the system. Many agencies are reluctant to open up their collaboration suites to support guest access for document collaboration due to security concerns, identity management issues, and ownership questions.

Agencies are also reluctant to use new document collaboration tools as part of interagency working groups or teams because of questions regarding records retention and compliance with the Federal Records Act and FOIA. For example, when two or more agencies are collaborating on a document, the document is controlled by the host agency. However, the document or certain parts of it may be a record of the guest agency. This leads to confusion about whether guest agencies must maintain ownership of their contributions to the document or the whole document, and if guest agencies have a legal obligation to save the document in the federal records system.

Document Collaboration Recommendations

Short-term:

1. NARA should issue guidance to clarify how the Federal Records Act applies to interagency document collaboration. Guidance should include:
    a. Clear direction that only one agency can be the owner of a collaboration document. If this document serves as the record, all other copies are a snapshot of the document in time and are NOT the record (i.e., the copies made by non-owner agencies are NOT a record).
    b. Acknowledgement that the approach to record management of interagency document collaboration requires reciprocation agreements to ensure clarity on records management responsibilities
    c. Examples of MOU / reciprocity agreements between three or more agencies, including a single owner and single records retention schedule. Since NARA approves each agency's records retention schedule, any deviation of that via a Reciprocal Agreement may also require NARA approval. NARA should work to normalize this behavior via inspections / community outreach.
2. Agencies should configure their settings to allow guest access to federal employees and contractors and establish access controls to ensure that guests only have access to files or documents when granted.[22]
    a. Agencies should issue clear policies on when and how to provide guest access, including when access should be terminated and any restrictions on providing guest access.
3. Agencies should add FedRAMP-authorized document collaboration tools to their allow list.

Long-term:

1. The centralized PMO should work with the CIO Council and other stakeholders to:
    a. Regularly evaluate and determine which tools for document collaboration meet the technical and security standards established by the interagency board and present those tools for best-in-class determination.
    b. Determine configuration settings for best-in-class collaboration suites and document collaboration tools to allow for interagency document collaboration.
2. GSA TTS should ensure there continues to be a document collaboration functionality within Max.gov

[22] Step by step instructions to enable guest access are available in Appendix C: Enabling Calendar Sharing and Guest Access for Collaboration

Overall Recommendations for Improving Interagency Collaboration

Agencies already have many of the tools and technology necessary to collaborate with each other and create a more interoperable government. However, outdated or agency-specific policies, restrictive configuration settings, and non-interoperability between various tools have prevented them from being used to collaborate with other agencies. The federal government also lacks a cohesive strategy to sustain continued virtual interagency collaboration. As productivity tools continue to add and promote collaboration features, the federal government needs a government-wide strategy to acquire tools for interagency collaboration.

Below are the short-term recommendations and long-term recommendations to improve interagency collaboration and make for a more interoperable government. The short term recommendations focus on what can be accomplished within the next 6 months while the long term recommendations focus on future state (e.g., 2+ years out). The federal government also needs to establish a long-term strategy for interagency collaboration and ensure government-wide coordination and policies. The long-term recommendations address the need for a continued and centralized focus on interagency collaboration so agencies can adopt new collaboration tools and use them to work with each other. Several of the short-term and long-term recommendations are in progress now, but will need monitoring to ensure full implementation.

Interagency Collaboration Recommendations - Short Term

1. Accelerate interagency collaboration for Microsoft 365 Teams federation pilot:
    a. OMB and the CIO Council should expand the current Microsoft 365 Teams federation pilot by
        i. Increasing the number of participating agencies
        ii. Replacing MOU requirements with government-wide registry agreement
    b. GSA and the CIO Council should conduct a similar pilot for Google Workspace environments. Google Workspace federation pilot should explore:
        i. Google Workspace to Microsoft 365 integration and calendar interoperability.
        ii. Google Workspace to Google Workspace integration and calendar interoperability.
        iii. Additional third party options as needed.
2. Agencies shall configure collaboration suites to allow guest access[23] for collaboration with guests from other agencies, to the extent practicable. Similarly, agencies shall allow their employees to use guest accounts to access the host agency's collaboration suite for collaboration.

[23] See Appendix C: Enabling Calendar Sharing and Guest Access for Collaboration for details.

   a. Agencies shall establish access controls to ensure that guests only have access to files, documents, and calendars when granted.
   b. Agencies should provide guidance to employees about when and how to provide guest access to other federal employees and federal contractors in a secure manner.
   c. Agencies should provide guidance to employees about when and how to participate as a guest when collaborating with another agency and any responsibilities they have (e.g., records retention).
      i. Including which FedRAMP-authorized product(s) are authorized for use within the agency.
      ii. Agencies should allow employees to receive files from other agencies when shared through FedRAMP-authorized tools.
   d. Agencies should use sensitivity labels to classify and protect documents, limit access to files and internal sites, and other collaborative spaces.
3. All agencies should whitelist web client versions of FedRAMP-authorized collaboration tools that require no account creation.[24]
4. Agencies should configure their systems to allow person-to-person sharing of calendar[25] (free/busy) across agencies, to the extent practicable.
   a. Agencies should provide guidance on permissions and access controls around syncing, sharing, and integrating calendars at different visibility levels.

5. NARA should update the 2009-02 Bulletin, conduct a formal assessment, and issue new guidance as needed for virtual meetings and document collaboration in multi-agency environments. Guidance should consider:
   a. The same approach to records creation and maintenance should be taken for virtual meetings as for in-person meetings; including the artifacts created for records purposes as a result of a meeting, whether in-person or virtual.
   b. Video conferencing chats should not be considered by default a record.
   c. Other virtual meeting participation features, such as polls, whiteboard, reactions or hands-up features, should be treated the same as in-person conversations and not be considered by default a record.
   d. Recording of a virtual meeting does not necessarily make it a record.
   e. The approach to record management of interagency document collaboration requires reciprocation agreements to ensure clarity on records management responsibilities.
   f. Capstone officials may be involved in the creation of records when using interagency collaboration tools. Capstone official participation in the use of interagency tools should not change how records are created, but how they are maintained.
   g. Records created in an unapproved tool must still be saved.

[24] See Appendix B: FedRAMP-Authorized Collaboration Tools for details.
[25] See Appendix C: Enabling Calendar Sharing and Guest Access for Collaboration for details.

6. FedRAMP PMO shall update the Security Controls Baseline to include SCRA controls consistent with up-to-date NIST standards and annual appropriations legislation
    a. This includes meeting the standards for SCRA of the Departments of Commerce and Justice, the National Aeronautics and Space Administration, and the National Science Foundation, like the requirement to consult with the FBI.

Interagency Collaboration Recommendations - Long Term

1. MAX.gov should include government-wide capabilities for:
    a. Federal Communities - including file sharing and document collaboration capabilities.
    b. Calendar - including free/busy and scheduling capabilities. [26]
2. Establish a PMO at GSA to have a centralized and managed office that can standardize technology adoption for interagency collaboration, ensure an aligned strategy across the government, and provide a learning environment for sustained long-term interagency collaboration.

Establishing a PMO for Interagency Collaboration

There is currently no established program tasked with enabling interagency collaboration capabilities; including 1) identifying secure, compatible and best-in-class collaboration solutions; 2) assisting in agency procurements, and; 3) defining technical and/or security standards, facilitating configuration, policy, and other functions. As a result of the pilot, OMB and GSA collectively recommend establishing a PMO at GSA. This will enable long-term planning and execution towards a more interoperable federal government.

Program Governance

The PMO should establish a governance model to ensure that the federal government has a strategic and unified approach for interagency collaboration capabilities. In collaboration with the CIO Council, a Steering Committee should be established that includes representative CIOs and other key stakeholders (e.g., CISO Council, FedRAMP JAB, NIST, CISA at the Department of Homeland Security, DoD). In addition to providing a long-term strategy for the PMO, the Steering Committee will define and regularly update the requirements to meet the federal government's needs for cross-government collaboration. The Steering Committee will also regularly evaluate collaboration capabilities and platforms as presented by the PMO and determine whether they meet the standards to be designated as best-in-class tools for interagency collaboration.[27]

[26] Recommendation to create a new tool to broker calendar free / busy data facilitating native calendar sharing and scheduling between agencies and view the public availability of others. See Appendix M: In-House Scheduling Solution for MAX.gov for details.

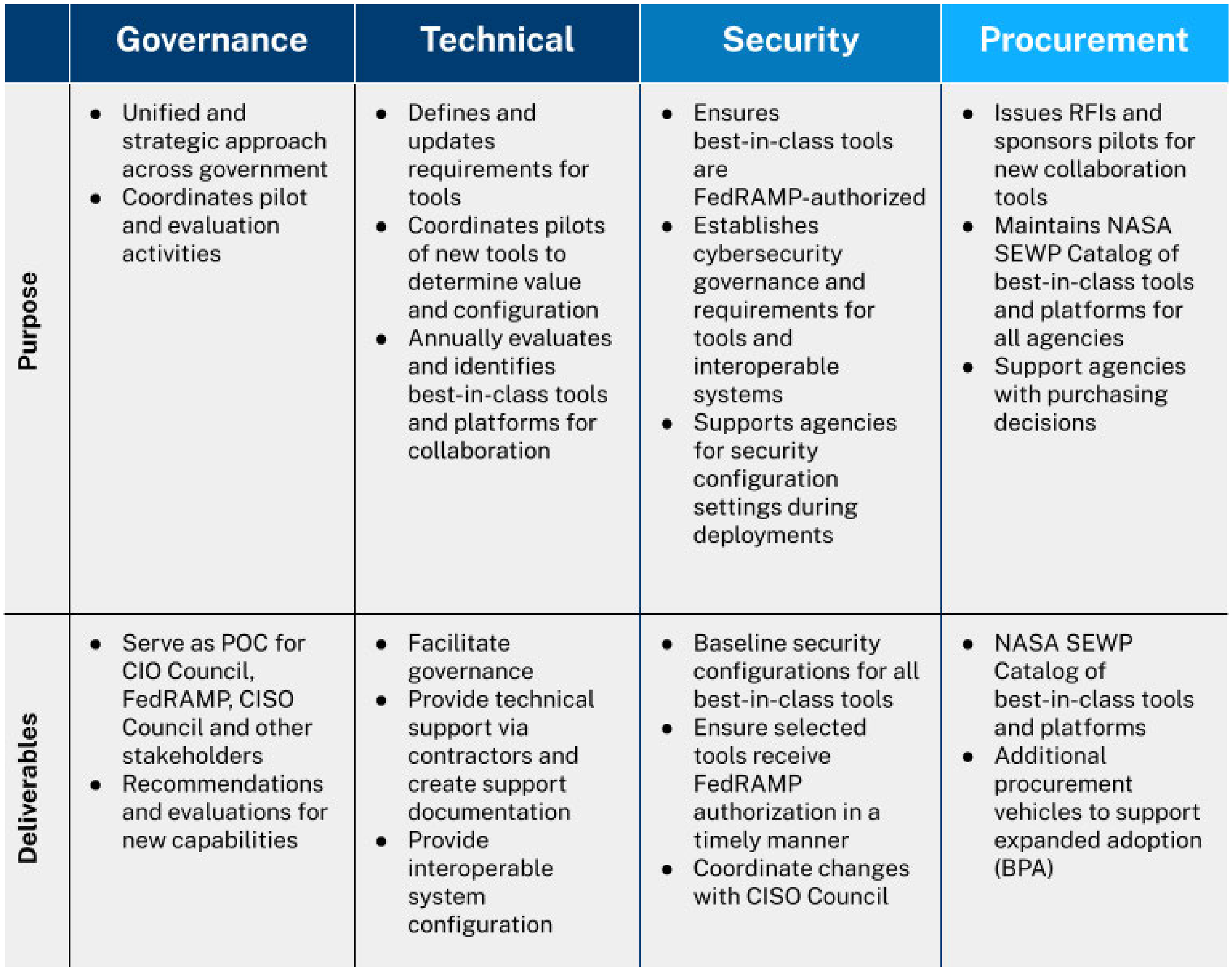
[27] Collaboration areas include email, collaboration suites, calendar sharing, video conferencing, large file sharing, document collaboration, and text-based-chat.

Program Management

The PMO, consisting of three full-time equivalents, is charged with standardizing the adoption of technologies for interagency collaboration. The PMO will support the interagency board and run day-to-day office operations. The PMO will be responsible for establishing a process to identify and evaluate tools that can be used for interagency collaboration. The process shall address the technical, security, and procurement needs for agencies to adopt tools for interagency collaboration.

Below are the four work streams, Governance, Technical, Security, and Procurement, and the deliverables the PMO will be charged with achieving:

Table 2: Interagency Collaboration PMO Workstreams



	Governance	Technical	Security	Procurement
Purpose	• Unified and strategic approach across government • Coordinates pilot and evaluation activities	• Defines and updates requirements for tools • Coordinates pilots of new tools to determine value and configuration • Annually evaluates and identifies best-in-class tools and platforms for collaboration	• Ensures best-in-class tools are FedRAMP-authorized • Establishes cybersecurity governance and requirements for tools and interoperable systems • Supports agencies for security configuration settings during deployments	• Issues RFIs and sponsors pilots for new collaboration tools • Maintains NASA SEWP Catalog of best-in-class tools and platforms for all agencies • Support agencies with purchasing decisions
Deliverables	• Serve as POC for CIO Council, FedRAMP, CISO Council and other stakeholders • Recommendations and evaluations for new capabilities	• Facilitate governance • Provide technical support via contractors and create support documentation • Provide interoperable system configuration	• Baseline security configurations for all best-in-class tools • Ensure selected tools receive FedRAMP authorization in a timely manner • Coordinate changes with CISO Council	• NASA SEWP Catalog of best-in-class tools and platforms • Additional procurement vehicles to support expanded adoption (BPA)

Responsibilities of the PMO

Within the PMO's first six months, the PMO will work with the CIO Council to establish a Steering Committee, work with all CFO Act agencies and establish Microsoft 365 federation to enable individuals to chat and share calendars across agencies, and establish a process to evaluate collaboration tools and take actions necessary to make sure collaboration tools meet security and technical requirements established by the interagency Steering Committee. The PMO will also work with NARA to finalize guidance and with FedRAMP to finalize SCRA into security control baseline. In addition, the PMO will work with the CISO Council to establish baseline security configurations for interagency collaboration tools. Finally, within its first year, the PMO should establish a storefront through NASA's Solution for Enterprise-Wide Procurement (SEWP) so that agencies can purchase best-in-class collaboration tools that have been preconfigured for interagency collaboration.[28]

The PMO will annually, at a minimum, identify and evaluate solutions for interagency collaboration. As part of the evaluation process, the PMO may take steps, such as issuing necessary requests for information (RFIs) and coordinating pilots to determine their value to the federal government. The pilots should decide on the necessary configuration for interagency collaboration, and ensure that the tools can be used for interagency collaboration. The PMO's evaluation process should also include any steps necessary to ensure that collaboration tools meet the requirements laid out by the Steering Committee and will be able to achieve a FedRAMP authorization. The PMO must identify multiple solutions for each collaboration area to ensure agencies can identify and adopt the appropriate tool to meet their needs; this includes supporting agencies in procurement actions via NASA SEWP and other procurement vehicles.

Several actions are underway to improve interagency collaboration. The PMO is also responsible for tracking these actions and working with the CIO Council to ensure they are implemented. The PMO should ensure that the following items are completed:

- NARA issues updated guidance on video conferencing, document collaboration and use of other collaboration tools in a multi-agency environment (expected Nov 2021).
- FedRAMP PMO incorporates supply chain risk assessment (SCRA) requirements into the security controls baseline (expected Dec 2021).
- All agencies will whitelist web client versions of FedRAMP-authorized collaboration tools which require no account creation and collaboration suites (tracking via IDC).
- All agencies will create guest access procedures (tracking via IDC).
- Google Workspace to Microsoft Teams calendar integration pilot between GSA and SBA (expected early 2022).

[28] GSA Emerging Technologies division believes NASA SEWP is the appropriate place to establish an initial contract vehicle for interagency collaboration tools because of the relative ease and speed in which the PMO would be able to set up a storefront and agencies can purchase best-in-class tools from it. The PMO will also be able to identify additional procurement vehicles as needed to support extended adoption of interagency collaboration tools.

- Microsoft 365 Federation scales to additional agencies (ongoing; target completion chat & calendar FY22 Q2).

Appendix A: Slack in the United Kingdom Case Study

Several Federal agencies use Slack for internal communications. In fact, according to the FedRAMP Marketplace, 40 agencies report to be using the service. If agencies want to collaborate on Slack, each agency must acquire its own licenses for the service before using a Slack service called Slack Connect to invite external partners to work with. This is a haphazard approach that does not leverage the federal government's buying power to negotiate for better pricing, nor is it a unified approach that enables any agency to chat with another using Slack.

The federal government should consider the United Kingdom's use of Slack as an example of a governmentwide chat solution. In contrast to how U.S. Federal agencies approach collaboration tools, specifically for chat, the United Kingdom uses Slack as the chat tool for the central government and allows anyone working in the central government to create a Slack account to chat with others in government. There are also channels for different departments and channels on a range of topics.

Although the government uses Microsoft Office 365 for their individual departmental needs, the whole government has access to Slack to support government wide communication. With the adoption of Slack, the UK government has reduced the email burden dramatically, fostered a community across five million public workers, and enabled multiple teams across the government to come together from different backgrounds and enhance policies. Slack does more than enable communication though, the platform also provides a place for meetings, channels for focus areas, and document collaboration, especially when members have different systems. The UK cross-government slack supports approximately 2,000 active users a week and 400 channels varying from cybersecurity to service design. Any government member with a "gov.uk" is able to join.[29]

Appendix B: FedRAMP-Authorized Collaboration Tools

To increase interagency collaboration, all agencies should whitelist collaboration tools that: 1) are FedRAMP-authorized, 2) do not require an account for guest access, and 3) are accessible on a web browser (i.e., no downloads required). The following is a list of the current collaboration tools that meet these requirements:

- □ **Adobe Connect** (Video Conferencing)
  Guest access allows: video conference*
  FedRAMP* Moderate *Authorization by: *Joint Authorization Board (JAB)*

- □ **Adobe Document Cloud** (File Sharing)
  Guest access allows: download files, comment on PDFs, fill and eSign PDFs
  FedRAMP Li-SaaS Authorization by: *United States Agency for Global Media*

[29] https://apolitical.co/en/solution_article/goodbye-email-hello-slack-how-chat-is-taking-over-government

- □ **Amazon Chime (**Video Conferencing)
  Guest access allows: video conference*
  FedRAMP* Moderate *Authorization by: *JAB only for the AWS US East/West Regions (not GovCloud)*

- □ **Amazon WorkDocs (**File Sharing)
  Guest access allows: view-only for documents
  FedRAMP* Moderate *Authorization by: *JAB*

- □ **Google Workspace** (File Sharing, Document Collaboration)
  Guest access allows:** downloading/uploading/preview files in Google Drive, editing/commenting in Google, Docs, Sheets, Slides, Drawings, Forms; no pin sharing required to fill out and submit Google Forms
  FedRAMP Moderate Authorization by: *General Services Administration for Google Workspace (FedRAMP high authorization in progress by JAB)*

- □ **Google Meet** (Video Conferencing)
  Guest access allows: video conference*
  FedRAMP Moderate Authorization by: *See above for Google Workspace*

- □ **Microsoft 365** (File Sharing, Document Collaboration)
  Guest access allows:** downloading/uploading files in OneDrive, editing and commenting in O365 tools: Microsoft Word, Excel, and PowerPoint
  FedRAMP Moderate Authorization by: *Department of Health and Human Services for Office 365 Multi-Tenant & Supporting Services also known as Microsoft GCC (FedRAMP high authorization for Microsoft GCC High in progress by DOJ)*

- □ **Microsoft Teams** (Video Conferencing)
  Guest access allows: video conference*, download files (only during video conference)
  FedRAMP Moderate Authorization by: *See above for Microsoft 365*

- □ **Webex for Government** (Video Conferencing)
  Guest access allows: video conference*
  FedRAMP Moderate Authorization by: *Department of Health and Human Services*

- □ **ZoomGov** (Video Conferencing)
  Guest access allows: video conference*
  FedRAMP Moderate Authorization by: *Department of Homeland Security*

* Video conference includes the standard features of screen sharing, text chat, link sharing, and view participants. Additional tool-specific features may be available.

** Guests may require a verification or pin code in addition to a link to access without an account.

Appendix C: Enabling Calendar Sharing and Guest Access for Collaboration

To increase interagency collaboration, all agencies should whitelist all FedRAMP-authorized collaboration suites, enable external calendar sharing, and configure their collaboration suite to enable access for guest users for the purposes of cross-agency collaboration. Below are a list of FedRAMP-authorized collaboration suites and the levels of guest access that can be granted in each collaboration suite, instructions for enabling calendar sharing using the natively supported iCalendar format, and instructions for enabling access for guest users

Google Workspace - *FedRAMP Moderate Authorization by General Services Administration for Google Workspace (FedRAMP high authorization in progress by JAB).* Google Workspace users can collaborate with both Google and non-Google guests. Verification for non-Google guests is via PIN. Admins can enable these features for the organization.

- **Google Drive, Google Docs, Google Sheets, and Google Slides:** Google Workspace users can share files, folders, docs, sheets, and slides with both Google and non-Google guests. Google Workspace users can give temporary access by setting an expiration date/time and revoke access by removing users from a group of shared users. Admins can revoke access for any guest at any time from admin control.

- **Google Meet:** Google Workspace users can schedule and host meetings with both Google and non-Google guests. Google Workspace users can mute and remove attendees from meetings. Both Google and non-Google guests can participate in video meetings, mute/unmute microphone, start/stop camera, view closed captioning, raise hand, screen sharing, chat, view attendees, participate on whiteboard, participate in question and answer feature, participate in polling, and participate in breakout rooms.

- **Google Chat:** Google Workspace users can invite Google guests to their Chat and Rooms. Non-Google guests are not able to participate in Chat or Rooms.

Microsoft Office 365 - *FedRAMP Moderate Authorization by Department of Health and Human Services for Office 365 Multi-Tenant & Supporting Services, also known as Microsoft GCC, (FedRAMP high authorization for Microsoft GCC High in progress by DOJ).* Microsoft Teams users can collaborate with both federated Microsoft Teams[30] and non-Microsoft Teams' guests. Verification for non-Microsoft Teams guests is via passcode. Admins can enable these features for the organization.

- **Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft SharePoint, Microsoft OneDrive:** Microsoft Teams users can share files, folders, word documents, excel spreadsheets, and powerpoints with both[31] federated Microsoft

[30] Federated Microsoft Teams guests are external users belonging to another organization and have specific access (i.e., federated) to your organization's resources.

[31] Federated Microsoft Teams Users (i.e, external users") cannot share files through teams chat however a link to the file can be shared.

Teams and non-Microsoft Teams guests. Microsoft Teams users can revoke access to guests at any time.

- **Microsoft Teams:**[32] Microsoft Teams users can invite federate Microsoft Teams guests to video conferences, Teams chats, and Channels. Microsoft Teams users can invite non-Microsoft Teams guests[33] to video conferences. Once the meeting is over, non -Microsoft Teams guests will not have access to the chat. Microsoft Teams users are able to mute and remove any attendee in a video conference, Teams chat, and Channel.

Configuration Guide for External Calendar Sharing

Agencies should allow their employees to share their calendar availability with employees at other federal agencies. The ability to view others' availability allows users to easily find times when meeting participants are available and schedule meetings. This is a more efficient process than exchanging emails between participants to find a time when everyone is available to meet.

Calendar Sharing settings are controlled at both the service and client level. Below are the configuration recommendations for each:

Configure Sharing Settings on Service or Server

To enable mailbox users to share their calendars externally, system administrators will need to do the following:

- **For Google Workspace -** set the "External Sharing" configuration to "*Only free/busy information (hide event details)*".
- **For Microsoft Exchange Online** -set the "External Sharing" configuration settings within the Microsoft 365 portal to "*Let your users share their calendars with people outside of your organization who have Office 365 or Exchange*", "*Allow anyone to access calendars with an email invitation*", and "*Show calendar free/busy information with time only*"[34]

Configure Sharing Settings on Mail Client

Once sharing settings on the service or server are configured, users will be able to share personal calendars with individuals outside their organization by doing the following:

- **For Google Workspace -** go to the calendar's "Settings" navigate to the calendar you want to share and under "Access permissions for events" select "*Make available to public*" and be sure to choose the "*See only free/busy (hide details)*" option.

[32] MS Teams is a chat *and* video conferencing tool. Chat conversations resulting from video conferences are preserved for the host agency after the video conference concludes. Features are available but may differ by user as policies are applied.

[33] Non-Microsoft Teams guests can also be invited to a meeting via a unique link creating the "anonymous user" concept in Teams meetings.

[34] These are highly encouraged, optional settings for sharing basic calendar free/busy information with external users

- **For Microsoft Outlook Web Access -** go to the calendar you want to share and select "Sharing and Permissions" from the ellipsis, then add the email address of the individuals outside your organization with whom you'd like to share your calendar. Be sure to verify "Can view when I'm busy" is populated in the drop-down before clicking "Share."

Configuration Guide for Guest Access

Both Google and Microsoft platforms support traditional user based authentication, PIN authentication, or passcode based authentication. Additionally, both Google Workspace and Microsoft 365 allow administrators to configure each respective collaboration suite to enable file sharing across public links, but due to security concerns, agencies are not recommended to allow public sharing of documents. (Details of public link configuration settings are not detailed here.)

- **User:** Depending on the configuration, this method requires an administrator or user to possess or create an account specific to the collaboration suite prior to the guest user accessing the shared document.
- **PIN or Passcode:** This method requires a user to confirm their identity after receipt of the email invitation to share a document. By clicking on the invite link, the guest user initiates the sign-in process. An email is sent to confirm the identity of the user; upon receipt of the confirmation email, a pin is acquired for use to access the shared document.

Configuration Guide for Google Workspace

The "Google Workspace Settings" walk through process below explains how to configure Google Workspaces for guest user access. In this case, the organization is called "Global Demo." For the purposes of this configuration, guest users are any users who do not have an identity credential within the "Global Demo" tenant. Guest users include the following users.

- GSA Affiliated Customer Account (GACA)
- Personal Google Accounts
- Pin Based (OTP) Accounts
- Anonymous User Accounts

Google Workspace Settings

1. Validate that "Sharing outside of tenant" is set to "**ON - Files owned by users in tenant can be shared outside of tenant. This applies to files in all shared drives as well.**"
    a. This setting enables users of the tenant example of "tenant" to share files with other users who aren't part of the same tenant.
    b. This is a required setting for sharing files outside of the tenant.
2. Validate that "**For files owned by users in the tenant warn when sharing outside of the tenant**" is checked.

   a. This setting enables a warning message to users of the tenant example of “tenant” they are about to share a file with users outside of their tenant.
   b. This is an optional, best practice setting for sharing files outside of the tenant.
3. Validate that "**Allow users in the tenant to send invitations to non-Google accounts outside the tenant**" is checked.
   a. This setting enables users of the tenant example of “tenant” to share files with other users even if they don’t have a Google Account. This is commonly referred to as pin based sharing. The default authentication time is seven days.
   b. This is an optional setting, only required to support sharing with users without Google accounts.
4. Validate that calendar sharing settings are configured to allow external sharing[35].
   a. Click “**Sharing Settings**”
   b. In the “**External Sharing options for primary calendars**” ensure “**Only free/busy information (hide event details)**” is selected.

Configuration Guide for Microsoft 365 Teams

Turning on guest access depends on the configuration of settings within Azure Active Directory, Microsoft 365, SharePoint, and Teams.

Azure Active Directory Admin Center

The “External Collaboration Settings” below explain the process to configure Azure Active Directory for guest user access, guest invite settings, and collaboration restrictions.

The “OTP Identity Provider Configuration” explains how to configure the supported identity providers for use in providing guest access for collaboration.

For the purposes of this configuration, guest users are any users who do not have an identity credential within the “Global Demo” tenant. Guest users include the following users.

- Personal Microsoft Accounts
- Pin Based (OTP) Accounts
- Anonymous User Accounts

External Collaboration Settings

1. Validate that "**guest users have limited access to properties and memberships of directory objects**" is selected.

[35] These are highly encouraged, optional settings for sharing basic calendar free/busy information with external users

   a. This setting blocks guests from enumeration of Azure Active Directory (AAD) users, groups, or other directory resources. Guests can see membership of all non-hidden groups.
   b. This is the default setting, organizational policies may require a more restrictive setting.
2. Validate that "**Anyone in the organization can invite guest users including guests and non-admins (most-inclusive)**" is selected.
   a. This setting allows users and administrators to invite guest users to the organization.
3. Validate that "**Enable guest self-service sign up via user flows**" is set to "**No.**"
   a. This setting enables guest users to participate in user flows allowing users to sign up for organizationally defined apps.
   b. This setting is optional and used as security best practice. Set it to "No," unless needed.
4. Validate that "**Allow invitations to be sent to any domain (most inclusive)**" is enabled.
   a. This setting is used to specify allowed or denied domain lists.

Configure One-Time Passcode Identity Provider

1. Click on "**Email one-time passcode.**"
   a. Clicking on this text opens the "Configure identity provider" blade.
2. Validate that "**Email one-time passcode**" is enabled.
   a. At time of documentation creation, there are two choices for "enabled." Any choice other than "Disabled" is required.

NOTE: There will be two options, enable or disable, once this functionality is out of preview.

Microsoft Admin Center

The "Microsoft Admin Center Org Settings" below demonstrates how to configure organization-wide settings for sharing. These settings let users within the organization add new users to the organization for guest sharing

Configure Organization Sharing Settings

1. Click on "**Settings.**"
   a. This will expand the sub menu to reveal the Org Settings selection.
2. Click on "**Org Settings.**"
   a. This will populate the Org Settings window with three tabs.
3. Click on the "**Security & Privacy**" tab within the window.
   a. This will populate the Security & Privacy list
4. Click on "**Sharing.**"

   a. This will open the Sharing Blade to the right
5. Validate “**Let users add new guests to the organization**” is checked.
   a. This allows users to add guests to the organization for guest-sharing.

SharePoint (and OneDrive) Admin Center

The “SharePoint External Sharing Settings” explains how to configure External Sharing policies for SharePoint and OneDrive. In addition to the guest-user configurations in Azure, an organization must specify the sharing levels of both SharePoint and OneDrive.

Configure External Sharing Policies

1. Click “**Sharing.**”
   a. This will populate the Sharing Screen, allowing you to set the sharing levels for SharePoint and OneDrive external users.
2. Change SharePoint and OneDrive slider settings to align with “**New and existing guests.**”
3. Validate “**People who use a verification code must reauthenticate after this many days**” is checked.
   NOTE: The default value is 30 days. Your organization may wish to increase or decrease the value

---

Teams Admin Center

The “Teams Organization Wide Settings” explains how to configure settings for Microsoft Teams to support guest user access.

Configure Org Wide Settings

1. Click “Org wide settings.”
   a. This will expand the sub-menu, revealing “external access.”
2. Click “External Access”
   a. This will populate the External Access screen.
3. Validate that "Users can communicate with Skype for business and Teams users" has been enabled.
   a. This is the default setting, if this setting is turned off, users can still join meetings anonymously unless prohibited by policy.
4. Validate that "Users can communicate with Skype Users" is enabled.
   a. This will allow users to search for and start a one-on-one text conversation or video call with Skype users.

Exchange Admin Center

The "Exchange Admin Center Settings" explains how to configure settings for sharing Microsoft Exchange to support external sharing of user calendars[36].

Configure Organization Sharing Policy

1. In the Exchange Admin Center click "Organization" and then "Sharing"
    a. This will load the "Sharing" page.
2. Click the "+" symbol under Organization Sharing
    a. This will pop up the "New Organization Relationship Screen" screen.
3. Define the following fields
    a. Relationship name - (e.g name of Domain to share with)
    b. Domain to share with - (e.g gsa.gov)
4. Validate that "Enable calendar free/busy information sharing" has been checked and that
    a. "Calendar free/busy information with time only" has been selected
    b. "Everyone in your organization" has been selected

Appendix D: In-House Scheduling Solution for MAX.gov

Background

Both Microsoft and Google calendars support the ***iCal format***, which is short for ***iCalendar*** i.e. *the format is defined in terms of a Multipurpose Internet Mail Extension (MIME) content type, through the object properties, alternative transport protocols are possible.* ***iCal*** is an open standard for exchanging calendar and scheduling information between users and computers. Microsoft and Google users can exchange calendar and scheduling information by subscribing to ***iCals*** using a Uniform Resource Locator (URL). The unique URLs are stored in Google and Microsoft calendars and are requested by calendar clients to exchange calendaring information.

Any changes made to calendars are shared with subscribed calendars. The frequency of request/exchange of scheduling information depends entirely upon the calendar client. Below are the historical request/exchange frequency of Microsoft and Google.

- Google normally updates every 18-24 hours
- Outlook updates upon app / program startup & every 1-3 hours
- Outlook.com updates every 3 hours

Challenge

The government utilizes Microsoft and Google calendars and requires real time availability of free/busy data between calendar solutions. During testing, subscribed calendars did not reflect changes made by others immediately. Instant syncing is an option if enabled and only if users are in the same Microsoft or Google tenant.

[36] These are highly encouraged, optional settings for sharing basic calendar free/busy information with federated domains.

Google provides native calendar interoperability however the integration relies upon a highly trusted account within Microsoft exchange to leverage the deprecated EWS api. Fundamental security practices such as following the principle of least privilege are sacrificed to attain this interoperability.

Solution

Creation of a Cross Agency Scheduling application based on a free / busy microservice.

The solution is a hub and spoke design. The hub shall broker (or proxy) API calls to other calendar systems from any member agency user API call. These calls may originate from a server based web application, browser or application plugin.

The ideal implementation of this design will be on a serverless architecture of choice provided by a cloud based platform such as Azure or AWS.

Components

Hub:

A central microservice consuming REST free / busy calendar service data. The hub will not store data, instead it will rely upon other services for just in time access to data. Any credentials required for access to REST services will be stored within a Password Vault (e.g Azure Key Vault or AWS Secrets Manager)

Order of operations

1. Free / Busy Lookup source is determined by return of MX query of user(s) FQDN from DNS
2. Service Account (Credential) Lookup matches MX query to record, returning credentials
3. Service Query (eg Microsoft, Google, or Exchange) connects to calendar service REST endpoint, returning free/busy information
    a. Service Query will be derived from Python Calendar-Interop-Relay[37]

Spoke:

The spokes are the user interface and are responsible for making the authenticated request to the hub.

Order of operations

1. User is Authenticated with user IdP
2. Hub provides authorization based on authentication of known domain suffix (all users)

[37] https://github.com/rallyhealth/calendar-interop-relay

3. Hub begins order of operations

The user interfaces may consist of one or more of the following

1. Native Interface - Ideal for Google and Microsoft Users
2. Custom Web Application - Ideal for any custom application (e.g Max.gov Calendaring)