NATIONAL ARCHIVES | Office *of the* Chief Records Officer

ELECTRONIC MESSAGING COMPLIANCE ASSESSMENT TOOLKIT

Purpose

Agencies generally have a business need to provide electronic messaging applications for employees, contractors, volunteers, and external experts to communicate quickly and efficiently across organizational boundaries. Messaging applications may provide enhanced security features, a way to communicate in real-time during official travel, and a forum for inter-agency communications.

Any electronic messaging communication tool used by an agency must meet federal requirements in the following areas:

- **Records management:** Electronic messages created in the course of agency business are federal records and must be captured and managed following a National Archives and Records Administration (NARA)-approved records schedule.
- **Security:** The use of electronic messaging applications must comply with federal security requirements, such as the National Institute of Standards and Technology (NIST) 800-53 and the Federal Information Security Modernization Act (FISMA).
- **Technical:** Agencies must have the appropriate Information Technology (IT) assets and infrastructure to support the appropriate use of electronic messaging applications and manage records.
- **Legal:** Agencies must be able to comply with various legal requirements, including the Freedom of Information Act (FOIA) and e-discovery, when using electronic messaging applications.

Audience

This toolkit is for agency stakeholders who make decisions about the procurement, use, management, and maintenance of electronic messaging applications, tools, or systems. This toolkit provides a list of potential stakeholders and their suggested responsibilities. For the purposes of this document, we refer to all electronic messaging tools, services, and systems collectively as “applications.” These applications include, but are not limited to, chat services, mobile device messaging services, and messaging services on third-party applications, such as Signal, WhatsApp, Telegram, WeChat, and Snapchat.

Background

New electronic messaging applications are frequently being developed. Agencies balance federal requirements with the needs of employees to conduct agency business efficiently and effectively. Prohibiting the use of electronic messaging to conduct agency business is difficult to enforce and does not address the needs of both business and employees. Agencies should encourage the use of approved electronic messaging applications on government-issued devices. By installing vetted applications on government-issued devices, agencies reduce risk and gain greater control over their electronic records.

There are automated and manual approaches to electronic message capture. Each approach has advantages and challenges from a federal records management perspective. Agencies may purchase third-party tools that automatically capture and preserve electronic messages. This removes the responsibility from the end user for capture and ensures the agency has complete and reliable copies of electronic messages. Without automated capture tools, agencies will need to rely on employees to capture electronic messages in a recordkeeping system. Note: electronic messages not automatically captured must be forwarded to an official account within 20 days, as required by the FRA (44 U.S.C. § 2911).

Training employees on their responsibilities and providing vetted applications for records capturing are recommended. Some electronic messaging applications offer features that enable automated capture and forward of messages to an electronic recordkeeping system. Other applications do not offer such features, instead requiring employees to manually identify, and forward each message, which may involve capturing a screenshot when forwarding is not possible.

Although there is no “one size fits all” solution for agencies to implement policies, processes, and procedures related to the use of electronic messaging, NARA recommends agencies adopt an agency-wide approach when researching, procuring, implementing, and managing electronic messaging applications. Records management programs should collaborate with their legal, information technology, and other relevant stakeholders on all aspects of electronic messaging use.

Agencies should establish a thorough vetting process for third-party applications, such as WhatsApp, Snapchat, Signal, and other messaging applications. This process should assess the application’s security features, data storage practices, records capture capabilities, and compliance with applicable statutes and regulations. This toolkit can assist agencies in the vetting process. It identifies stakeholders to include when evaluating and selecting electronic messaging applications. It also provides considerations and questions for agencies to review during the decision-making process. For agencies that have already implemented an electronic messaging application, this tool can be used to assess their current compliance risks and develop suitable approaches to mitigate those risks.

This toolkit includes the following sections:

- Stakeholder List
- Considerations and Questions for the following areas of interest:
    - General Business Needs and Requirements
    - Records Management
    - Agency Policy / End–User Responsibilities
    - Technical Capabilities and Requirements
    - Additional Legal Concerns and Risks
    - Classified Records and Access Restrictions

General Best Practices

Below is a list of best practices agencies can use to guide an application review and implementation.

- Select an application that allows the agency to determine and administer user controls.
- Consider available products or services that provide automated capture and retention of electronic messaging records. If the selected application does not have automated capture, agencies must develop policies and training for end users on how to capture and forward images to a recordkeeping system.
- Review existing enterprise information technology assets/applications to determine if a suitable tool already exists to meet the business need. For example, using Microsoft Teams on mobile devices for intra- and inter-agency communication.
- Create and follow a formal vetting process to review and approve the use of third-party applications, such as WhatsApp, Snapchat, Signal, etc.
- Adopt, disseminate, enforce, and update policies documenting which tools are available, how they may be obtained, and which tools or tool functions are disallowed.
- Require users to agree to the Rules of Behavior for mobile government-furnished equipment when the device is first issued. Users should review and accept the Rules of Behavior on an annual basis.
- Train employees and contractors on the agency's electronic messaging requirements. Help employees understand what constitutes a federal record, the agency's process for capturing and managing electronic messaging records, and reporting unauthorized dispositions.
- When possible, block the download of disallowed messaging applications on agency-owned devices.
- Use Mobile Device Management (MDM) to manage applications and mobile devices.
- Include the Agency Records Officer or appropriate records management staff in all stages of selection, deployment and decommissioning.

Records Management Best Practices

Below are best practices for compliance with records management requirements for electronic messaging applications.

- Use a third-party application to automate the capture of electronic messages at the carrier level.

- Ensure permanent electronic messaging records are captured and maintained in an official recordkeeping system.
- Determine if temporary electronic messaging records can be maintained in the electronic messaging application for the duration of their retention period.
- Include processes to identify and exclude personal and non-record messages from official records capture.
- Turn off disappearing messages if an agency does not use a third-party application to ensure automatic capture of messages.

Stakeholder List

Below is a list of stakeholders and their general responsibilities. Agencies may use this list to identify agency stakeholders who should be involved in discussions and decisions related to the use of communication applications.

NOTE: This list uses titles common to most federal agencies. Your agency may use different terminology or titles for these positions, and they can be applied accordingly. This is not an exhaustive list. Your agency may identify other stakeholders that should be included in your discussions.

STAKEHOLDER	GENERAL RESPONSIBILITIES
Senior Agency Official for Records Management (SAORM)	The SAORM can assist with obtaining leadership buy-in, resource allocation, and overall stakeholder coordination.
Agency Records Officer (ARO)	Your ARO is responsible for overarching agency-wide records management policies, procedures, training, and implementation. They are also usually the primary point-of-contact between the agency and NARA.
Departmental Records Office (DRO)	Many cabinet-level agencies have a centralized DRO, who may set department-wide policy for all components (agencies/operatives) within the department.
Chief Information Officer (CIO)	Your CIO (or equivalent) can speak to the technical requirements of messaging application, tool, or system implementation and functionality.
System Administrator/Vendor(s)	Similar to the CIO, system administrators or vendors can help ensure that an application, tool, or system can be properly identified and implemented.
Security Officer/Information Security Officer	Your agency's security officer can coordinate with other federal agencies about cyber-security and whether specific applications, tools, or systems meet federal security requirements.

STAKEHOLDER	GENERAL RESPONSIBILITIES
General Counsel (GC)	Your agency's General Counsel should be involved in all legal aspects of messaging application, tool, or system use and implementation. They can help mitigate risks associated with the use of certain applications, tools, or systems.
Procurement Officer	Your agency's procurement officer can help explore purchasing opportunities and finalize contracts.

Considerations And Questions

If your agency is considering a specific application for electronic messaging, NARA recommends that your agency discuss these considerations and questions with your stakeholder group. A higher frequency of 'no' or 'unsure' responses to these questions indicates greater risk associated with the agency's use of the messaging application.

The checklists below are designed to be used for each application your agency is considering for communication.

NAME OF APPLICATION UNDER CONSIDERATION:

BUSINESS FUNCTION IT SUPPORTS / GENERAL SCOPE:

OTHER NOTES:

General Business Needs and Requirements

CONSIDERATION / QUESTION	STAKEHOLDER(S) INVOLVED	RESPONSE
Has your agency determined a business need for the communication application under consideration?	ALL	● YES ● NO ● UNSURE
Have you determined who will be using the tool?	ALL	● YES ● NO ● UNSURE
Has your agency determined that use of the specific application under review is necessary and appropriate to meet the identified business need?	ALL	● YES ● NO ● UNSURE
Has your agency reviewed the specific application for compliance with all federal requirements? (Note: the checklists to follow will also help answer this question)	ALL	● YES ● NO ● UNSURE
Are there existing enterprise applications that can be used or modified to meet the identified business need?	ALL	● YES ● NO ● UNSURE

Records Management

CONSIDERATION / QUESTION	STAKEHOLDER(S) INVOLVED	RESPONSE
Can the application create, manage, and properly dispose of records in accordance with the Federal Records Act (FRA), 36 CFR 1222, 1224, 1236, and the appropriate records disposition schedule(s)?	ALL, led by the Agency Records Officer (ARO)	● YES ● NO ● UNSURE
Have you determined which NARA-approved records schedule(s) would apply to records created in the application? For example, this may be an agency-specific records schedule, the GRS 6.1 (Capstone), or multiple records schedules.	ALL, led by the Agency Records Officer (ARO)	● YES ● NO ● UNSURE
Can you separate temporary and permanent records created in the application, and manage them accordingly? For example, can you ensure that the messages of senior (Capstone) officials are captured as permanent records?	ALL, led by the Agency Records Officer (ARO)	● YES ● NO ● UNSURE
Does your agency have a plan to protect the records if the provider shuts down or retires the application?	ALL, led by the Agency Records Officer (ARO)	● YES ● NO ● UNSURE
Are all records fully accessible to meet your general business and legal obligations?	ALL, led by the Agency Records Officer (ARO)	● YES ● NO ● UNSURE
Can records created by or in the application be captured in an automated fashion? For example, can records be automatically exported to a recordkeeping system?	Agency Records Officer (ARO), Chief Information Officer (CIO)	● YES ● NO ● UNSURE
If automated capture or export is not available, can the proper management of the records be achieved via manual (human required) processes?	ALL, led by the Agency Records Officer (ARO)	● YES ● NO ● UNSURE
Can all required metadata be created, captured, and maintained in	Agency Records Officer	● YES

CONSIDERATION / QUESTION	STAKEHOLDER(S) INVOLVED	RESPONSE
accordance with 36 CFR 1222.26 and NARA Bulletins 2015-04 and 2025-01?	(ARO), Chief Information Officer (CIO)	● NO ● UNSURE
Can agency administrators disable auto-delete or disappearing functions from the messaging application?	Agency Records Officer (ARO), Chief Information Officer (CIO)	● YES ● NO ● UNSURE

RISK ASSESSMENT: The more your agency answers “no” or “unsure” to the above questions, the greater the risk your agency may be accepting. Possible risks include:

- Failure to create records as required by 36 CFR 1222, thus lacking proper documentation of general business functions.
- Failure to capture and manage records as required by 36 CFR 1222 and 1224 may lead to an unauthorized disposition, pursuant to 36 CFR 1230.
- Inability to respond to Congressional requests, Inspector General inquiries, or Freedom of Information Act (FOIA) requests due to a lack of records access or availability.
- Failing programmatic or financial audits due to the unavailability of records.
- Keeping records longer than legally required increases storage costs and ongoing inclusion in records searches for FOIA and legal discovery when identifying responsive records.
- Loss of historically valuable (permanent) records.

Agency Policy / End-User Responsibilities

CONSIDERATION / QUESTION	STAKEHOLDER(S) INVOLVED	RESPONSE
Is your agency prepared to develop, maintain, update, and enforce agency policies related to the use of the application?	ALL, led by the Agency Records Officer (ARO)	● YES ● NO ● UNSURE
Do agency policies delineate end-user responsibilities when using the communication application under consideration?	ALL, led by the Agency Records Officer (ARO)	● YES ● NO ● UNSURE
Do agency policies address which devices may utilize which applications? (agency-issued devices, bring-your-own devices, mobile devices, desktop computers, etc.).	ALL, led by the Agency Records Officer (ARO)	● YES ● NO ● UNSURE
Do agency policies specify required training on the proper use of the application? For example, training on how to properly capture federal records, especially if manual processes are required.	Agency Records Officer (ARO), Chief Information Officer (CIO)	● YES ● NO ● UNSURE
Do agency policies address whether end-users can cull (remove) certain data or messages (such as non-record or personal records)?	Agency Records Officer (ARO), General Counsel	● YES ● NO ● UNSURE
Do agency policies address <u>who</u> may apply disposition against the messages? For example, is it each end-user, the records management office, or some other entity?	Agency Records Officer (ARO), General Counsel	● YES ● NO ● UNSURE
Does your agency have a policy in place relative to collaborating via electronic messaging with other agencies, including about shared records management responsibilities?"	Agency Records Officer (ARO), General Counsel, Chief Information Officer, System Administrator / Vendor	● YES ● NO ● UNSURE

RISK ASSESSMENT: The more your agency answers “no” or “unsure” to the above questions, the greater risk your agency may be accepting. Possible risks include:

- Inconsistent use of an application throughout the agency, where the agency lacks control of who is using what applications and functions.
- Lack of end users’ understanding of their responsibilities and improper use of an electronic messaging application.
- Circumvention of agency policies on information technology security and information management.
- Loss of access to records that support your agency’s general business needs.
- Unauthorized disposition cases opened by NARA due to failure to manage records to meet the legal records management obligations of the agency (36 CFR 1230).

Technical Capabilities and Requirements

CONSIDERATION / QUESTION	STAKEHOLDER(S) INVOLVED	RESPONSE
Is the application FedRAMP compliant, if applicable?	Chief Information Officer, System Administrator / Vendor, Procurement Officer	● YES ● NO ● UNSURE
Does the agency have adequate controls in place to protect sensitive information transmitted or stored through the application?	Chief Information Officer, System Administrator / Vendor, Security Officer / Information Security Officer, Agency Records Officer (ARO)	● YES ● NO ● UNSURE
Has your agency determined if certain features of the application should be disabled? (such as due to non-compliance with records management requirements)	Chief Information Officer, System Administrator / Vendor	● YES ● NO ● UNSURE
Are data security and privacy risks associated with the application regularly assessed and mitigated?	Chief Information Officer, System Administrator / Vendor, Security Officer / Information Security Officer, Agency Records Officer (ARO)	● YES ● NO ● UNSURE
Can permanent records be exported from the application in formats acceptable to NARA standards?	Chief Information Officer, System Administrator / Vendor, Agency Records Officer (ARO)	● YES ● NO ● UNSURE
Is a Mobile Device Management (MDM) solution available to manage and secure mobile devices using this application for official purposes?	Chief Information Officer, System Administrator / Vendor	● YES ● NO ● UNSURE
Does the MDM solution enforce security policies, restrict app usage and ensure compliance with NARA regulations?	Chief Information Officer, System Administrator /	● YES ● NO

CONSIDERATION / QUESTION	STAKEHOLDER(S) INVOLVED	RESPONSE
	Vendor, Security Officer / Information Security Officer	● UNSURE

Risk Assessment: The more your agency answers “no” or “unsure” to the above questions, the greater the security risk. Not having sufficient security controls in place can increase risk. Possible risks include:

- Exposure to security risks or data breaches due to a lack of restrictions and proper controls on application usage. For example, if security controls are not properly evaluated, applications may put sensitive information at risk for unauthorized access or breaches.
- Lack of oversight on individual user accounts increases exposure to all risks related to records management, security, and legal requirements.
- Loss of permanent records because of the inability to export records in acceptable formats.
- An increase in user errors, data mishandling, or non-compliance with agency policies due to a lack of training and documentation.
- Absence of MDM solutions may leave mobile devices vulnerable to security threats, data breaches, or unauthorized access.

Additional Legal Concerns and Risks

CONSIDERATION / QUESTION	STAKEHOLDER(S) INVOLVED	RESPONSE
Have you reviewed the application for general legal risks?	General Counsel	● YES ● NO ● UNSURE
Are electronic messages text-searchable to meet information requests, such as FOIA?	General Counsel	● YES ● NO ● UNSURE
Can all legal and discovery needs be met with the use of the application?	General Counsel	● YES ● NO ● UNSURE
Does the terms of service agreement with the vendor include applicable records management requirements?	General Counsel, Agency Records Office (ARO), Chief Information Officer (CIO), Procurement Officer.	● YES ● NO ● UNSURE
If a terms of service agreement applies to the product, does it comply with applicable federal laws and policies?	General Counsel, Agency Records Office (ARO), Chief Information Officer (CIO), Procurement Officer.	● YES ● NO ● UNSURE

Risk Assessment: The more your agency answers “no” or “unsure” to the above questions, the greater the risk your agency may be accepting. Possible risks include:

- Failure to identify responsive records to FOIA requests leaves the agency vulnerable to congressional inquiry, as well as further legal action or litigation.
- Failure to respond, or to respond completely, to discovery requests increases the risk of losing legal challenges or of additional litigation.

- Failure to manage records in accordance with the agency's legal obligations could result in NARA opening an unauthorized disposition case, pursuant to 36 CFR 1230.
- Failure to understand records management responsibilities when participating in communications with other agencies. All agencies are responsible for capturing and managing the records they send or receive.

Classified Records and Access Restrictions

CONSIDERATION / QUESTION	STAKEHOLDER(S) INVOLVED	RESPONSE
Does the application support the creation and receipt of sensitive communications (PII, CUI, National Security Classified)?	Agency Records Officer (ARO), Chief Information Officer (CIO), Security Officer / Information Security Office, General Counsel	● YES ● NO ● UNSURE
If applicable, is Controlled Unclassified Information (CUI) including Personally Identifiable Information (PII) managed properly, in accordance with 32 CFR Part 2002?	Agency Records Officer (ARO), Chief Information Officer (CIO), Security Officer / Information Security Office, General Counsel	● YES ● NO ● UNSURE
If applicable, is National Security Classified information managed properly and protected from loss, possible compromise, or unauthorized disclosure, in accordance with Executive Order 13526? For example, only individuals with the proper clearance have access to the communications and records.	Agency Records Officer (ARO), Chief Information Officer (CIO), Security Officer / Information Security Office, General Counsel	● YES ● NO ● UNSURE
If the application involves another agency hosting a network to allow your agency to create and receive National Security Classified information, is there a Memorandum of Understanding (MOU) in place outlining records management responsibilities and processes? (for example: records ownership, records export, records declassification review)	Agency Records Officer (ARO), Chief Information Officer (CIO), Security Officer / Information Security Office, General Counsel	● YES ● NO ● UNSURE

Risk Assessment: The more your agency answers “no” or “unsure” to the above questions, the greater the risk your agency may be accepting. Possible risks include:

- Accidental disclosure of sensitive information (PII, CUI, National Security Classified), in violation of Executive Order 13526, 32 CFR Part 2002, or other applicable regulations.

Conclusion

After completing the risk assessments for each electronic messaging application under consideration, an agency can determine which application presents the lowest risk by meeting federal requirements. This toolkit includes recommendations; however, the approach is ultimately a decision made by the agency. Agencies that have already implemented an electronic messaging application may find this tool useful for assessing their compliance risks.

NARA recommends that agencies bring together all relevant stakeholders to answer and discuss the assessment questions. A higher frequency of 'no' or 'unsure' responses in the assessment indicates increased regulatory compliance risk associated with the agency's use of the messaging application. NARA strongly encourages agencies to consider the risks associated with using particular tools, along with their potential benefits. Agencies are responsible for meeting their records management, legal, technical, and security requirements when using any application, tool, or system. Once the assessment team has completed its initial work, agencies may find it valuable to have the team continue supporting the deployment and oversight of the electronic messaging application.

This toolkit represents only the first step in an overall agency implementation process. Once an agency completes the vetting process and selects a tool to meet their business needs and applicable regulatory requirements, the agency will need to ensure that policies, procedures, training, user agreements, and a method for evaluating and enforcing compliance are in place when the application is deployed.

Further Resources:

- NARA Bulletin 2023-04: Managing Records Created on Collaboration Platforms
- Electronic Messages White Paper