



Office of Inspector General  
United States Department of State

AUD-GEER-25-10

Office of Audits

January 2025

**(U) Audit of U.S. Embassy Kyiv, Ukraine,  
Records Retention for Electronic  
Messaging**

GLOBAL EMERGENCIES AND EMERGING RISKS



# HIGHLIGHTS

Office of Inspector General  
United States Department of State

AUD-GEER-25-10

## **(U) What OIG Audited**

(U) According to the Foreign Affairs Manual, all Department of State (Department) personnel have a legal responsibility to ensure federal records they create or receive while conducting Department business are preserved on Department platforms. Department personnel are generally prohibited from using electronic messaging (eMessaging) platforms without an archive or export feature that allows users to easily preserve messages related to Department business. However, given the critical threat environment faced by U.S. personnel in Ukraine, U.S. Embassy Kyiv has required the use of third-party eMessaging application Signal to rapidly disseminate essential security-related information.

(U) The Office of Inspector General (OIG) conducted this audit to determine whether U.S. Embassy Kyiv, Ukraine, had implemented measures to preserve federal records created using eMessaging applications.

## **(U) What OIG Recommends**

(U) OIG made three recommendations to Embassy Kyiv and four recommendations to the Bureau of Administration to address the deficiencies identified in this report. Based on Management's response to a draft of this report, the recommendations for Embassy Kyiv are closed, and the recommendations for the Bureau of Administration are resolved, pending further action. A synopsis of Management's comments and OIG's reply follow each recommendation in the Results section of this report. Embassy Kyiv and the Bureau of Administration responses to a draft of this report are reprinted in their entirety in Appendices B and C, respectively.

January 2025

OFFICE OF AUDITS

GLOBAL EMERGENCIES AND EMERGING RISKS

## **(U) Audit of U.S. Embassy Kyiv, Ukraine, Records Retention for Electronic Messaging**

### **(U) What OIG Found**

(U) Embassy Kyiv did not implement adequate measures to preserve federal records created using eMessaging platforms. Although Embassy Kyiv distributed a Management Notice in April 2024 reminding staff of federal records retention requirements, it did not institute additional measures to ensure staff preserved records created or received using eMessaging applications. OIG also found that many Embassy Kyiv personnel reported using the eMessaging platform Signal to conduct official Department business but did not consistently preserve correspondence in accordance with federal requirements.

(U) This occurred, in part, because Embassy Kyiv records management officials did not prioritize Department requirements for preserving records. For example, Embassy Kyiv officials did not consult the Bureau of Administration or obtain its authorization to use Signal, did not assess the extent to which Signal was being used by embassy personnel to conduct official business, and did not issue a Management Notice to remind staff of federal records retention requirements when using eMessaging applications until April 2024, even though Signal had been adopted for use at Embassy Kyiv in August 2022.

(U) Embassy Kyiv personnel also did not consistently preserve electronic messages (eMessages) because current guidance for preserving and protecting Signal messages used for official business is insufficient. According to both Department and Embassy Kyiv personnel, Department procedures for preserving Signal messages are burdensome and do not fully address the technical limitations and information security vulnerabilities that personnel encounter when they attempt to preserve messages.

(U) Until limitations in preserving Signal messages are addressed, the Department remains at risk of losing official records related to Embassy Kyiv's operations—such as key communications with Ukrainian counterparts and senior officials—contrary to recordkeeping requirements.

## CONTENTS

---

(U) OBJECTIVE .....	1
(U) BACKGROUND .....	1
(U) Use of Electronic Messaging Applications at U.S. Embassy Kyiv .....	2
(U) Guidance for Electronic Messaging Applications .....	3
(U) Electronic Messaging Applications Utilizing Encryption.....	4
(U) AUDIT RESULTS .....	5
(U) Finding A: Embassy Kyiv Did Not Implement Adequate Measures To Preserve Federal Records Created Using eMessaging Applications .....	5
(U) RECOMMENDATIONS.....	22
(U) APPENDIX A: PURPOSE, SCOPE, AND METHODOLOGY.....	24
(U) Data Reliability.....	25
(U) Work Related to Internal Control .....	25
(U) Prior Office of Inspector General Reports.....	28
(U) APPENDIX B: U.S. EMBASSY KYIV, UKRAINE, RESPONSE.....	29
(U) APPENDIX C: BUREAU OF ADMINISTRATION RESPONSE .....	34
(U) ABBREVIATIONS .....	36

## (U) OBJECTIVE

---

(U) The Office of Inspector General (OIG) conducted this audit to determine whether U.S. Embassy Kyiv, Ukraine, had implemented measures to preserve federal records created using electronic messaging applications.

## (U) BACKGROUND

---

(U) Managing records properly ensures the preservation of and timely access to the knowledge and information in the Department of State's (Department) custody. According to the Department, records are the foundation of open government and critical to transparency.<sup>1</sup> Furthermore, preservation of federal records is essential to the Department's ability to respond to any Freedom of Information Act requests from the public.

(U) The Foreign Affairs Manual (FAM) states that all Department personnel have a legal responsibility and business obligation to ensure federal records they create or receive while conducting Department business are captured, preserved, managed, and protected on Department-approved systems and platforms.<sup>2, 3</sup> However, the FAM also states that personnel are not required to preserve transitory records that do not provide evidence of substantive Department business.<sup>4</sup>

### **(U) Federal Records**

(U) According to 44 United States Code § 3301, federal records include all recorded information . . . made or received by a federal agency under federal law or in connection with the transaction of public business and preserved . . . as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States government.

### **(U) Transitory Records**

(U) The Foreign Affairs Manual, 5 FAM 435, states that personnel are not required to preserve correspondence that does "not provide evidence of substantive Department business and/or whose value to the Department is minimal and of a particularly short-term nature." Such records can relate to routine activities like coordinating logistics, internal office activities, to-do task lists, or copies of circulated internal information such as agency instructions, notifications, and newsletters.

---

<sup>1</sup> (U) As stated in the Department's "Records Management for Everyone" training. This online training on records management is completed by every Department employee on an annual basis.

<sup>2</sup> (U) 5 FAM 414(b), "Scope."

<sup>3</sup> (U) To reinforce every employee's recordkeeping responsibilities, the Department requires all personnel to complete federal records management training on an annual basis via course PK217, "Records Management for Everyone." The Department's "Records Management for Everyone" training includes limited content on preserving eMessages.

<sup>4</sup> (U) 5 FAM 435(e), "Non-Government Electronic Messaging Applications and Platforms."

(U) The Bureau of Administration's Records and Archives Management Division (A/RA) analyzes, evaluates, and oversees the Department's records management program, activities, and operations.<sup>5</sup> In addition, each overseas post is required to establish and maintain an active records management program that preserves the decisions of Department personnel and evidence of Department business. A post records management program must establish and implement internal policies and procedures that, at a minimum, inform post personnel of their recordkeeping responsibilities and ensure records are captured and stored on approved Department systems.<sup>6</sup> As part of the records management program, the management officer is responsible for appointing a Post Records Coordinator to liaise with post sections on records management activities.<sup>7</sup>

### **(U) Use of Electronic Messaging Applications at U.S. Embassy Kyiv**

(U) In technical comments provided in response to a draft of this report, Embassy Kyiv officials noted that,

given the critical threat environment posed by regular drone attacks as well as hypersonic, ballistic, and other missile threats, U.S. Embassy Kyiv requires all U.S. [government] personnel, both temporary and permanent, to maintain a suite of cell phone applications, including the third-party [electronic messaging] application Signal, which are part of a comprehensive security effort to ensure awareness, accountability, and rapid communication of essential security information to mitigate danger to all US [government] personnel in Ukraine.

(U) Accordingly, Embassy Kyiv requires all incoming U.S. government personnel traveling to Ukraine to download and use the electronic messaging (eMessaging) application Signal while at post. Signal is an end-to-end-encrypted<sup>8</sup> instant eMessaging application that allows users to send direct or group messages to other users. According to an Embassy Kyiv security official present during the February 2022 evacuation of Embassy Kyiv,<sup>9</sup> Signal was adopted following the resumption of embassy operations in May 2022 as a means to rapidly disseminate security alerts to embassy personnel. The official said Signal was chosen because it was perceived to be more secure than alternative eMessaging platforms like WhatsApp. An April 2024 Embassy Kyiv Management Notice further stated that Russia's invasion of Ukraine in February 2022 compelled U.S. Embassy Kyiv to establish a viable means to rapidly disseminate security alert information "on a commonly accessible eMessaging platform; the Signal application filled that

---

<sup>5</sup> (U) 1 FAM 215.3-7(c), "Records and Archives Management Division (A/GIS/IPS/RA)."

<sup>6</sup> (U) 5 FAM 418.9, "Posts."

<sup>7</sup> (U) 5 FAM 418.9-1, "Management Officer."

<sup>8</sup> (U) According to the Bureau of Diplomatic Security's Cyber Threat Analysis Division, encryption is the process of encoding the data one device is sending to another in a form that only the receiving device will be able to translate, which unauthorized parties viewing the encrypted data should not be able to understand.

<sup>9</sup> (U) Embassy Kyiv planned for and executed an evacuation in February 2022 following months of public warnings from the Biden Administration about a possible full-scale invasion by Russia.

niche.”<sup>10</sup> Accordingly, all U.S. government personnel at Embassy Kyiv are required to have access to Signal on their mobile phones at all times to receive immediate physical security communications.

(SBU) In its Cyber Threat Assessment for the U.S. Mission to Ukraine, the Bureau of Diplomatic Security’s (DS) Cyber Threat Analysis Division concluded (b) (7)(F)

[REDACTED]

<sup>11</sup> (b) (7)(F)

(U) One Embassy Kyiv official stressed that Embassy Kyiv continues to use Signal on the recommendation of U.S. government entities, including DS, concerned with ensuring secure, rapid, and easily accessible communications in a high-threat environment.<sup>12</sup> Signal remains an important platform for Embassy Kyiv operations because it is used for critical embassy security communications, including tracking personnel movements and announcing air raid instructions.

### **(U) Guidance for Electronic Messaging Applications**

(U) The FAM states that all Department personnel must use Department-approved systems, platforms, and applications to the fullest extent possible to conduct Department business.<sup>13, 14</sup> However, the Department has also acknowledged the expanding official use of nongovernment platforms, including eMessaging applications.<sup>15, 16</sup> Accordingly, the FAM outlines circumstances and scenarios in which Department personnel are allowed to use nonofficial eMessaging

---

<sup>10</sup> (U) U.S. Embassy Kyiv Management Notice 24-039, “US Embassy Kyiv Records Guidance for eMessages,” April 26, 2024.

<sup>11</sup> (U) DS, Directorate of Cyber and Technology Security, Cyber Threat Analysis Division, “Cyber Threat Assessment, U.S. Mission to Ukraine” (January 2023).

<sup>12</sup> (U) Embassy Kyiv records management officials noted that another reason the embassy adopted Signal was that they required the use of a platform accessible to all U.S. government agencies working out of Embassy Kyiv. For example, although the Department uses the Microsoft suite of applications, the U.S. Agency for International Development uses Google’s suite of software to conduct its business. Thus, a communications platform like Microsoft Teams is not available to all U.S. government personnel in Ukraine.

<sup>13</sup> (U) 5 FAM 431(b)(2), “General.”

<sup>14</sup> (U) For example, 5 FAM 432, “Department’s Central Email Archive,” states that all emails and attachments that are created or received to conduct Department business are federal records and clarifies that the Department’s central email system automatically captures, manages, and preserves all emails sent and received on Department systems into a central archive.

<sup>15</sup> (U) Electronic messaging, as defined in 5 FAM 415, “Definitions,” is “information sent or received between individuals over a communications platform or device. Electronic messages apply to text messaging, chat/instant messaging, and other forms of electronic messaging applications available through social media or mobile devices. They can reside on agency networks and devices, on personal devices, or [be] hosted by third-party providers.”

<sup>16</sup> (U) OIG previously reported on the need for the Department to issue additional guidance to fulfill recordkeeping requirements when using electronic messaging applications in *Management Assistance Report: Remote Missions Face Challenges Maintaining Communications With Locally Employed Staff and Host Country Government Officials* (AUD-MERO-21-16, March 2021).

applications. Specifically, the use of nonofficial eMessaging applications to conduct Department business is permitted when (1) the application is the only means of communication a partner is willing to use or (2) engagement is greatly enhanced by using such means of communication to carry out the Department's mission, such as coordinating routine operations or communicating during emergency, contingency, and continuity events.<sup>17</sup>

(U) The FAM further states that, when nongovernment eMessaging applications are used to conduct Department business, users in the group must take subsequent steps to ensure the records are captured on official Department systems.<sup>18</sup> In August 2023, A/RA formalized additional Department records guidance in "Records Guidance for Electronic Messages (eMessages)," which specifies the types of eMessages that must be preserved and exported to fulfil Federal Records Act requirements. The guidance includes specific procedures on how to preserve such records in official Department systems.

### **(U) Electronic Messaging Applications Utilizing Encryption**

(U) DS's Cyber Threat Analysis Division broadly warned that foreign intelligence entities can target U.S. government personnel traveling overseas and that adversaries may monitor unencrypted communications.<sup>19</sup>

(U) Although DS advised Department personnel to conduct business and sensitive communications only on U.S. government networks, in instances in which personnel must use eMessaging applications, the bureau recommended the use of encrypted eMessaging applications as a means to protect personal communications.<sup>20</sup> As noted, according to the Cyber Threat Analysis Division, encryption is the process of encoding the data one device is sending to another it in a form that only the receiving device will be able to translate, which unauthorized parties viewing the encrypted data should not be able to understand. eMessaging applications that utilize encryption, such as Facebook Messenger, WhatsApp, Signal, and Telegram, have been increasingly used by embassies and consulates around the world for secure communications. Figure 1 demonstrates how unencrypted eMessages can potentially be intercepted by an unauthorized party, and Figure 2 illustrates how encrypted eMessaging applications protect messages from being intercepted.

---

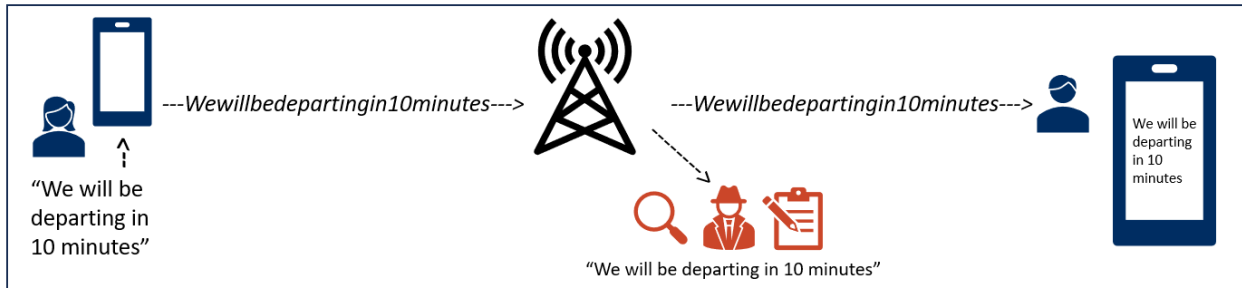
<sup>17</sup> (U) 5 FAM 435(c), "Non-Government Electronic Messaging Applications and Platforms."

<sup>18</sup> (U) 5 FAM 435(d).

<sup>19</sup> (U) The Cyber Threat Analysis Division produces cyber threat advisories, special reports, and comprehensive threat assessments concerning threats to, and potential vulnerabilities of, Department networks. The Division regularly distributes assessments through Department cables and maintains a report repository on an internal Department website.

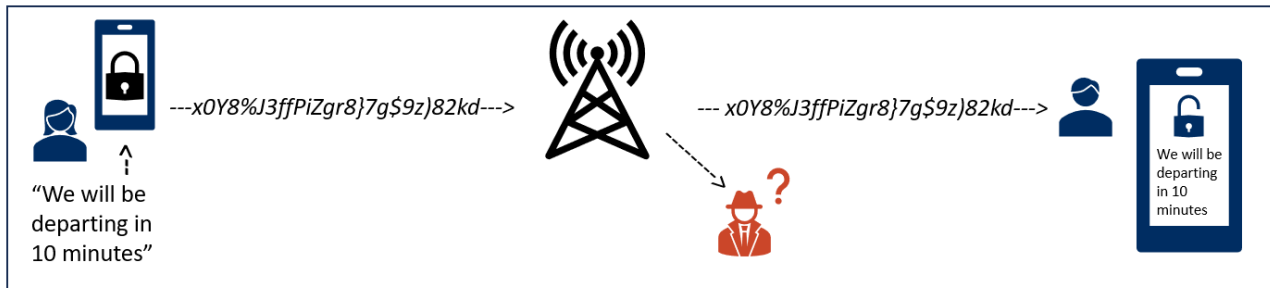
<sup>20</sup> (U) DS, Directorate of Cyber and Technology Security, Cyber Threat Analysis Division, "Cyber Threat Travel Mitigation Strategies" (October 2023).

**(U) Figure 1: Unencrypted eMessages Can Be Intercepted by Unauthorized Parties**



**(U) Source:** Generated by OIG based on figures developed by the DS Cyber Threat Analysis Division.

**(U) Figure 2: eMessaging Applications Using Encryption Protect Messages from Interception**



**(U) Source:** Generated by OIG based on figures developed by the DS Cyber Threat Analysis Division.

**(U) AUDIT RESULTS**

**(U) Finding A: Embassy Kyiv Did Not Implement Adequate Measures To Preserve Federal Records Created Using eMessaging Applications**

(U) OIG found that Embassy Kyiv did not implement adequate measures to preserve federal records created using eMessaging platforms. Although Embassy Kyiv distributed a Management Notice in April 2024 reminding staff of records retention requirements, it did not institute additional measures to ensure staff preserved records created or received using eMessaging applications. Moreover, OIG found that many Embassy Kyiv personnel reported using Signal to conduct official Department business but did not consistently preserve correspondence from the platform in accordance with federal records retention requirements.



(U) This occurred, in part, because Embassy Kyiv records management officials<sup>21</sup> did not prioritize Department requirements for preserving records. For example, Kyiv records management officials did not consult the Bureau of Administration or obtain its authorization to use Signal, did not assess the extent to which Signal was being used by embassy personnel to conduct official business, and did not issue a Management Notice to remind staff of federal records retention requirements when using eMessaging applications until April 2024, even though Signal had been adopted for use at Embassy Kyiv in August 2022. In addition, Embassy Kyiv personnel did not consistently preserve messages in accordance with recordkeeping requirements because Department guidance on preserving and protecting Signal messages used for official business was insufficient. Both Department and Embassy Kyiv personnel stated that established procedures for preserving Signal messages are burdensome and do not fully address the technical limitations and information security vulnerabilities that personnel encounter when they attempt to preserve messages.

(U) Until limitations in preserving Signal messages are addressed, Embassy Kyiv remains at risk of losing official records related to its operations—including key communications with Ukrainian counterparts and senior officials including the Ambassador—contrary to federal recordkeeping requirements.

***(U) Embassy Kyiv Personnel Did Not Consistently Preserve eMessaging Correspondence in Accordance With Department Requirements***

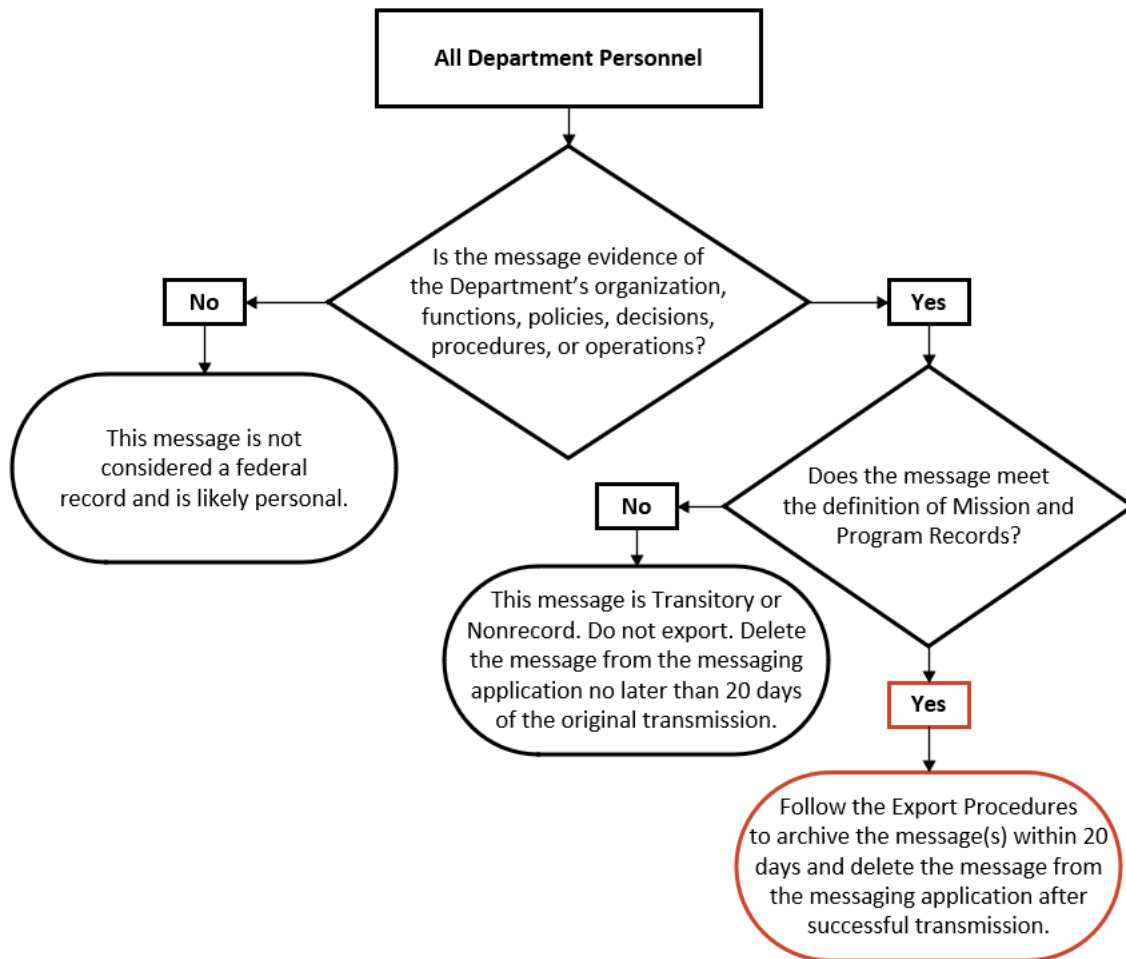
(U) A/RA's "Records Guidance for Electronic Messages" states that records related to the unique and substantive activities of post or that provide evidence of decision making must be retained under federal recordkeeping requirements. The FAM further states that personnel are not required to preserve correspondence that does "not provide evidence of substantive Department business and/or whose value to the Department is minimal and of a particularly short-term nature."<sup>22</sup> Such records, often referred to as transitory records, relate to routine activities like coordinating logistics, internal office activities, to-do task lists, or copies of circulated internal information such as agency instructions, notifications, and newsletters. An A/RA official told OIG that, if there is any doubt about whether an eMessage constitutes a federal record, however, Department personnel should retain the correspondence on an official Department system "to be safe." Figure 3 shows A/RA's supplementary guidance to help Department personnel determine whether the content of an eMessage must be preserved as a federal record.

---

<sup>21</sup> (U) OIG uses the term "records management officials" to encompass all post personnel designated with records responsibilities as listed in 5 FAM 418.9, "Posts." This section states that the Principal Officer at each post is responsible for establishing and maintaining an active records management program. The FAM further lists the responsibilities of the Management Officer and Section Chiefs. OIG interviewed Embassy Kyiv records management officials in April 2024, including the designated Post Records Coordinator, prior to staff departing to onward assignments in June 2024.

<sup>22</sup> (U) 5 FAM 435(e), "Non-Government Electronic Messaging Applications and Platforms."

**(U) Figure 3: Decision Tree for Determining Whether an eMessage Must Be Exported and Captured as a Federal Record**



**(U) Source:** Generated by OIG from A/RA's "Records Guidance for Electronic Messages."

(U) In April 2024, Embassy Kyiv emailed to embassy personnel a Management Notice entitled "Records Guidance for Electronic Messages" that stated that Embassy Kyiv personnel were authorized to use Signal only for "transitory and non-record" messages.<sup>23</sup> Such business would generally not require formal preservation. The April 2024 Management Notice further clarified that federal records subject to preservation include "any information created or received by a government agency that is relevant to its operations or decision-making processes" and shared the A/RA procedures for preserving federal records generated or received on Signal.<sup>24</sup> Because some eMessaging platforms, including Signal, have no text export functionality, Department

<sup>23</sup> (U) U.S. Embassy Kyiv Management Notice 24-039, "US Embassy Kyiv Records Guidance for eMessages," April 26, 2024. This Management Notice was distributed a few weeks after OIG first contacted Embassy Kyiv officials on April 8, 2024, regarding planned audit work related to eMessage records retention.

<sup>24</sup> (U) Ibid.

Records Management guidance directs users to take screenshots<sup>25</sup> of the entirety of any conversation reflecting Department business, forward the screenshots to a Department email address, and then delete the messages from Signal.<sup>26</sup>

(U) OIG conducted 12 interviews across 9 sections and offices at Embassy Kyiv to determine whether Department personnel have preserved federal records directly from Signal, whether personnel knew how to preserve records from Signal, and whether personnel were aware of any measures implemented by Embassy Kyiv management to reinforce the requirement to preserve federal records from Signal. Specifically, OIG interviewed personnel from Embassy Kyiv’s Management section, Consular section, Political section, Economics section, Public Affairs section, Regional Security Office, International Narcotics and Law Enforcement Office, Assistance Coordination Unit, and Front Office.

(U) Despite the April 2024 Management Notice stating that Signal was authorized only for transitory, non-record messages, OIG found that personnel across Embassy Kyiv were regularly using Signal to conduct substantive Department business, including mission and programmatic communications. OIG summarized descriptions of how Embassy Kyiv personnel reported using Signal at Embassy Kyiv in Table 1.

**(U) Table 1: How Embassy Personnel Use Signal To Conduct Department Business**

<b>(U) Signal Use</b>	<b>(U) Description of Use at Embassy Kyiv</b>
<b>Mandatory Mission Security-Related Chat Group</b>	Embassy Kyiv security personnel utilize this chat group to rapidly disseminate security alerts to all U.S. government personnel in Kyiv.
<b>Leadership Decision Making</b>	Embassy Kyiv leadership, including the Ambassador, Deputy Chief of Mission, and security personnel, utilize a dedicated Signal group for urgent mission communications including deliberating on security-related decisions. These decisions may then be distributed via Signal to alert all U.S. government personnel in Kyiv.
<b>Embassy Section Groups</b>	Many embassy sections use internal group chats to conduct day-to-day business such as sharing relevant news articles, coordinating meetings, or tracking the movements of staff.
<b>Ambassador Communications</b>	Multiple embassy officials told OIG that the Ambassador often makes requests and coordinates with staff via Signal.
<b>External Communications</b>	Embassy personnel stated they use eMessaging platforms to correspond with local or other foreign contacts in governments or partner organizations. This correspondence included communications with Ukrainian contacts to discuss policy issues, conduct preliminary negotiations, share news, and coordinate meetings.
<b>High-Level Visits</b>	Embassy personnel said they have created specific Signal groups to plan and coordinate information and logistics for high-level visitors.

<sup>25</sup> (U) A screenshot is a digital image that captures the contents of a computer or device's screen at a specific moment.

<sup>26</sup> (U) A/RA’s “Records Guidance for Electronic Messages” (August 2023).

**(U) Signal Use**

**(U) Description of Use at Embassy Kyiv**

<b>Consular Outreach</b>	Consular personnel may utilize Signal to securely communicate with American citizens or collect documentation related to American citizen services cases.
<b>Embassy Operational Updates</b>	Embassy Kyiv management maintains various chat groups to communicate operational information such as shuttle schedules or planned power outages.

**(U) Source:** Generated by OIG based on a survey of personnel from all Department sections at Embassy Kyiv.

(U) OIG found that Embassy Kyiv personnel from seven out of nine sections reported regularly using Signal to conduct Department business, including describing examples of correspondence that would constitute original federal records. Some Embassy Kyiv personnel told OIG that they used Signal to communicate information relevant to Embassy Kyiv’s operations and decision-making processes—information that was substantive and not strictly short-term in nature.

(U) Several officials at Embassy Kyiv told OIG that they had conducted official Department business on Signal on a limited basis at some point in time but that they also had never attempted to preserve Signal messages per Department guidance. For example, some sections told OIG that they used Signal to regularly correspond with local Ukrainian contacts in the normal course of diplomatic communications, including discussing policy, conducting preliminary negotiations, and relaying news about the Government of Ukraine. However, these same officials also noted they had never attempted to preserve messages in accordance with Department guidance.<sup>27</sup>

(U) Although OIG found that several Embassy Kyiv sections utilized Signal to conduct Department business subject to federal recordkeeping requirements, only Embassy Kyiv’s Consular section reported preserving federal records directly from Signal. An official from the Consular section stated that they preserved records directly from Signal because of their general knowledge of federal recordkeeping requirements. Personnel from all other Embassy Kyiv sections indicated that they had not preserved records directly from Signal, though many expressed the belief that their communications were transitory and therefore not subject to records retention requirements.

(U) Finally, OIG found that communications among members of a key embassy leadership group on Signal were not preserved in accordance with Department recordkeeping requirements. Specifically, Embassy Kyiv officials told OIG that embassy leadership, including the Ambassador, Deputy Chief of Mission, the Regional Security Officer, and other U.S. government officials, utilized a dedicated Signal group for deliberating on urgent mission-critical issues including security-related concerns. Based on decisions made in the group, officials subsequently issued

---

<sup>27</sup> (U) The Department’s “Records Management for Everyone” training, which must be completed by every Department employee on an annual basis, includes limited content on the preservation of eMessages. As this training was presumably completed by every Department employee at Embassy Kyiv within the year, personnel were informed that they were responsible for proactively identifying federal records created on eMessaging platforms when corresponding with local contacts and preserving them, as required.

security directives to Embassy Kyiv personnel. Some Embassy Kyiv officials acknowledged that such communications include evidence of time-sensitive decision making related to the safety and security of personnel and therefore likely are federal records. However, these same officials acknowledged that they were not aware of measures taken to ensure the preservation of records from this Signal chat group.

(U) A/RA's "Records Guidance for Electronic Messages" states that Mission Records "[r]elate to the unique and substantive functions and activities of the bureau or post that are required to meet legal or fiscal obligations . . . or provide evidence of decision-making."<sup>28</sup> Such federal records include documentation on security awareness, countermeasures, threats, and other related subjects.

(U) When presented with a description of the correspondence contained within Embassy Kyiv leadership's dedicated Signal group, an A/RA official concluded that the chat group constituted federal record material because the correspondence reflected original deliberations and decision making by embassy leadership. The same official specifically noted that, if a high-profile security incident involving Embassy Kyiv personnel were to occur, many U.S. government entities would be interested in understanding the context and timing of the related leadership decisions. Some Embassy Kyiv personnel told OIG that information from the leadership's Signal chat group is often reproduced in other communications, such as Emergency Action Committee cables or other security reports developed by the Embassy Kyiv Regional Security Office. However, OIG found that the embassy had not yet developed a process to ensure that the original records from this Signal chat group are preserved in accordance with Department requirements. A/RA officials told OIG that, if embassy leadership is using an eMessaging platform to conduct Department business, there must be additional efforts to retain those records.<sup>29</sup>

### ***(U) Records Management Officials Did Not Prioritize Department Requirements for Preserving Records***

(U) Embassy Kyiv did not implement adequate measures to preserve federal records created using eMessaging platforms, in part, because Embassy Kyiv records management officials did not prioritize Department requirements for preserving Signal messages. For example, according to the FAM, Department personnel are generally prohibited from conducting official Department business on eMessaging applications without an archive or export feature to preserve messages. Staff are instructed to contact the Department's records office immediately if using such an application is critical to carrying out the Department's mission.<sup>30</sup> However,

---

<sup>28</sup> (U) A/RA's "Records Guidance for Electronic Messages (eMessages)," (August 2023).

<sup>29</sup> (U) In technical comments provided in response to a draft of this report, Embassy Kyiv informed OIG that the "original contents of [Embassy Kyiv leadership's] [S]ignal chat group are now being preserved in accordance with requirements." However, OIG was unable to verify this statement because supporting documentation was not provided.

<sup>30</sup> (U) 5 FAM 435(a),(b), "Non-Government Electronic Messaging Applications and Platforms."

Embassy Kyiv records management officials did not consult or obtain authorization from the Bureau of Administration about Embassy Kyiv's use of Signal until April 2024.

(U) The FAM also requires each post to establish and maintain an active records management program that preserves the decisions of Department personnel and evidence of Department business. Specifically, a post records management program must establish and implement internal policies and procedures that, at a minimum, require (1) informing post personnel of their recordkeeping responsibilities, (2) ensuring records are captured and stored on approved Department systems, and (3) continually examining and updating post records management policies and procedures to reflect current post program functions and operations and to comply with Department records management policies and procedures.<sup>31</sup> The Management Officer, specifically, is responsible for appointing a Post Records Coordinator to liaise with post sections on records management activities.<sup>32</sup>

(U) However, Embassy Kyiv did not formally designate a Post Records Coordinator until April 2024. Specifically, the Embassy Kyiv Information Management Officer indicated that he had been serving as the default Post Records Coordinator since his arrival in 2021, though Embassy Kyiv did not formally designate him as the Post Records Coordinator until April 2024. The Information Management Officer departed Embassy Kyiv in June 2024, and, as of October 2024, Embassy Kyiv had not designated a replacement Post Records Coordinator.

(U) Although Embassy Kyiv has required the use of Signal for security purposes such as tracking personnel movements since at least August 2022,<sup>33</sup> Embassy Kyiv did not formally inform post personnel of their recordkeeping responsibilities for eMessages until distributing Department guidance regarding the preservation of eMessages on April 26, 2024.<sup>34</sup> OIG also found that Embassy Kyiv records management officials did not reach out to personnel at post to assess the use of Signal at post and therefore were unaware of the extent to which post personnel were using Signal to conduct official business.

(U) Embassy Kyiv made progress towards greater compliance with records management standards after distributing the April 2024 Management Notice; however, OIG found that personnel from four of nine sections remained unfamiliar with official procedures for preserving records from Signal even after the Management Notice was issued. The Embassy Kyiv Information Management Officer charged with post records coordination responsibilities told OIG that he was working on preliminary ideas to inform post personnel of their recordkeeping responsibilities and to increase compliance. These ideas included sending out

---

<sup>31</sup> (U) 5 FAM 418.9, "Posts."

<sup>32</sup> (U) 5 FAM 418.9-1(1), "Management Officer."

<sup>33</sup> (U) In technical comments provided in response to a draft of this report, Embassy Kyiv indicated that embassy personnel faced a challenging working environment in May 2022 when the embassy resumed operations following the Russian invasion and that priority was not given to records management at that time. Specifically, Embassy Kyiv noted that, at that time, the only management office member present in Kyiv was the facilities manager.

<sup>34</sup> (U) OIG first contacted Embassy Kyiv officials regarding planned audit work related to eMessage records retention on April 8, 2024.

monthly reminders via email or via Signal itself. However, the Information Management Officer departed the embassy in June 2024, and, as of October 2024, a replacement had not been designated. Furthermore, as of October 2024, Embassy Kyiv had not issued any further notices informing post personnel of their recordkeeping responsibilities, including preserving relevant communications on eMessaging applications, or taken other steps to ensure compliance with federal records retention requirements.

(U) The widespread use of Signal across the embassy, coupled with the frequent rotation of U.S. government personnel through Ukraine, presents unique challenges to Embassy Kyiv's records management program.<sup>35</sup> Effective management of federal records is essential for Department operations. It ensures that agencies can efficiently locate and retrieve records needed in the daily performance of their missions and that the Department has a reliable means of preserving essential information about Department operations and decision making. When a post does not fully comply with federal records retention requirements, the Department is at risk of losing critical records related to operations, including key communications with host-country counterparts, essential information regarding security-related decisions, and relevant directives from senior staff including the Ambassador. These records could include key decision making involving the safety and security of U.S. government personnel. To promote the preservation of federal records created at Embassy Kyiv, OIG is offering the following recommendations.

**Recommendation 1:** (U) OIG recommends that U.S. Embassy Kyiv officially designate a Post Records Coordinator to regularly review post's records management practices and liaise with embassy sections on records management requirements, as required by 5 Foreign Affairs Manual 418.9.

**Management Response:** (U) U.S. Embassy Kyiv concurred with the recommendation and stated that it designated a Post Records Coordinator on November 25, 2024, prior to the release of OIG's draft report. Embassy Kyiv further noted that the embassy's management team has been "sorely understaffed" since the embassy's reopening in May 2022. Embassy Kyiv provided OIG with documentation showing that it designated a Post Records Coordinator and a copy of its January 2025 Records Management Standard Operating Procedure on federal recordkeeping responsibilities.

**OIG Reply:** (U) Based on U.S. Embassy Kyiv's concurrence and the documentation provided to address the recommendation, OIG considers this recommendation implemented and closed and no further action is required. Specifically, OIG verified that Embassy Kyiv officially designated a Post Records Coordinator in November 2024 and that Embassy Kyiv's January 2025 Records Management Standard Operating Procedure specifies the coordinator's responsibilities to liaise with embassy sections as required by 5 Foreign Affairs Manual 418.9.

---

<sup>35</sup> (U) Staff assigned to Embassy Kyiv typically only serve 1-year tours. The increased rotation of staff through Embassy Kyiv may require more frequent reminders about complying with federal records retention requirements when using eMessaging applications.

**Recommendation 2:** (U) OIG recommends that U.S. Embassy Kyiv (1) develop and implement post-specific guidance on federal recordkeeping responsibilities, including the definition of what types of electronic messaging communications must be retained to comply with federal records retention requirements as well as direction on how to preserve records received or created on electronic messaging platforms and (2) develop and implement a procedure to periodically communicate the guidance to post personnel and keep the guidance updated on Embassy Kyiv's SharePoint page.

**Management Response:** (U) U.S. Embassy Kyiv concurred with the recommendation and stated that the embassy had adopted a post standard operating procedure on federal recordkeeping responsibilities, January 2025 Records Management Standard Operating Procedure, including definitions of what types of records must be retained and procedures to ensure regular updates, communication, and dissemination of both current requirements and record preservation for fully unclassified records through multiple channels, including Signal, and alongside all other security management notices on the Embassy's SharePoint platform. Embassy Kyiv provided OIG with a copy of its new January 2025 Records Management Standard Operating Procedure on federal recordkeeping responsibilities.

**OIG Reply:** (U) Based on U.S. Embassy Kyiv's concurrence and the documentation provided to address the recommendation, OIG considers the recommendation implemented and closed and no further action is required. Specifically, OIG reviewed Embassy Kyiv's January 2025 Records Management Standard Operating Procedure, dated January 17, 2025. The procedure states that the Post Records Management Coordinator is responsible for ensuring "reminders and updates on records management are communicated periodically by sending via email and/or messaging applications at least quarterly, and that guidance is generally available to the community" on the Embassy Kyiv SharePoint page. In addition, the standard operating procedure provides instructions for how electronic messaging communications must be retained, stating that one must ensure "that communications involving key decision-making are preserved by forwarding screenshots of [S]ignal chats if necessary" to one's state.gov email address in order to ensure they are preserved in accordance with federal recordkeeping requirements, "even if replicated in other formats like emails or cables."

**Recommendation 3:** (U) OIG recommends that U.S. Embassy Kyiv develop and implement internal controls to ensure that post records management officials routinely liaise with post sections on records management requirements, remain aware of the extent to which electronic messaging applications are used to conduct Department of State (Department) business, and implement internal policies to promote the preservation of records on electronic messaging platforms in accordance with Department requirements.

**Management Response:** (U) U.S. Embassy Kyiv concurred with the recommendation and stated that, as part of its January 2025 Records Management Standard Operating Procedure, "the Post Management Officer and Records Coordinator now have clearly defined responsibilities to provide oversight and guidance and to remind post personnel of their record disposition responsibilities as described in 5 FAM 418.9 and subsequent



sections and to advise personnel on both internal policies and best practices to promote the preservation of eMessaging records in line with the latest Department guidance.” Embassy Kyiv provided OIG with a copy of its new January 2025 Records Management Standard Operating Procedure on federal recordkeeping responsibilities.

**OIG Reply:** (U) Based on U.S. Embassy Kyiv’s concurrence and the documentation provided to address the recommendation, OIG considers the recommendation implemented and closed and no further action is required. Specifically, OIG reviewed Embassy Kyiv’s January 2025 Records Management Standard Operating Procedure, dated January 17, 2025. The procedure outlines responsibilities for the Mission Ukraine Post Records Management Coordinator including conducting “regular check-ins with embassy sections to promote compliance with requirements,” reviewing “records management practices at post annually,” and maintaining “a log of interactions and follow-ups with sections.” The procedure further states that the Embassy Kyiv Management Officer is responsible for engaging in regular outreach to embassy sections to promote records management practices, overseeing implementation of records management policies and procedures, and for ensuring a post records management coordinator is appointed and that designations are updated in a timely manner to account for transfers or other changes in personnel.

***(U) Department Guidance and Procedures Require Improvement***

(U) OIG determined that Embassy Kyiv personnel also did not consistently preserve messages in accordance with recordkeeping requirements because Department guidance for preserving and protecting Signal messages used for official business was insufficient. For example, although all Department personnel must complete mandatory federal records management training on an annual basis,<sup>36</sup> Embassy Kyiv staff told OIG they were uncertain about eMessaging records retention requirements, had questions about what types of communications constituted a record subject to preservation, and were confused about how to retain messages from Signal.

(U) OIG previously reported<sup>37</sup> that eMessaging applications were essential to the daily operations of remote missions and that Department guidance was needed to fulfill recordkeeping requirements when using such applications.<sup>38</sup> OIG closed the recommendation

---

<sup>36</sup> (U) The required annual records management training from the Department’s Foreign Service Institute is called PK217 “Records Management for Everyone.” As of August 2024, the training contains limited information regarding “Records on Non-State Systems, Personal Accounts, or Devices.” It includes links to 5 FAM 435, direction to forward records to a Department system within 20 days, and a “Frequently Asked Questions” document specifically focused on the use of eMessaging applications.

<sup>37</sup> (U) OIG, *Management Assistance Report: Remote Missions Face Challenges Maintaining Communications With Locally Employed Staff and Host Country Government Officials* (AUD-MERO-21-16, March 2021).

<sup>38</sup> (U) The Department may decide to establish operations in a separate location, known as a “remote mission,” after an embassy is evacuated. In its *Management Assistance Report: Remote Missions Face Challenges Maintaining Communications With Locally Employed Staff and Host Country Government Officials* (AUD-MERO-21-16, March 2021), OIG reported that the Yemen Affairs Unit, Venezuela Affairs Unit, and Embassy Mogadishu relied on the use of eMessaging applications. For example, an Embassy Mogadishu official reported that the Somali government did not have an established government email address system, leading the embassy to rely heavily on the use of electronic messaging applications for communications.

involving eMessaging records retention that it made in that report after the Bureau of Administration issued eMessaging guidance in 2021. However, according to both Department and Embassy Kyiv personnel, established procedures for preserving Signal messages can be improved. Specifically, Department procedures for preserving eMessages are burdensome and do not fully address the technical limitations and information security vulnerabilities that personnel encounter when they attempt to preserve messages.

*(U) Burdensome Procedures*

(U) The FAM requires that, when non-U.S. government eMessaging applications are used to conduct Department business, users must capture records on official Department systems. Specifically, personnel must copy or forward records from an eMessaging platform to a Department email account within 20 calendar days of the creation or receipt of a federal record.<sup>39</sup> As mentioned previously, when there is no export functionality available on an eMessaging application—as is the case for Signal—supplementary A/RA guidance directs employees to take screenshots of relevant messages and then forward the screenshots to a state.gov email address.<sup>40</sup> When presented with A/RA’s guidance, several Embassy Kyiv personnel commented that the described procedures were burdensome and time consuming, especially given the significant workload at post.

(U) Moreover, many Embassy Kyiv personnel emphasized their belief that Department business conducted via Signal is appropriately retained through other platforms. For example, some embassy personnel noted that, in some cases, the essential content of Signal communications is later replicated in other official Department platforms, such as email or Department cables. In such cases, key information from Signal communications would be preserved. However, this approach does not strictly comply with Department policy, as the FAM does not specify any exceptions to the requirement to copy or forward communications directly from an eMessaging platform to a Department email account. An A/RA official indicated that transcribing information directly from Signal into other official Department communications such as an email, cable, or report, although not technically compliant with the established guidance, could be an acceptable alternative to retaining information. However, the A/RA official emphasized that this practice risks the omission of information contained in the original correspondence. Several Embassy Kyiv personnel told OIG that they would like Department policy and guidance to be more flexible regarding Signal use and to explicitly address some of the challenges encountered when attempting to preserve records.

*(U) Technical Limitations*

(U) Embassy Kyiv personnel also described technical limitations in following the Department’s procedures for retaining records from eMessaging platforms. For example, some staff told OIG that they could not follow the A/RA screenshot procedure without encountering technological

---

<sup>39</sup> (U) 5 FAM 435(d)(1), “Non-Government Electronic Messaging Applications and Platforms.” Forwarding records to a Department email account will result in the automatic preservation of a screenshot containing a record of concern.

<sup>40</sup> (U) A/RA’s “Records Guidance for Electronic Messages (eMessages),” (August 2023).

barriers, such as Department firewalls that prevented them from attaching screenshots directly to emails using Department email accounts. As a result, they indicated, complying with policy would force them to first attach Signal screenshots to an email using their personal email account and then send the email to their Department email account.<sup>41</sup> Embassy Kyiv personnel expressed strong reservations to OIG about utilizing personal email accounts to send evidence of Department business, and a DS official also noted that this method of transmission could be unencrypted, which would be less secure.<sup>42</sup> Another Department records management official told OIG that, even when screenshots containing records are transmitted to a Department email account, one could not easily locate the records at a future point in time. The official explained that, because screenshot files in a Department inbox are not text-searchable, this could create problems locating evidence of key Department decisions or complying with Freedom of Information Act requests, for example.<sup>43</sup>

(U) In addition, some Embassy Kyiv personnel told OIG that some of their Ukrainian counterparts enable “ephemeral” eMessage settings, which auto-delete correspondence after a short period of time (as short as 30 seconds after they are viewed), leaving embassy staff with limited time to preserve original messages.<sup>44</sup> For this reason, some officials shared their view that correspondence over eMessaging platforms is often very similar to a verbal conversation, where the expectation is that a Department employee would later recall the conversation content and transcribe key information directly into a Department system, such as an email or a memo. However, Department policy and guidance does not account for the fact that Department personnel may not always be able to immediately preserve ephemeral messages generated on eMessaging platforms or provide a means for staff to later transcribe key

---

<sup>41</sup> (U) 5 FAM 434, “Personal Email Accounts,” states that all Department personnel are discouraged from using a personal email account to conduct U.S. government business. However, the FAM says that personal email accounts can be used to conduct official business in very limited circumstances, such as when access to Department systems is limited or restricted.

<sup>42</sup> (U) Transmitting a screenshot of Signal correspondence containing records from a personal email account to a Department email account introduces an added information security vulnerability, according to DS. Specifically, if the user does not immediately delete the Signal screenshot from their personal email account outbox, the correspondence containing records could be vulnerable if the user’s personal email account is hacked or compromised at a future time.

<sup>43</sup> (U) Screenshot files from mobile phones are .png file type, which are not text searchable. A/RA acknowledged this issue to OIG and stated that they work to make higher level post officials aware of this limitation and request that they include descriptive metadata within an email to make records easier to find at a future point. OIG notes that adding descriptive metadata to an email subject line is not currently outlined in the procedures to retain messages from eMessaging applications.

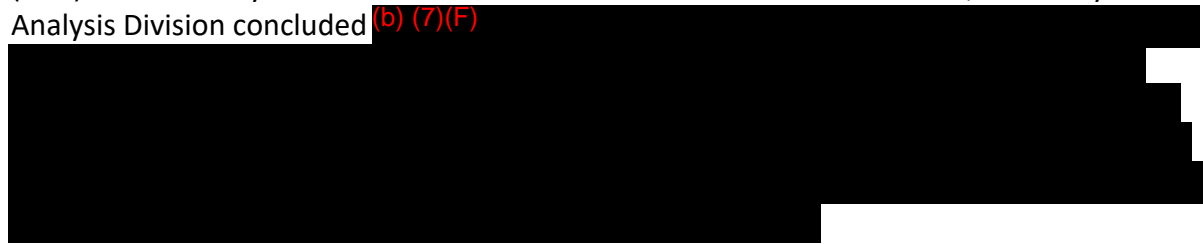
<sup>44</sup> (U) A/RA’s “Records Guidance for Electronic Messages” notes that Department personnel are prohibited from enabling automatic deletion in third-party applications. Embassy Kyiv personnel told OIG that local contacts often opt in to the auto-deletion of messages because of personal preference or information security concerns and that, as a result, post personnel do not always have the opportunity to immediately preserve Signal messages.

information from a Signal communication into another Department system.<sup>45</sup> Finally, one Embassy Kyiv official stated that they were aware of software that could automatically preserve records from other eMessaging platforms like WhatsApp and that, if the Department were to sanction use of this software, it would facilitate staff's ability to comply with federal records retention requirements.<sup>46</sup>

*(U) Information Security Vulnerabilities*

(U) An Embassy Kyiv security official told OIG that he opposed Department guidance instructing staff to take screenshots of messages from eMessaging platforms. He noted that the process essentially removes the inherent protections provided by encryption and would instead convert the contents of the correspondence into an unencrypted image file that could be vulnerable. He also expressed general concerns about information security in Ukraine, specifically, stating that, if someone's device were hacked, unencrypted screenshots containing federal records could be compromised.<sup>47</sup> In addition, an official from DS acknowledged that the transmission of records using an unreliable or compromised telecommunications network could also increase the risk that screenshots of correspondence could be intercepted. For example, transmitting images via text message over an unsecure router or cellular network increases vulnerability because the unencrypted image data can be more easily accessed by unauthorized parties.

~~(SBU)~~ In its 2023 Cyber Threat Assessment for the U.S. Mission to Ukraine, the DS Cyber Threat Analysis Division concluded (b) (7)(F)



---

<sup>45</sup> (U) According to 24 STATE 50368, "Introducing the Bureau of Diplomatic Technology," May 13, 2024, recent Bureau of Diplomatic Technology initiatives to expand access to desktop versions of eMessaging applications like Signal on official Department systems may now allow staff a means to more easily preserve correspondence from eMessaging applications. Specifically, users of these desktop versions could potentially transcribe pertinent information from Signal correspondence directly onto Department systems without transmitting screenshot files.

<sup>46</sup> (U) Officials from the Bureau of Diplomatic Technology, Office of Endpoint Engineering Support told OIG that they were looking into commercial products that could automatically retain messages from eMessaging platforms.

<sup>47</sup> (U) Procedures outlined in 5 FAM 435 and A/RA's "Records Guidance for Electronic Messages" broadly direct users to delete federal records from eMessaging applications after successfully forwarding to a state.gov email account. However, this guidance does not account for the additional vulnerabilities to records, where: (1) the screenshot image file of the records may remain on a user's cellular device after transmission to email; (2) the screenshot file may remain on a user's personal email account if they were unable to transmit directly via their Department account; and (3) deleted files often remain in a system's 'trash' for a limited period of time, which means such files may remain accessible to a hacker. Accordingly, transmitting records in accordance with Department procedures results in vulnerabilities that A/RA guidance had not accounted for at the time of the audit.

*(U) Established Department Guidance Is Inconsistent*

(U) The FAM states that Department personnel are “generally prohibited” from conducting official Department business on eMessaging applications that do not allow communications to be preserved, including Signal.<sup>48</sup> However, officials from A/RA told OIG that their office does not actually have the authority to formally prohibit using Signal. They stated that, in practice, the use of Signal is “permitted but discouraged” because of the challenges to efficiently preserve correspondence that contains federal records. A/RA officials stated that they ultimately defer to the needs of users at post, including regarding the use of whichever eMessaging platform is optimal for conducting Department business in any given country.

(U) The Bureau of Diplomatic Technology has recently enabled expanded access to eMessaging applications like WhatsApp and Signal, allowing Department users to access such applications on Department desktop systems via secure means. Officials from the Bureau of Diplomatic Technology provided data to OIG showing that these capabilities were being used extensively by Department personnel worldwide. Specifically, more than 3,000 Department personnel at more than 160 posts had registered to gain access to non-enterprise eMessaging applications in the Department’s unclassified computer system, OpenNet.<sup>49</sup> Although an official from the Bureau of Diplomatic Technology speculated that a sizeable number of these users were accessing and using Signal, the same official later told OIG that the Bureau of Diplomatic Technology could not provide a specific breakdown of how many users were using each eMessaging platform because Department users “leverage their own personal non-[Department of State] accounts to log-in and communicate over the [eMessage] applications.”

(U) The Bureau of Diplomatic Technology’s efforts to sanction and enable broader access to eMessaging applications like Signal among Department personnel worldwide raises questions about the FAM’s current “general prohibition” on certain eMessaging platforms. A/RA officials told OIG that they would be willing to consider revising the FAM’s stated “general prohibition” on eMessaging platforms like Signal and to provide greater clarity to users regarding eMessaging policy and record preservation responsibilities.

(U) Furthermore, OIG found that the Department lacked specific, reliable information on the extent to which eMessaging applications like Signal are used at posts around the world to conduct Department business. Despite Bureau of Diplomatic Technology data showing that 3,000 Department personnel were registered to access eMessaging platforms at more than 160 posts worldwide, only about a dozen posts had formally contacted A/RA about their use of Signal. A/RA officials told OIG that they had not assessed the extent to which eMessage platforms were used worldwide and acknowledged that the use of eMessaging applications by Department personnel may be more widespread, given that some users may not be aware of or

---

<sup>48</sup> (U) 5 FAM 435(a), “Non-Government Electronic Messaging Applications and Platforms.”

<sup>49</sup> (U) Specifically, Department personnel could access eMessaging platforms by accessing a virtual desktop while working on the Department’s OpenNet system. The data from the Bureau of Diplomatic Technology also show that more than 20 Embassy Kyiv personnel had registered to access eMessaging applications through the virtual desktop technology.

follow the guidance to contact A/RA regarding their planned use of Signal, in particular. Without specific and reliable information on the extent and nature of posts' use of eMessaging applications, the Department is limited in its ability to develop and implement targeted and relevant guidance for records retention that better reflects the needs of the Department's worldwide eMessaging needs.

*(U) Improving Guidance and Potential Flexibilities*

(U) Embassy Kyiv is just one of many Department posts that have adopted the use of eMessaging applications to support diplomacy and operations in a contingency environment. Insufficient Department guidance limits the ability of personnel at overseas posts to ensure that federal records received and managed on eMessaging applications are efficiently, properly, and securely retained in accordance with federal law. Improving guidance can help users of eMessaging applications at posts worldwide preserve records in accordance with federal requirements more effectively and efficiently. A/RA officials acknowledged that technologies used by the Department continue to rapidly evolve and stated that they were willing to consult DS and the Bureau of Diplomatic Technology about addressing emergent challenges related to records management. To ensure that the challenges stemming from the Department's expanding use of secure eMessaging platforms are addressed, OIG is offering the following recommendations:

**Recommendation 4:** (U) OIG recommends that the Bureau of Administration, in coordination with the Bureau of Diplomatic Technology and Bureau of Diplomatic Security, assess the extent to which electronic messaging applications, including Signal, are used at posts worldwide to conduct Department of State business.

**Management Response:** (U) The Bureau of Administration concurred with the recommendation.

**OIG Reply:** (U) Based on the Bureau of Administration's concurrence with the recommendation, OIG considers the recommendation resolved, pending further action. This recommendation will be closed when OIG receives documentation demonstrating that the Bureau of Administration has, in coordination with the Bureau of Diplomatic Technology and Bureau of Diplomatic Security, assessed the extent to which electronic messaging applications, including Signal, are used at posts worldwide to conduct Department of State business.

**Recommendation 5:** (U) OIG recommends that the Bureau of Administration, in coordination with the Bureau of Diplomatic Technology and Bureau of Diplomatic Security, determine the availability of acceptable alternative procedures and methods for preserving federal records from electronic messaging applications by (1) identifying alternative methods for preserving records from electronic messaging applications without export functions and (2) determining whether replicating electronic messaging correspondence in cables, emails, or official reports is an acceptable alternative means of preserving records of these communications.

**Management Response:** (U) The Bureau of Administration concurred with the recommendation.

**OIG Reply:** (U) Based on the Bureau of Administration's concurrence with the recommendation, OIG considers the recommendation resolved, pending further action. This recommendation will be closed when OIG receives documentation demonstrating that the Bureau of Administration has, in coordination with the Bureau of Diplomatic Technology and Bureau of Diplomatic Security, determined the availability of acceptable alternative procedures and methods for preserving federal records from electronic messaging applications by (1) identifying alternative methods for preserving records from electronic messaging applications without export functions and (2) determining whether replicating electronic messaging correspondence in cables, emails, or official reports is an acceptable alternative means of preserving records of these communications.

**Recommendation 6:** (U) OIG recommends that, if alternative procedures and methods for preserving federal records from electronic messaging applications are identified following implementation of Recommendation 5, the Bureau of Administration update the guidance for retaining electronic messages in the Foreign Affairs Manual and Records Guidance for Electronic Messages accordingly.

**Management Response:** (U) The Bureau of Administration concurred with the recommendation.

**OIG Reply:** (U) Based on the Bureau of Administration's concurrence with the recommendation, OIG considers the recommendation resolved, pending further action. This recommendation will be closed when OIG receives documentation demonstrating that, if alternative procedures and methods for preserving federal records from electronic messaging applications are identified following implementation of Recommendation 5, the Bureau of Administration has updated the guidance for retaining electronic messages in the Foreign Affairs Manual and Records Guidance for Electronic Messages.

**Recommendation 7:** (U) OIG recommends that, following the implementation of Recommendations 4, 5, and 6, the Bureau of Administration, in coordination with the Bureau of Diplomatic Technology and Bureau of Diplomatic Security, reevaluate the general prohibition on certain electronic messaging applications and update the Foreign Affairs Manual accordingly.

**Management Response:** (U) The Bureau of Administration concurred with the recommendation and stated that it will update the Foreign Affairs Manual.

**OIG Reply:** (U) Based on the Bureau of Administration's concurrence with the recommendation and planned actions, OIG considers the recommendation resolved, pending further action. This recommendation will be closed when OIG receives documentation demonstrating that, following the implementation of Recommendations 4, 5, and 6, the Bureau of Administration, in coordination with the Bureau of Diplomatic

Technology and Bureau of Diplomatic Security, has reevaluated the general prohibition on certain electronic messaging applications and updated the Foreign Affairs Manual accordingly.



## (U) RECOMMENDATIONS

---

**Recommendation 1:** (U) OIG recommends that U.S. Embassy Kyiv officially designate a Post Records Coordinator to regularly review post's records management practices and liaise with embassy sections on records management requirements, as required by 5 Foreign Affairs Manual 418.9.

**Recommendation 2:** (U) OIG recommends that U.S. Embassy Kyiv (1) develop and implement post-specific guidance on federal recordkeeping responsibilities, including the definition of what types of electronic messaging communications must be retained to comply with federal records retention requirements as well as direction on how to preserve records received or created on electronic messaging platforms and (2) develop and implement a procedure to periodically communicate the guidance to post personnel and keep the guidance updated on Embassy Kyiv's SharePoint page.

**Recommendation 3:** (U) OIG recommends that U.S. Embassy Kyiv develop and implement internal controls to ensure that post records management officials routinely liaise with post sections on records management requirements, remain aware of the extent to which electronic messaging applications are used to conduct Department of State (Department) business, and implement internal policies to promote the preservation of records on electronic messaging platforms in accordance with Department requirements.

**Recommendation 4:** (U) OIG recommends that the Bureau of Administration, in coordination with the Bureau of Diplomatic Technology and Bureau of Diplomatic Security, assess the extent to which electronic messaging applications, including Signal, are used at posts worldwide to conduct Department of State business.

**Recommendation 5:** (U) OIG recommends that the Bureau of Administration, in coordination with the Bureau of Diplomatic Technology and Bureau of Diplomatic Security, determine the availability of acceptable alternative procedures and methods for preserving federal records from electronic messaging applications by (1) identifying alternative methods for preserving records from electronic messaging applications without export functions and (2) determining whether replicating electronic messaging correspondence in cables, emails, or official reports is an acceptable alternative means of preserving records of these communications.

**Recommendation 6:** (U) OIG recommends that, if alternative procedures and methods for preserving federal records from electronic messaging applications are identified following implementation of Recommendation 5, the Bureau of Administration update the guidance for retaining electronic messages in the Foreign Affairs Manual and Records Guidance for Electronic Messages accordingly.

**Recommendation 7:** (U) OIG recommends that, following the implementation of Recommendations 4, 5, and 6, the Bureau of Administration, in coordination with the Bureau of Diplomatic Technology and Bureau of Diplomatic Security, reevaluate the general prohibition

on certain electronic messaging applications and update the Foreign Affairs Manual accordingly.

## (U) APPENDIX A: PURPOSE, SCOPE, AND METHODOLOGY

---

(U) The Office of Inspector General (OIG) conducted this audit to determine whether U.S. Embassy Kyiv, Ukraine, had implemented measures to preserve federal records created using electronic messaging (eMessaging) applications.

(U) OIG conducted this audit from May 2024 to December 2024 in the Washington, DC, metropolitan area and at U.S. Embassy Kyiv, Ukraine. OIG interviewed personnel from every Department of State (Department) section at Embassy Kyiv to determine (1) whether Embassy Kyiv management implemented measures to ensure federal records retention, (2) the extent to which eMessaging applications were used to conduct Department business, and (3) whether personnel were complying with electronic message retention requirements.

(U) OIG conducted this performance audit in accordance with generally accepted government auditing standards. These standards require that OIG plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objective. OIG believes that the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objective. This report relates, in part, to Overseas Contingency Operation Atlantic Resolve and was completed in accordance with OIG's oversight responsibilities described in Section 419 of the Inspector General Act of 1978, as amended.<sup>1,2</sup>

(U) OIG reviewed relevant requirements outlined in federal laws, the Department's Foreign Affairs Manual, the Bureau of Administration, Records and Archive Management Division's "Records Guidance for Electronic Messages," and Embassy Kyiv communications, including Management Notices and Security Notices. OIG also obtained, reviewed, and analyzed correspondence between Embassy Kyiv and the Bureau of Administration regarding authorization to use Signal for Department business.

(U) To determine to what extent and in what manner Embassy Kyiv had used eMessaging applications and the extent to which embassy personnel were complying with federal retention requirements when using eMessaging applications, OIG interviewed representatives from each of the Department sections at Embassy Kyiv. In total, OIG interviewed 12 staff members from 9 Department sections and offices at Embassy Kyiv.

(U) To understand Department requirements and guidance regarding the use of eMessaging applications, OIG interviewed personnel from the Bureau of Administration, Records and Archives Management Division (A/RA); the Bureau of Diplomatic Technology, including the Endpoint Engineering Services Division and the Enterprise Center Operations Center; and the Bureau of Diplomatic Security, Cyber Threat Analysis Division. Furthermore, OIG coordinated its

---

<sup>1</sup> (U) 5 United States Code § 419, "Special provisions concerning overseas contingency operations."

<sup>2</sup> (U) Operation Atlantic Resolve is the U.S. contingency operation to deter Russian aggression against NATO and to reassure and bolster the alliance in the wake of Russia's 2022 full-scale invasion of Ukraine.

work with other OIGs conducting oversight work related to Ukraine through participation in the OIG Ukraine Oversight Interagency Working Group.

(U) OIG conducted 12 interviews across 9 Department sections and offices at Embassy Kyiv to determine whether Department personnel had preserved federal records directly from Signal, whether personnel knew how to preserve records from Signal, and whether personnel were aware of any measures implemented by Embassy Kyiv management to reinforce the requirement to preserve federal records from Signal. Specifically, OIG interviewed personnel from Embassy Kyiv's Management section, Consular section, Political section, Economics section, Public Affairs section, Regional Security Office, International Narcotics and Law Enforcement office, the Assistance Coordination office, and the Front Office including the Deputy Chief of Mission.

(U) OIG conducted interviews with each section independently to corroborate information regarding the extent to which Signal was used at post, in what manner Signal was used, what challenges personnel encountered using Signal, and whether Embassy Kyiv had sufficiently communicated records retention procedures to personnel at post. OIG also obtained and reviewed embassy communications, including embassy Security Notices and Management Notices distributed since April 2022, to corroborate information provided by Embassy Kyiv personnel. Because the audit team interviewed personnel representing all Department sections and offices at Embassy Kyiv, OIG did not develop a sampling plan.

### **(U) Data Reliability**

(U) OIG used computer-processed information provided by A/RA and Embassy Kyiv as part of its audit evidence. However, OIG could not independently obtain encrypted Signal correspondence or chat records from Department personnel. OIG requested examples of attempts to preserve federal records when Embassy Kyiv personnel indicated to OIG that they had retained records from Signal in accordance with Department guidance. OIG also relied on self-reports from personnel in each section regarding their use of Signal for security-related communications, transitory messages, and to conduct day-to-day Department business. Overall, OIG determined that the information it relied on was sufficient and appropriate to answer the audit objective.

### **(U) Work Related to Internal Control**

(U) OIG considered a number of factors, including the subject matter of the audit, to determine whether internal control was significant to the audit objective. Based on its consideration, OIG determined that internal controls were significant for this audit. OIG then considered the components of internal control and the underlying principles included in *Standards for Internal Control in the Federal Government*<sup>3</sup> to identify internal controls that were significant to the audit objective. Considering internal control in the context of a comprehensive internal control

---

<sup>3</sup> (U) Government Accountability Office, *Standards for Internal Control in the Federal Government* (GAO-14-704G, September 2014).

framework can help auditors to determine whether underlying internal control deficiencies exist.

(U) For this audit, OIG concluded that four of five internal control components from the *Standards for Internal Control in the Federal Government*—Risk Assessment, Control Activities, Information and Communication, and Monitoring—were significant to the audit objective. The Risk Assessment component assesses the risks facing the entity as it seeks to achieve its objectives. This assessment provides the basis for developing appropriate risk responses. The Control Activities component includes the actions management establishes through policies and procedures to achieve objectives and respond to risks in the internal control system, which includes the entity’s information system. The Information and Communication component relates to the quality information that management and personnel communicate and use to support the internal control system. The Monitoring component relates to activities management establishes and operates to assess the quality of performance of the internal control system over time and promptly resolve the findings of audits and other reviews. OIG also concluded that four of the principles related to the selected components were significant to the audit objective, as described in Table A.1.

**(U) Table A.1: Internal Control Components and Principles Identified as Significant**

<b>(U) Components</b>	<b>(U) Principles</b>
Risk Assessment	Management should identify, analyze, and respond to risks related to achieving the defined objectives.
Control Activities	Management should design control activities to achieve objectives and respond to risks.
Information and Communication	Management should internally communicate the necessary quality information to achieve the entity’s objectives.
Monitoring	Management should establish and operate activities to monitor the internal control system and evaluate the results.

**(U) Source:** Generated by OIG from an analysis of internal control components and principles from the Government Accountability Office, *Standards for Internal Control in the Federal Government* (GAO-14-704G, September 2014).

(U) OIG reviewed Department policies, interviewed personnel at Embassy Kyiv, analyzed Department procedures and guidance for electronic messages, and reviewed internal Embassy Kyiv communications to gain an understanding of the internal controls related to the components and principles identified as significant for this audit. Specifically:

- (U) To determine whether Embassy Kyiv identified, analyzed, and responded to risks related to the preservation of federal records on eMessaging platforms, OIG:
  - (U) Surveyed Embassy Kyiv personnel to identify all sections that were using Signal to conduct critical mission and programmatic communication.
  - (U) Interviewed Embassy Kyiv personnel to assess the extent to which they were complying with established Department procedures for preserving messages on Signal.

- (U) Reviewed relevant Embassy Kyiv communications, including Management Notices and Security Notices, as well as correspondence between Embassy Kyiv and the Bureau of Administration.
- (U) Interviewed Embassy Kyiv records management officials to determine whether they had identified and analyzed the risks associated with embassy personnel using Signal extensively to conduct critical communications and preserve records in accordance with Department requirements and, if so, what measures they might have taken to mitigate those risks.
- (U) To determine whether the Department identified, analyzed, and responded to risks related to the usage of Signal at posts overseas, OIG:
  - (U) Interviewed Department officials to identify the challenges of complying with established Department procedures for preserving messages on Signal.
  - (U) Reviewed correspondence between Embassy Kyiv and Bureau of Administration officials.
  - (U) Met with officials from the Bureau of Administration and the Bureau of Diplomatic Technology to determine the extent to which eMessaging applications were being used by Department personnel worldwide and to determine whether the Department had identified and analyzed the risks associated with posts' growing use of eMessaging platforms.
- (U) To determine whether Embassy Kyiv instituted measures to preserve federal records created using eMessaging applications, OIG:
  - (U) Interviewed the officials designated with records management program responsibilities to identify measures instituted at Embassy Kyiv related to eMessaging record retention.
  - (U) Interviewed Embassy Kyiv personnel to determine whether they were aware of formal policies or procedures on how to comply with federal recordkeeping requirements when using eMessaging platforms.
- (U) To determine whether Embassy Kyiv internally communicated measures to preserve federal records created using eMessaging applications, OIG:
  - (U) Reviewed embassy Management Notices and Security Notices to determine whether Embassy Kyiv communicated Department policies, procedures, and guidance on records management for electronic messages.
  - (U) Analyzed an April 2024 Embassy Kyiv Management Notice to identify how Signal was authorized for use and to identify the guidance for the preservation of records from eMessaging platforms.
- (U) To determine whether Embassy Kyiv established and operated activities to monitor the effectiveness of its measures to preserve federal records, OIG:
  - (U) Interviewed Embassy Kyiv personnel to evaluate how the Post Records Coordinator at the embassy had assessed compliance with federal recordkeeping requirements for personnel using eMessaging platforms.
  - (U) Interviewed Embassy Kyiv personnel to determine whether they were aware of any follow-up being done by the embassy to determine compliance with records retention policy and guidance.

(U) Internal control deficiencies identified during the audit that are significant within the context of the audit objective are presented in the Audit Results section of this report.

### **(U) Prior Office of Inspector General Reports**

**(U) *Management Assistance Report: Remote Missions Face Challenges Maintaining Communications With Locally Employed Staff and Host Country Government Officials (AUD-MERO-21-16, March 2021)***. OIG reported that U.S. direct hire staff at the Yemen Affairs Unit, Venezuela Affairs Unit, and at Embassy Mogadishu relied on the use of electronic messaging applications to communicate with locally employed staff and government officials in the host country. This occurred even though the staff did not always archive messages in accordance with Department guidance and federal recordkeeping requirements. OIG made one recommendation on this matter and closed the recommendation after the Bureau of Administration issued eMessaging guidance in 2021.

## (U) APPENDIX B: U.S. EMBASSY KYIV, UKRAINE, RESPONSE

---



*Embassy of the United States of America*

*Kyiv, Ukraine*

UNCLASSIFIED

January 14, 2024

Samantha Carter  
Director  
Global Emergencies and Emerging Risks  
Office of the Inspector General  
U.S. Department of State  
1700 North Moore Street  
Arlington, VA 22209

Dear Ms. Carter:

Thank you for the opportunity to respond to the draft report, “Audit of U.S. Embassy Kyiv, Ukraine, Records Retention for Electronic Messaging.” I appreciate the extensive work of the audit team, and the specific recommendations provided. These insights will help the U.S. Embassy in Kyiv, and the broader operations of the U.S. Department of State, achieve greater effectiveness in our compliance with federal records retention efforts, as we continue to strive to be a first-in-class mission, advancing U.S. priorities on the frontlines of one of the most critical foreign policy challenges of our time. This has been one of the top five goals of our mission since my arrival in May 2022, during the first months of Russia’s war in Ukraine.

I also appreciated OIG’s recognition of eMessaging records management as a global issue, as I was to see the recognition of limitations imposed by the current operating criteria and guidance. Embassy Kyiv is not the only

UNCLASSIFIED



-2-  
UNCLASSIFIED

mission where U.S. diplomatic personnel rely on eMessaging applications to achieve our objectives, nor are eMessaging applications solely the purview of U.S. government employees serving in duty stations beyond the borders of the United States. As the report notes, appropriate retention of federal records is a required element of our work as federal employees, as is my unflinching commitment to the safety of my team, serving in a wartime environment where missile and drone attacks are regular occurrence. I concur with the OIG's conclusion that the guidance for retaining federal records on eMessaging applications warrants updating and revision, that the guidance is out-of-date, and that it is potentially a source of vulnerability for our operational security. It is with these risks in mind that we have crafted a whole-of-government effort to strategically minimize the risk to all embassy personnel, an effort which has benefited from the incorporation of the Signal messaging application.

My first and foremost priority is the safety of my personnel and the security of my mission. The Emergency Action Committee, which advises Department leadership on the security situation in Ukraine, has recommended Signal as the eMessaging platform best suited for our current needs, because of its protection in the current counterintelligence environment in Ukraine. I have accepted its recommendation to incorporate Signal as part of our overarching risk mitigation strategy, which includes dynamic phone applications, movement restrictions, and other security protocols designed and implemented to ensure the safety and efficacy of all USG personnel serving in Ukraine.

In addition to ensuring the safety of our team, I have prioritized building a top-class mission in Ukraine. This includes our commitment to productive outcomes with our OIG colleagues working under Chief of Mission authority

UNCLASSIFIED

-3-  
UNCLASSIFIED

here in Kyiv, with visiting OIG and GAO leadership, and with evaluation teams, as well as with the beneficial recommendations from resulting evaluations. This is the right position and the only one that ensures our operation as the first-in-class mission we seek to be. This priority is also essential given the pace of operations in Kyiv. The U.S. Embassy in Kyiv operates at the unyielding pace necessary to advance U.S. priorities in an active war zone, supporting our Ukrainian partners to counter Russia's unwarranted and unjust war of aggression against a country of 80 million people. Since the embassy resumed operations in Kyiv in May 2022, my team has facilitated 24 Cabinet-level visits, the first Presidential visit in 14 years, and 27 Congressional delegations.

With this context in mind, Embassy Kyiv would like to offer the following additional insights, context, and suggestions to this report to the recommendation for action on the embassy's behalf:

**Recommendation 1:** OIG recommends that U.S. Embassy Kyiv officially designate a post records coordinator to regularly review post's records management practices and liaise with embassy sections on records management requirements, as required by 5 Foreign Affairs Manual 418.9.

**Embassy Kyiv Response:** Embassy Kyiv concurs with the recommendation and designated a post records coordinator on 25 Nov 2024, prior to release of the draft report. Following the Department's current guidance for records management practices, the post record coordinator has drafted – and the embassy has adopted – a post standard operating procedure (SOP) outlining current guidance and practical application for all embassy personnel. This includes establishing an annual schedule for review and

UNCLASSIFIED

-4-  
UNCLASSIFIED

re-distribution of post's approved practices to ensure broad understanding and adoption of the most current requirements, criteria, and responsibilities among all embassy sections. We further welcome this outcome, as having an established SOP is essential for a post with both one-year tour rotations and a cap on overnight staffing. The Embassy's Management team, including Diplomatic Technology, has been sorely understaffed since the Embassy's reopening under Ordered Departure status on May 18, 2022. I have raised this concern in multiple cables to the Department.

**Recommendation 2:** OIG recommends that U.S. Embassy Kyiv (1) develop and implement post-specific guidance on federal recordkeeping responsibilities, including the definition of what types of electronic messaging communications must be retained to comply with federal records retention requirements as well as direction on how to preserve records received or created on electronic messaging platforms and (2) develop and implement a procedure to periodically communicate the guidance to post personnel and keep the guidance updated on Embassy Kyiv's SharePoint page.

**Embassy Kyiv Response:** Embassy Kyiv concurs with the recommendation and has already addressed both the need for clear post-specific guidance on recordkeeping responsibilities, including adopting SOPs outlining processes to ensure updates and distribution of the guidance and definition of what types of electronic messaging communications must be retained. Further, the SOP – as described above – includes procedures to ensure regular updates, communication, and dissemination of both current requirements and record preservation methods for fully unclassified records through multiple channels, including Signal, and alongside all other security and management notices on the Embassy's SharePoint platform.

UNCLASSIFIED

-5-  
UNCLASSIFIED

**Recommendation 3:** OIG recommends that U.S. Embassy Kyiv develop and implement internal controls to ensure that post records management officials routinely liaise with post sections on records management requirements, remain aware of the extent to which electronic messaging applications are used to conduct Department business, and implement internal policies to promote the preservation of records on electronic messaging platforms in accordance with Department requirements.

**Embassy Kyiv Response:** Embassy Kyiv concurs with the recommendation. As part of the adopted SOPs described above, the Post Management Officer and Records Coordinator now have clearly defined responsibilities to provide oversight and guidance and to remind post personnel of their record disposition responsibilities as described in 5 FAM 418.9 and subsequent sections and to advise personnel on both internal policies and best practices to promote the preservation of eMessaging records in line with the latest Departmental guidance on both records retention and operational security.

Sincerely,



Bridget A. Brink  
Ambassador

UNCLASSIFIED

## (U) APPENDIX C: BUREAU OF ADMINISTRATION RESPONSE

---




United States Department of State

Washington, DC 20520

UNCLASSIFIED

January 16, 2024

TO: Office of Inspector General

FROM: A/SKS – Timothy Kootz 

SUBJECT: Audit of Embassy Kyiv, Ukraine, Records Retention for Electronic Messaging, AUD-GEER-25-XX

The Bureau of Administration (A Bureau) has reviewed the draft OIG Audit of Embassy Kyiv, Ukraine (AUD-GEER-25-XX). A Bureau concurs with the OIG's recommendations and provides the following comments in response:

**Recommendation 4:** OIG recommends that the Bureau of Administration, in coordination with the Bureau of Diplomatic Technology and Bureau of Diplomatic Security, assess the extent to which electronic messaging applications, including Signal, are used at posts worldwide to conduct Department of State business.

**Management Response:** A Bureau concurs with the recommendation.

**Recommendation 5:** OIG recommends that the Bureau of Administration, in coordination with the Bureau of Diplomatic Technology and Bureau of Diplomatic Security, determine the availability of acceptable alternative procedures and methods for preserving federal records from electronic messaging applications by (1) identifying alternative methods for preserving records from electronic messaging applications without export functions and (2) determining whether replicating electronic messaging correspondence in cables, emails, or official reports is an acceptable alternative means of preserving records of these communications.

**Management Response:** A Bureau concurs with the recommendation.

**Recommendation 6:** OIG recommends that, if alternative procedures and methods for preserving federal records from electronic messaging applications are identified following implementation of Recommendation 5, the Bureau of Administration update the guidance for retaining electronic messages in the Foreign Affairs Manual and Records Guidance for Electronic Messages accordingly.

**Management Response:** A Bureau concurs with the recommendation.

**Recommendation 7:** OIG recommends that, following the implementation of Recommendations 4, 5, and 6, the Bureau of Administration, in coordination with the Bureau of Diplomatic Technology and Bureau of Diplomatic Security, reevaluate the general prohibition on certain electronic messaging applications and update the Foreign Affairs Manual accordingly.

**Management Response:** A Bureau concurs with the recommendation and will update the FAM accordingly.

## (U) ABBREVIATIONS

---

A/RA	Bureau of Administration, Records and Archives Management Division
DS	Bureau of Diplomatic Security
eMessages	Electronic Messages
eMessaging	Electronic Messaging
FAM	Foreign Affairs Manual
OIG	Office of Inspector General



## **HELP FIGHT** FRAUD, WASTE, AND ABUSE

1-800-409-9926

[Stateoig.gov/HOTLINE](https://stateoig.gov/HOTLINE)

If you fear reprisal, contact the  
OIG Whistleblower Coordinator to learn more about your rights.

[WPEAOmbuds@stateoig.gov](mailto:WPEAOmbuds@stateoig.gov)