Office of Inspector General
United States Department of State

AUD-MERO-21-16 Office of Audits March 2021

(U) Management Assistance Report: Remote Missions Face Challenges Maintaining Communications With Locally Employed Staff and Host Country Government Officials

MANAGEMENT ASSISTANCE REPORT

CONTENTS

(U) Summary of Review

(U) In the event of a natural disaster, political instability, or other security threats, the Department of State (Department) may decide to evacuate an embassy and establish operations in a separate location known as a "remote mission," often in another country, for an indefinite period of time. Remote missions include the Yemen Affairs Unit (YAU), which is operating remotely from the U.S. Embassy in Riyadh, Saudi Arabia; the Venezuela Affairs Unit (VAU), which is operating remotely from the U.S. Embassy in Bogota, Colombia; and Embassy Mogadishu, Somalia, which began operating remotely from the U.S. Embassy in Nairobi, Kenya, but now mostly operates from the Mogadishu International Airport in Somalia.

(U) While U.S. direct hire staff typically relocate to the location where the remote mission has been established, locally employed (LE) staff remain in the host country to support the remote mission. In some instances, after an embassy's closure, LE staff perform their duties working remotely from their homes.

(U) During an audit of remote missions, which is currently underway, the Office of Inspector General (OIG) identified challenges remote missions encounter communicating with LE staff and host country officials. This Management Assistance Report is intended to provide early reporting on those challenges to prompt timely corrective action. First, LE staff who remain behind in the host country often lose access to OpenNet, the Department's computer network, following the suspension of operations. Second, it may not be possible to provide remote access to OpenNet to those LE staff working remotely or teleworking from home following the suspension of operations due to information security concerns.

~~(SBU)~~ OIG also found that U.S. direct hire staff at the YAU, the VAU, and Embassy Mogadishu rely on the use of electronic messaging applications, (b) (3) (B), (b) (7)(E), (b) (7)(F) to communicate with LE staff in the host country, as well as with host country government officials in order to continue diplomatic relations. According to YAU and VAU officials, use of these applications was adopted out of necessity because they are often the only feasible mode of communication available. Further, in some instances, host country government officials prefer to use specific electronic messaging applications over others. For example, Venezuelan interim government and Somali government officials prefer to use (b) (3) to communicate because they perceive it to be a more secure application as (b) (3) (B), (b) (7)(E), (b) (7)(F) However, the use of these applications does not always align with Department guidance, which, among other things, is designed to safeguard sensitive information and promote compliance with Federal record-keeping requirements.

(U) To address the challenges faced by remote missions, OIG recommends that the Department establish guidance and procedures to ensure posts develop contingency plans for remote missions, including providing LE staff with continued access to OpenNet when feasible so they can carry out their assigned job duties following the suspension of operations. OIG also recommends that the Department update its policies and guidance to ensure the use of specific electronic messaging applications aligns with the unique needs of remote missions while simultaneously protecting sensitive information and fulfilling Federal record-keeping requirements.

(U) OIG made four recommendations that are intended to address the challenges identified in this report. On the basis of responses from the Bureaus of Diplomatic Security, Administration, Information Resource Management, and the Foreign Service Institute, OIG considers all four recommendations resolved, pending further action. A synopsis of management's comments to the recommendations offered and OIG's reply follow each recommendation in the Results section of this report. Management's responses to a draft of this report are reprinted in their entirety in Appendices A through C, respectively.

(U) BACKGROUND

(U) About Remote Missions

To ensure the safety of mission personnel during natural disasters, political instability, or other security threats, the Department may evacuate an embassy or consulate and establish operations in a separate location. Often the new location is in another country, where mission-essential functions continue, and the embassy effectively operates as a "remote mission." Missions that have operated remotely include the Yemen Affairs Unit, the Venezuela Affairs Unit, and Embassy Mogadishu.[1]

- **(U) Yemen Affairs Unit (Remote Mission Site: U.S. Embassy Riyadh, Saudi Arabia) –** In February 2015, the Department suspended operations at the U.S. Embassy in Sana'a, Yemen, due to deteriorating security conditions resulting from the Houthis' takeover of the government.[2] One month later, the Department established the YAU remote mission at the U.S. Consulate in Jeddah, Saudi Arabia, under the Bureau of Near Eastern Affairs.[3] On October 24, 2018, the YAU relocated from Jeddah to the U.S. Embassy in Riyadh, Saudi Arabia.
- **(U) Venezuela Affairs Unit (Remote Mission Site: U.S. Embassy Bogota, Colombia) –** In March 2019, the Department suspended operations at the U.S. Embassy in Caracas, Venezuela, due to security concerns and the deteriorating political situation in the country. On August 5, 2019, the Department established the VAU remote mission at the U.S. Embassy in Bogota, Colombia, under the Bureau of Western Hemisphere Affairs.

[1] (U) Other missions that have operated from secondary locations include Libya, Syria, and Cuba.

[2] (U) The Houthis are an armed Islamic group that emerged in northern Yemen in the 1990s. The Houthi movement is officially called Ansar Allah.

[3] (U) The Department's regional bureaus oversee the U.S. embassies and consulates and coordinate U.S. foreign relations in their respective geographic areas.

- **(U) U.S. Embassy Mogadishu, Somalia (Remote Mission Site: U.S. Embassy Nairobi, Kenya) –** On September 8, 2015, after years of turmoil following the collapse of Somalia's central government in 1991, the Department formally established the U.S. Mission to Somalia, based at Embassy Nairobi, Kenya. In December 2018, the Department designated a facility at the Mogadishu International Airport as a U.S. diplomatic facility under the Bureau of African Affairs, though some support staff continue to be based at Embassy Nairobi.

(U) Personnel at embassies and consulates usually include a combination of direct hires—that is, U.S. citizens who are Civil Service or Foreign Service employees—and LE staff. LE staff are typically citizens of the host country and are employed under the authority of the Chief of Mission. Following an evacuation or suspension of operations, LE staff may remain in the host country and continue to work, depending on the mission's needs.[4] For example, since 2015, LE staff based in Yemen have worked to support the YAU now located at U.S Embassy Riyadh. Similarly, since 2019, LE staff based in Venezuela have worked to support the VAU located at U.S. Embassy Bogota. Moreover, in some instances, after an embassy's closure, LE staff may perform their duties while working remotely or teleworking from their homes in the host country. For both the YAU and VAU, some of the LE staff have been either working remotely or teleworking from their homes due to the closure of the U.S. embassies in both Yemen and Venezuela.

(U) Information Technology Support to Overseas Missions

(U) Staff at remote missions rely on a range of applications, systems, and equipment to execute mission-essential operations. They also rely on several Department bureaus for IT services and support.

(U) Bureau of Diplomatic Security's Directorate of Cyber and Technology Security

(U) The Directorate of Cyber and Technology Security within the Bureau of Diplomatic Security (DS) is responsible for safeguarding the Department's global cyber infrastructure, including computer networks, systems, data, mobile devices, and new technologies at overseas embassies and consulates. This directorate works with the Bureau of Information Resource Management (IRM) to respond to cyber-attacks, insider threats, and other threats to the Department's IT infrastructure.

(U) Bureau of Information Resource Management

(U) IRM is responsible for providing secure communications, networking, and computing platforms to support the Department's mission in the United States and around the world. IRM's Directorate of Information Assurance identifies, develops, implements, and maintains processes across the Department's IT network to reduce cybersecurity risks.

[4] (U) U.S. Embassy Mogadishu does not currently employ any LE staff in Somalia.

The Chief Information Security Officer within this directorate leads efforts to develop and maintain the Department-wide information security program aimed at ensuring the protection of information and information systems. IRM's Office of Mobile and Remote Access provides, administers, and maintains mobile and remote access capabilities for the Department. Additionally, each embassy and post has an IRM section, headed by an Information Management Officer, responsible for managing IT resources and providing support to staff. Further, on October 30, 2020, IRM and the Bureau of Diplomatic Security announced a collaboration to clarify and allocate cyber roles and responsibilities. The two bureaus jointly agreed to appoint an Enterprise Chief Information Security Officer who will be responsible for directing and reporting agency-wide compliance with current and emergent Federal and legislative cybersecurity mandates to Department leadership, Office of Management and Budget, and Congress. The Enterprise Chief Information Security Officer will be responsible for carrying out the Department's interagency and global cybersecurity programs and initiatives.

(U) Bureau of Administration's Office of Information Programs and Services

(U) The Office of Information Programs and Services within the Bureau of Administration's Global Information Services Directorate administers the Department's records management, privacy, classification, declassification, and public access programs. The Office issues guidance on how messages conveyed via email, electronic messaging applications, or other communication mechanisms are archived to comply with Department record-keeping requirements. Specifically, the Foreign Affairs Manual (FAM), states that the Department's activities executed via electronic messaging must be archived within 20 days.[5]

(U) Bureau of Global Talent Management's Office of Overseas Employment

(U) The Bureau of Global Talent Management's Office of Overseas Employment (GTM/OE) establishes policies regarding the employment of LE staff and provides support to overseas posts on a variety of LE employment issues. In addition to establishing and administering policies and regulations relating to recruitment, employment, compensation, performance management, recognition, discipline, separation, and retirement of LE staff, GTM/OE also provides policy interpretations and procedural guidance to overseas missions, including researching and resolving labor relations issues and disputes. Department guidance regarding the oversight and management of LE staff at remote missions is broadly outlined in a 2017 policy issued by GTM/OE, *Policy on Employment of Locally Employed Staff (LE) at U.S. Missions in Suspended Operations Status*.

[5] (U) 5 FAM 444.2c(1), "Communications Via Non-Government Messaging Applications and Platforms."

(U) Purpose of This Management Assistance Report

(U) This management assistance report is intended to provide early reporting on deficiencies identified during OIG's audit of remote diplomatic missions, which is currently underway. The primary objective of the broader audit is to determine whether the Department has instituted adequate protocols to (1) inform the decision to establish a remote diplomatic mission, (2) identify and provide resources to support mission-essential functions, (3) guide daily operations, and (4) evaluate and mitigate risks associated with the execution of foreign assistance programs that are overseen remotely. OIG conducted this performance audit in accordance with generally accepted government auditing standards. Those 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 objectives. OIG faced challenges in completing this work because of the COVID-19 pandemic. These challenges included limitations on in-person meetings, difficulty accessing information, prohibitions on travel, and related difficulties within the Department that affected its ability to respond to OIG requests for information in a timely manner. Despite the challenges, OIG believes that the evidence obtained provides a reasonable basis for the findings and conclusions presented in this report. This report relates, in part, to Overseas Contingency Operations and was completed in accordance with OIG's oversight responsibilities described in Section 8L of the Inspector General Act of 1978, as amended.

(U) RESULTS

(U) Finding A: Early Planning for the Activation of Remote Missions Is Critical in Addressing Communication Challenges With Locally Employed Staff

(U) OIG identified challenges encountered by LE staff working in the host country in support of the remote mission. Specifically, LE staff who remain behind in the host country often lose access to OpenNet, the Department's computer network, following the suspension of operations. Further, it may not be possible to provide remote access to OpenNet to those LE staff working remotely or teleworking from home following the suspension of operations due to information security concerns. To address these challenges, OIG recommends that the Department establish guidance and procedures to ensure posts develop contingency plans and prepare for the activation of remote missions, including plans for providing LE staff with continued access to OpenNet when feasible so that they are able to carry out their assigned job duties following the suspension of operations.

(U) Information Security Concerns May Impact Whether Locally Employed Staff Can Be Provided with Remote Access to the Department's Network

(U) Current policies governing remote access (i.e., accessing OpenNet from a location outside of a post such as from a staff member's home) to OpenNet are established in the Foreign Affairs

Handbook (FAH).[6] LE staff are permitted to have remote access to OpenNet, but the decision to grant remote access is generally made on a case-by-case basis.[7] Specifically, a Counterintelligence Working Group[8] must approve each post's participation in the remote access program. It is then up to management and the Regional Security Officer (RSO) to work together with IRM and other stakeholders at each post to consider security threats before approving a specific account request. In the case of both Yemen and Venezuela, security concerns led to the decision not to grant LE staff remote access to OpenNet. Specifically, the RSO at the YAU stated that providing LE staff with remote access to OpenNet presents a security threat and could place Department information at risk because it is not uncommon for LE staff in Yemen to be monitored or detained by the Houthis. Similarly, the RSO for the VAU also noted security concerns as the primary reason for not giving LE staff in Caracas remote access to OpenNet following the suspension of operations in 2019.

(U) Nevertheless, IRM officials stated that because of the COVID-19 pandemic, IRM has made OpenNet accessible to thousands of U.S. direct hire and LE staff working from home. Specifically, the Department has developed new tools and flexibilities to make it easier for all Department staff, including LE staff, to work remotely. For example, IRM recently enabled additional proxy services that allow users to access OpenNet applications through the Global OpenNet Browser, one of the Department's remote access platforms. IRM has also enabled several new methods to allow users to access OpenNet remotely. For example, staff may be given remote access to OpenNet using soft tokens[9] or multifactor authentication applications[10] installed on an individual's phone. Finally, IRM officials noted that it may be possible to grant LE staff partial or limited access to OpenNet in those countries where security concerns may otherwise restrict full access to OpenNet.

(U) IRM officials stated that it is possible that some of the tools developed in response to the COVID-19 pandemic could potentially be extended to LE staff working at posts in suspended operations status. However, IRM officials stated that it is easier to establish multifactor authentication and provide LE staff with other tools, equipment, services, and support needed to facilitate their ability to work remotely prior to the suspension of operations. Specifically, prior to the suspension of operations, LE staff would still have direct access to Department IT systems and support personnel needed to assist them with facilitating their ability to work from home. However, for this to occur successfully, contingency planning to prepare for the

[6] (U) Remote access to Department networks, either domestically or abroad is outlined in 12 FAH-10 H-174, "Remote Access."

[7] (U) For example, at posts that are categorized as "Critical Technical and/or Critical Human Intelligence Threat," LE staff are prohibited from having remote access to OpenNet. However, a DS official stated that if remote access for LE staff is determined to be necessary, then the post may request an exception to the rule.

[8] (U) 12 FAH-10 H-174.1a,b(2)(a), "Remote Access – Management Responsibilities."

[9] (U) A soft token delivers a PIN number using software on Department-approved mobile devices.

[10] (U) Multifactor authentication requires two or more methods for users to log into a given account. For example, users might enter a username and password as a first step and then as a second step, enter a number, code, or confirmation generated by an application installed on their phone.

activation of remote missions, including developing plans to provide LE staff with continued access to OpenNet, is necessary.

(U) DS is responsible for providing guidance and policy to assist posts with emergency planning. According to 12 FAH-1, "Emergency Planning Handbook," diplomatic missions throughout the world are required to develop an Emergency Action Plan that outlines post-specific procedures for responding to emergency situations,[11] including evacuations and suspensions of operations. Among other things, Emergency Action Plans require posts to have multiple methods of communication that can be used during a crisis and that the Emergency Action Committee in consultation with subject matter experts, should develop plans for alternate, contingency, and emergency communications systems that could be used during a crisis.[12] However, the FAH does not require the Emergency Action Plan to include plans for communicating with LE staff who will remain in the host country and continue to work following a suspension of operations. For example, there is no policy requiring posts to determine whether and how LE staff will maintain access to official Department email systems, nor is there guidance to posts to consider providing LE staff with remote access to OpenNet following the suspension of operations. Furthermore, if security conditions on the ground prohibit providing LE staff with remote access to OpenNet, there is no policy requiring posts to periodically reevaluate the option to grant LE staff remote access to OpenNet even when conditions change.

(U) Loss of Access to the Department's Network Hinders the Ability of Locally Employed Staff to Carry Out Assigned Job Duties

(U) LE staff at overseas posts typically work at the embassy compound and access OpenNet through computers located onsite. However, when operations were suspended and remote missions were established for Yemen and Venezuela, local servers that hosted OpenNet accounts were shut down resulting in LE staff losing access to the Department's internal IT network, including official Department email accounts.[13] U.S. direct hire supervisors at both the YAU and VAU stated that lack of access to the Department's websites, data systems, and applications poses a significant problem because it hinders the extent to which LE staff can effectively and efficiently carry out their day-to-day responsibilities.

[11] (U) See 12 FAH-1 H-031, "General."

[12] (U) 12 FAH-1 H-781b, "Communications and Contingency Planning"; 12 FAH-1, Annex K, "Drawdown and Evacuation." Additionally, there are other sections of the FAH that discuss communications during an emergency. For example, 12 FAH-1 H-730, "Coordination," outlines the responsibility of posts to assemble appropriate contact lists in order to ensure staff can respond effectively to a particular crisis. It refers staff to 2 FAH-2 H-116, which includes guidance on accounting for LE staff during an emergency and directs post to maintain contact information for all staff under Chief of Mission authority as a means to maintain effective communication during an emergency.

[13] ~~(SBU)~~ LE staff in Venezuela were provided with Foreign Affairs Network accounts prior to the suspension of operations in 2019. The Foreign Affairs Network is an alternative, official Department email platform available to staff without OpenNet access. However, LE staff in Yemen were not provided with alternative official email accounts until 2019 and relied on the (b) (7)(F), (b) (7)(E), (b) (3) (B) for the first 4 years after operations were suspended.

(U) For example, an LE staff member supporting the YAU's Public Affairs Section from Yemen stated that he does not have access to the State Assistance Management System (a system Department officials use to help manage grants). Without access to this system, he is unable to directly update information in the system, as required by his job duties, and must instead send grant data to a U.S. direct hire staff who enters information into the system on his behalf. Furthermore, each time he needs information, he must ask a U.S. direct hire staff with OpenNet access to obtain it and provide it to him via his America.gov account.[14] Although he stated that he is grateful for the help provided by the U.S. direct hire staff, he acknowledged that it is time-consuming for them to assist him and is not an efficient or effective way for him to do his work. Similarly, an LE budget analyst and accountant supporting the VAU from Caracas stated that she relies on a variety of internal Department financial applications that can only be accessed through OpenNet to carry out her day-to-day responsibilities. Since the suspension of operations in Caracas, she must prepare information outside of OpenNet and then ask a U.S. direct hire staff with OpenNet access to enter the information into the relevant Department financial data system on her behalf.

(U) A former Management Counselor at the YAU characterized the inability of LE staff to access OpenNet as "the single biggest challenge facing LE staff in Yemen." He provided examples of how the lack of access to OpenNet has also increased the workload of the U.S. direct hire supervisors responsible for overseeing LE staff from the remote mission. For example, he stated that when LE staff in Yemen need to process HR information, the LE staff in Yemen must send the relevant information to the Management Counselor in Riyadh, who transcribes the information into the proper Department form (that can only be accessed via OpenNet) and then submits it on the LE staff's behalf.

(U) The lack of access to OpenNet also hampers LE staff's ability to register and complete required training, as well as training that is key to professional development. The Foreign Service Institute (FSI) is the Department's primary training facility, and its mission includes "developing the skills, knowledge and abilities of Department personnel and preparing them for increased responsibility." Typically, Department personnel register for both in-person training and online courses via the FSI website, which can only be accessed through OpenNet. Without direct access to OpenNet, LE staff at missions in suspended operations are hindered in their ability to register for training through the FSI website.

(U) OIG found that LE staff working in Venezuela could periodically access the FSI website via OpenNet and complete training when visiting the VAU in Bogota or serving on short-term assignments at other embassies and consulates in the region. However, LE staff in Yemen cannot visit the YAU in Saudi Arabia due to travel restrictions. Nonetheless, according to FSI officials, Department personnel who do not have access to OpenNet and the FSI website can

[14] ~~(SBU)~~ In 2019, LE staff in Yemen were provided with America.gov accounts. America.gov is another, alternative official Department email platform typically used by Public Diplomacy staff. However, from 2015 to 2019, LE staff in Yemen did not have access to any official Department email accounts and instead relied on (b) (7)(F), (b) (7)(E), (b) (3) (B) to conduct Department business.

send an email to the FSI registrar requesting enrollment in a specific online course. Once the request is approved, FSI responds to the enrollee via email with a link to the course and logon instructions. Enrollees may then access the online course via any internet connection. Thus, LE staff may take FSI training courses even when they do not have access to OpenNet. However, OIG found that U.S. direct hire supervisors at the YAU, as well as the LE staff supporting the YAU, were unaware of this option.

(U) In a previously issued report, OIG reported that the Office of Overseas Employment within the Bureau of Global Talent Management had issued a policy on LE staff at missions in suspended operations status.[15] The policy states that LE staff may request training to complete their work commitments, but does not offer guidance on how U.S. direct hire supervisors might overcome the challenges specific to remote missions.[16] As a result, OIG recommended that the Office of Overseas Employment develop guidance outlining specific mechanisms for providing LE staff at posts in suspended operations status with ongoing opportunities for training, including those required to fulfill position-specific training requirements and to promote professional development. However, it is also essential that LE staff and their U.S. direct hire supervisors understand the mechanism by which staff without access to OpenNet can access the Department's online training courses.

Recommendation 1: (U) OIG recommends that the Bureau of Diplomatic Security establish and implement a process to perform a fully coordinated, in-depth risk assessment to properly identify and gauge the necessity and benefits of providing remote, OpenNet access to locally employed staff who continue to work in the host country following a suspension of operations, and that it develop and implement guidance for posts on the subsequent steps required when OpenNet access is deemed necessary.

Management Response: (U) DS did not concur with OIG's original recommendation as stated in a draft of this report, "based on the potential counterintelligence risks posed by enabling LE Staff off-site remote access to Department systems and information." DS further stated that "the Department first needs to perform a fully coordinated, in-depth risk assessment to properly identify and gauge the actual necessity and benefits of providing remote, OpenNet access to LE Staff and whether adequate and affordable security controls and counterintelligence countermeasures are available to pursue such an option." DS concluded by noting that, "Should off-site access be deemed necessary, at a minimum, Regional Security Officer counterintelligence awareness/cyber briefing should accompany each OpenNet remote access approval for LE Staff."

OIG Reply: (U) OIG's original recommendation in a draft of this report recommended that the Bureau of Diplomatic Security, in collaboration with the Bureau of Global Talent

[15] (U) OIG, *Management Assistance Report: Additional Guidance Needed to Improve the Oversight and Management of Locally Employed Staff Serving at Remote Missions* 16, 19 (AUD-MERO-20-40, September 2020).

[16] (U) See Bureau of Global Talent Management, Office of Overseas Employment, *Policy on Employment of Locally Employed (LE) Staff at Missions in Suspended Operations* Status, 2017.

Management and the Bureau of Information Resource Management, develop guidance directing posts to develop contingency plans for establishing, supporting, and maintaining locally employed staff who will continue to work in the host country following a suspension of operations. The contingency plans should address how posts will determine (1) whether and how locally employed staff will retain access to official Department of State systems including remote access to OpenNet; (2) whether and how locally employed will be provided equipment to facilitate their ability to work from home; and (3) whether and how locally employed staff will be periodically re-evaluated for being granted remote access to OpenNet in the event that it cannot be given immediately following the suspension of operations.

(U) Although DS did not concur with the original recommendation, the actions outlined in its response to a draft of this report (see Appendix A), when implemented, represent an acceptable alternative that meets the intent of the original recommendation. OIG is therefore modifying the original recommendation and replacing Recommendation 1 to reflect the acceptable alternative actions proposed by DS. As a result, OIG considers the revised recommendation resolved, pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that DS has (1) established and implemented a process to perform a fully coordinated, in-depth risk assessment to properly identify and gauge the necessity and benefits of providing remote, OpenNet access to LE staff who continue to work in the host country a following suspension of operations, and has (2) developed and implemented guidance for posts on the subsequent steps required when OpenNet access is deemed necessary.

Recommendation 2: (U) OIG recommends that the Foreign Service Institute, in coordination with the Bureau of Global Talent Management, establish and communicate guidance and procedures for locally employed staff to gain access to the Department of State's online distance learning courses when access to OpenNet cannot be provided.

Management Response: (U) FSI concurred with the recommendation (see Appendix B), stating that it "will coordinate with [the Bureau of Global Talent Management] to send [a cable to all diplomatic and consular posts] outlining how locally employed staff can enroll in FSI distance learning courses by June 30, 2021."

OIG Reply: (U) In a draft of this report, Recommendation 2 was originally addressed to the Bureau of Global Talent Management, in coordination with FSI. However, following the issuance of a draft of this report and in consultation with both bureaus, OIG agreed to revise Recommendation 2 to make FSI the primary action office. Therefore, on the basis of FSI's concurrence with the recommendation and planned actions, OIG considers the recommendation resolved, pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that FSI has taken action to establish and communicate guidance and procedures for LE staff to gain access to the Department's online distance learning courses when access to OpenNet cannot be provided.

(U) Finding B: Additional Guidance Is Needed to Fulfill Record-Keeping Requirements When Using Electronic Messaging Applications

~~(SBU)~~ U.S. direct hire staff at the YAU, the VAU, and Embassy Mogadishu rely on the use of electronic messaging applications, [redacted] (b) (3) (B), (b) (7)(E), (b) (7)(F) to communicate both with LE staff who continue to work in the host country, as well as host country government officials in order to continue diplomatic relations. According to YAU and VAU officials, the use of these applications was adopted out of necessity because they are often the only feasible mode of communication available and because host country government officials prefer to use them. Further, in some instances, host country government officials prefer to use specific electronic messaging applications over others. However, the use of these applications does not always align with Department guidance, which, among other things, is designed to safeguard sensitive information and promote compliance with Federal record-keeping requirements. To address these challenges, OIG recommends that the Department update its policies and guidance to ensure the use of specific electronic messaging applications aligns with the unique needs of the remote missions while simultaneously protecting sensitive information and fulfilling Federal record-keeping requirements.

(U) Electronic Messaging Applications Are Essential to the Daily Operations of Remote Missions

~~(SBU)~~ The FAM defines an electronic message as "information sent or received between individuals over an electronic communications platform or device," and such messages include "communications sent through text messaging, chat/instant messaging, and other forms of electronic messaging applications available through social media or mobile devices, whether they reside on agency networks and devices, on personal devices, or on networks hosted by third party providers."[17] The FAM further states that Department officials are permitted to conduct business using nonofficial electronic messaging accounts, applications, or platforms if "[t]he application or platform is the only means of communication our partner is willing to use or the primary means that a group of partners is using."[18] In addition, LE staff may use their own personal devices such as smart phones and tablets to access official applications like Department email accounts, as well as messaging applications [redacted] (b) (3) (B), (b) (7)(E), (b) (7), to communicate with their colleagues and counterparts.

~~(SBU)~~ [redacted] (b) (3) (B), (b) (7)(E), are applications that are typically installed on a phone, and allow users to text, chat, and share media, including voice messages and video, with individuals or groups. According to one YAU official, some of his Yemeni contacts communicate exclusively via [redacted] (b) (7)(E), thus requiring him to use the application as well. Similarly, a VAU official stated that almost all of her communications with her contacts in Venezuela are through [redacted] (b) (3) (B), An Embassy Mogadishu official also reported that some Somali government officials do not have email accounts and no established government email address system exists for the Somali

[17] (U) 5 FAM 444.1, "Defining Electronic Messaging (eMessaging)."

[18] (U) 5 FAM 444.2b(1), "Communications Via Non-Government Messaging Applications and Platforms."

government, leading them to rely heavily on the use of electronic messaging applications to communicate with their Somali counterparts.[19]

~~(SBU)~~ YAU and VAU officials also told OIG that they prefer to use (b) (7)(E), (b) (7)(F), (b) (3) (B) for several reasons, including cyber security concerns and to accommodate the preferences of host country government officials. For example, from 2017 to 2019, (b) (7)(E), (b) (7)(F) s a result, some LE staff in Yemen reported that prefer to use (b) (7) for sensitive communications and that they now delete (b) (3) (B), (b) (7)(E), messages that contain any information about Department business from their phones whenever they leave the house (b) (7)(E), (b) (7)(F) Similarly, LE staff in Caracas face security threats (b) (7)(E), (b) (7)(F) As a result, staff in Venezuela have expressed concerns about how the use of certain communications including electronic messaging applications may present an increased risk to the physical safety of LE staff if any of their correspondence should be intercepted by hostile groups. At least one LE staff member in Venezuela noted that she prefers to use (b) (3) for more sensitive conversations. Similarly, a senior Embassy Mogadishu official stated that while they use (b) (3) (B), for most of their text-based correspondence, some of their Somali contacts will only share sensitive information via (b) (3) because they perceive it as a more secure way to communicate. Finally, a senior official at the VAU stated that the Venezuelan interim government prefers to use (b) (3) as the primary communications platform to discuss sensitive information because they also perceive it to be more secure. (b) (3) (B), (b) (7)(E), (b) (7)(F) staff at all three remote missions, as well as their diplomatic counterparts, believe it is a safer platform.

(U) Department Guidance on the Use of Electronic Messaging Applications Is Informed by Information Security Concerns and the Need to Comply With Department Record-Keeping Requirements

~~(SBU)~~ Department policies regarding which applications are allowed is informed primarily by information security concerns and the need for Department personnel to comply with record-keeping requirements.[20] For example, one cable issued by the Secretary in February 2018 and another issued in July 2019 outlined the Department's changing policy regarding the use of (b) (7) In the February 2018 cable, the Secretary noted that (b) (7) is allowed as long as

[19] ~~(SBU)~~ Officials also noted that the COVID-19 pandemic has restricted face-to-face meetings with many of their diplomatic counterparts, further increasing their reliance on electronic messaging applications. Staff at remote missions have also relied on (b) (3) (B), (b) (7)(E), (b) (7)(F) Staff at the VAU stated that they relied on (b) to contact LE staff and other local officials in Venezuela following the suspension of operations in 2019.

[20] (U) See generally 5 FAM 400, "Records Management."

Department record-keeping requirements are met.[21] Specifically, the cable stated that Department personnel must "forward a complete copy of the record to his or her official electronic messaging account withing 20 days." However, in July 2019, the Under Secretary for Management announced that Department personnel are "prohibited from conducting official Department of State business on any electronic messaging application that does not allow methods for archiving content."[22] The notice further states that "[c]urrently, [redacted] is an example of a platform that does not allow this capability and thus is prohibited for use to conduct official business."

~~(SBU)~~ In June 2020, officials from IRM's Office of Mobile and Remote Access implemented a new process for vetting those applications that are used to conduct Department business. According to IRM officials, under the new process, they only prohibit the use of those applications that present a definitive threat to Department IT systems. According to its webpage, as of September 2020, the only four prohibited applications are TikTok, ToTok, FaceApp, and Yandex Taxi. Officials in IRM's Office of Mobile and Remote Access explained that the change is intended to provide overseas missions more flexibility when conducting their day-to-day business. While [redacted] is no longer considered a prohibited application under the new process, officials from the Office of Information Programs and Services within the Bureau of Administration's Global Information Services Directorate stated they still consider [redacted] to be "generally" prohibited because messages in [redacted] cannot be easily forwarded to an official Department email address for record-keeping purposes. For this reason, these officials stated that Department personnel should use [redacted] as a last resort and consult with their office before proceeding with its use.

(U) To address these challenges, the Department should update its policies and guidance to ensure the use of specific electronic messaging applications aligns with the unique needs of the remote missions while simultaneously protecting sensitive information and fulfilling Federal record-keeping requirements.

> **Recommendation 3:** ~~(SBU~~) OIG recommends that the Bureau of Administration, in conjunction with the Bureau of Information Resource Management, update initially and periodically thereafter, as appropriate, its guidance on how to fulfill record-keeping requirements when using specific electronic messaging applications [redacted] to a) align with the unique needs of remote missions, protect sensitive information, and fulfill Federal record-keeping requirements while b) complying with Department of State policies regarding approved and prohibited electronic messaging applications that can/cannot be used to conduct Department of State business.

[21] (U) Cable 18 STATE 11006, "Policy and Procedures for the Use of Electronic Messaging Applications in the Conduct of State Department Business."

[22] (U) Department of State July 10, 2019, announcement 52650, "A Message from the Under Secretary for Management on Electronic Messaging Applications and Other Records Management Responsibilities."

Management Response: (U) The Bureau of Administration did not provide formal comments in response to a draft of this report. However, the bureau responded via email that it "concurs with Recommendation 3 and has no additional comments at this time."

OIG Reply: ~~(SBU)~~ Although the Bureau of Administration did not provide a formal response to a draft of this report, OIG considers the Bureau of Administration's concurrence via email sufficient to consider the recommendation resolved, pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that the Bureau of Administration, in conjunction with IRM, updates initially and periodically thereafter, as appropriate, its guidance on how to fulfill record-keeping requirements when using specific electronic messaging applications (b) (3) (B), (b) (7)(E), (b) (7)(F) [redacted] to a) align with the unique needs of remote missions, protect sensitive information, and fulfill Federal record-keeping requirements while b) complying with Department policies regarding approved and prohibited electronic messaging applications that can/cannot be used to conduct Department business.

(U) OTHER MATTERS

~~(SBU)~~ During the course of the audit, staff at remote missions told OIG that it was challenging to keep up with the latest Department policies regarding which applications are allowed for conducting Department business. They stated that guidance is often found in various internal websites, cables, and notices issued from their management chain at post, and that they sometimes do not know which guidance is most current or which takes precedence. In addition to the changing guidance regarding the use of (b) (3) [redacted] other applications have also been subject to multiple changes in guidance over the last few years. For example, the Department's position on the use of (b) (3) [redacted] has changed over time. Specifically, in 2019, there was no official Department policy on the use of (b) (3) [redacted] In April 2020, the Department issued a notice stating that (b) (7) [redacted] was not authorized for official business,[23] followed by a statement in June 2020 that (b) (3) [redacted] was allowed for official use but only on certain Department devices.

~~(SBU)~~ While IRM's Office of Mobile and Remote Access lists those mobile applications that are prohibited on its webpage, it does not include information on desktop applications like (b) (3) [redacted] nor does it include information on considerations for the use of specific applications, like the fact that users should consult with the Bureau of Administration's Office of Information Programs and Services before using (b) (7) [redacted] An official from Embassy Mogadishu stated that, despite consulting with the Information Management Officer at post, "there is still some murkiness when it comes to understanding which applications are allowed and the conditions that must be considered regarding their use," and he cited (b) (7) [redacted] as an example. An Information Management Officer also reported some confusion over the use of (b) (3) [redacted] and whether a waiver was required for its use, particularly if it is

[23] ~~(SBU)~~ IRM April 9, 2020, Informational Bulletin, "Further guidance to the use of (b) [redacted] as referenced in 20 State 36876."

considered "generally prohibited." With respect to (b) (3) one official at the VAU stated that they previously relied heavily on the use of (b) (3) and the changing guidance on the use of (b) (3) in 2020 "put general communications at the VAU in a state of chaos."

(U) IRM officials stated that it would not be possible to provide guidance on every electronic messaging application available to Department personnel and that inquiries related to the use of specific applications must be handled on a case-by-case basis. OIG recognizes this challenge; however, without clear, relevant, and available guidance, Department personnel at remote missions and LE staff supporting them risk not complying with Department policies that are intended to minimize vulnerabilities.

> **Recommendation 4:** (U) OIG recommends that the Bureau of Information Resource Management establish and maintain a webpage on OpenNet that will be considered the authoritative source for all up-to-date information regarding the use of specific electronic messaging applications and other communication platforms. Once the webpage is established, Department of State personnel should be notified about where the information can be found.
>
> **Management Response:** (U) IRM stated that it concurred with the recommendation (see Appendix C).
>
> **OIG Reply:** (U) On the basis of IRM's concurrence with the recommendation, OIG considers the recommendation resolved, pending further action. This recommendation will be closed when OIG receives and accepts documentation demonstrating that IRM has established a webpage on OpenNet that will be considered the authoritative source for all up-to-date information regarding the use of specific electronic messaging applications and other communications platforms and notified Department personnel about where the information can be found.

(U) RECOMMENDATIONS

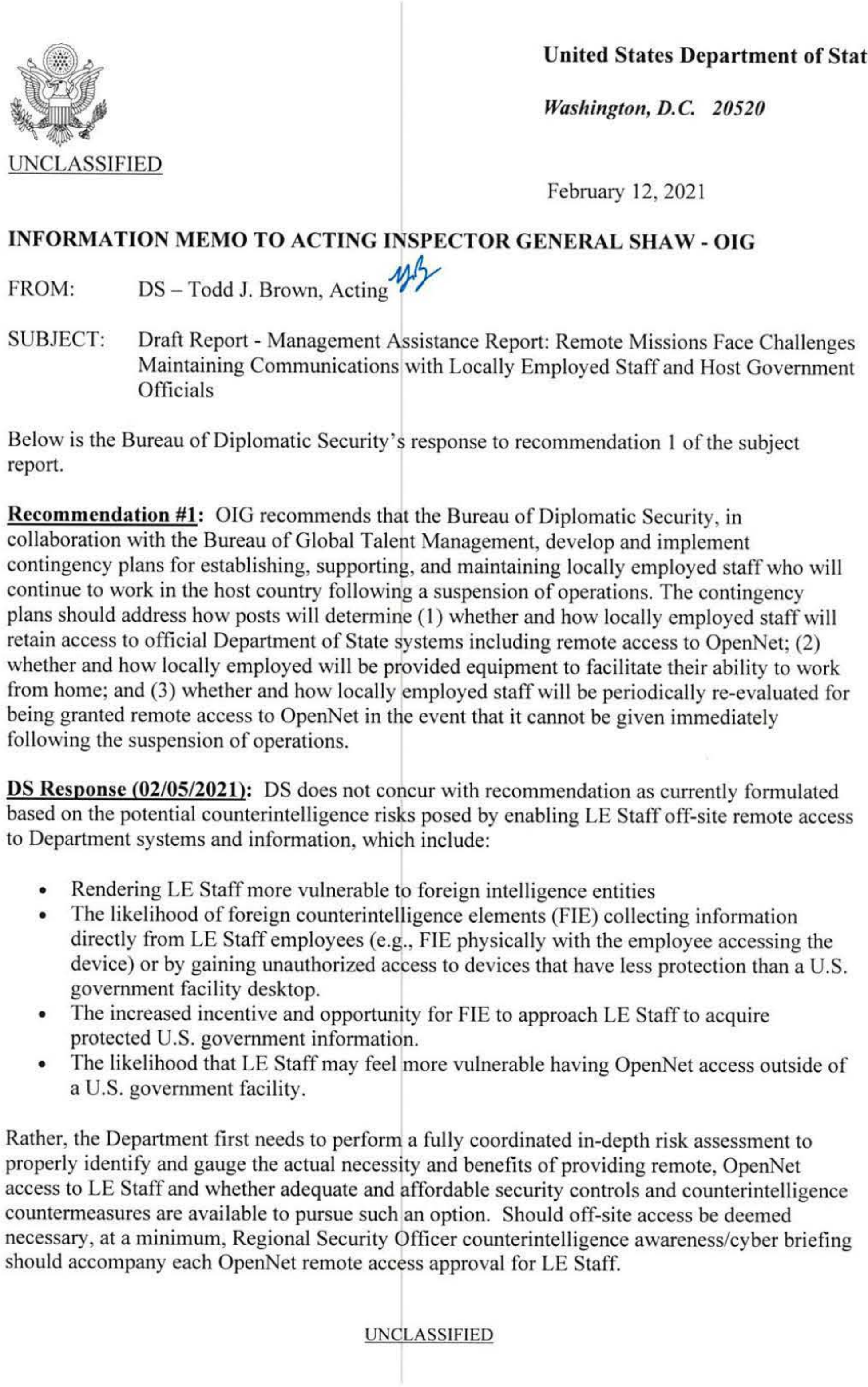
Recommendation 1: (U) OIG recommends that the Bureau of Diplomatic Security establish and implement a process to perform a fully coordinated, in-depth risk assessment to properly identify and gauge the necessity and benefits of providing remote, OpenNet access to locally employed staff who continue to work in the host country following a suspension of operations, and that it develop and implement guidance for posts on the subsequent steps required when OpenNet access is deemed necessary.

Recommendation 2: (U) OIG recommends that the Foreign Service Institute, in coordination with the Bureau of Global Talent Management, establish and communicate guidance and procedures for locally employed staff to gain access to the Department of State's online distance learning courses when access to OpenNet cannot be provided.

Recommendation 3: ~~(SBU)~~ OIG recommends that the Bureau of Administration, in conjunction with the Bureau of Information Resource Management, update initially and periodically thereafter, as appropriate, its guidance on how to fulfill record-keeping requirements when using specific electronic messaging applications (b) (3) (B), (b) (7)(E), (b) (7)(F) [redacted] to a) align with the unique needs of remote missions, protect sensitive information, and fulfill Federal record-keeping requirements while b) complying with Department of State policies regarding approved and prohibited electronic messaging applications that can/cannot be used to conduct Department of State business.

Recommendation 4: (U) OIG recommends that the Bureau of Information Resource Management establish and maintain a webpage on OpenNet that will be considered the authoritative source for all up-to-date information regarding the use of specific electronic messaging applicatins and other communication platforms. Once the webpage is established, Department of State personnel should be notified about where the information can be found.

(U) APPENDIX A: BUREAU OF DIPLOMATIC SECURITY RESPONSE



United States Department of State

Washington, D.C. 20520

UNCLASSIFIED

February 12, 2021

INFORMATION MEMO TO ACTING INSPECTOR GENERAL SHAW - OIG

FROM: DS – Todd J. Brown, Acting

SUBJECT: Draft Report - Management Assistance Report: Remote Missions Face Challenges Maintaining Communications with Locally Employed Staff and Host Government Officials

Below is the Bureau of Diplomatic Security's response to recommendation 1 of the subject report.

Recommendation #1: OIG recommends that the Bureau of Diplomatic Security, in collaboration with the Bureau of Global Talent Management, develop and implement contingency plans for establishing, supporting, and maintaining locally employed staff who will continue to work in the host country following a suspension of operations. The contingency plans should address how posts will determine (1) whether and how locally employed staff will retain access to official Department of State systems including remote access to OpenNet; (2) whether and how locally employed will be provided equipment to facilitate their ability to work from home; and (3) whether and how locally employed staff will be periodically re-evaluated for being granted remote access to OpenNet in the event that it cannot be given immediately following the suspension of operations.

DS Response (02/05/2021): DS does not concur with recommendation as currently formulated based on the potential counterintelligence risks posed by enabling LE Staff off-site remote access to Department systems and information, which include:

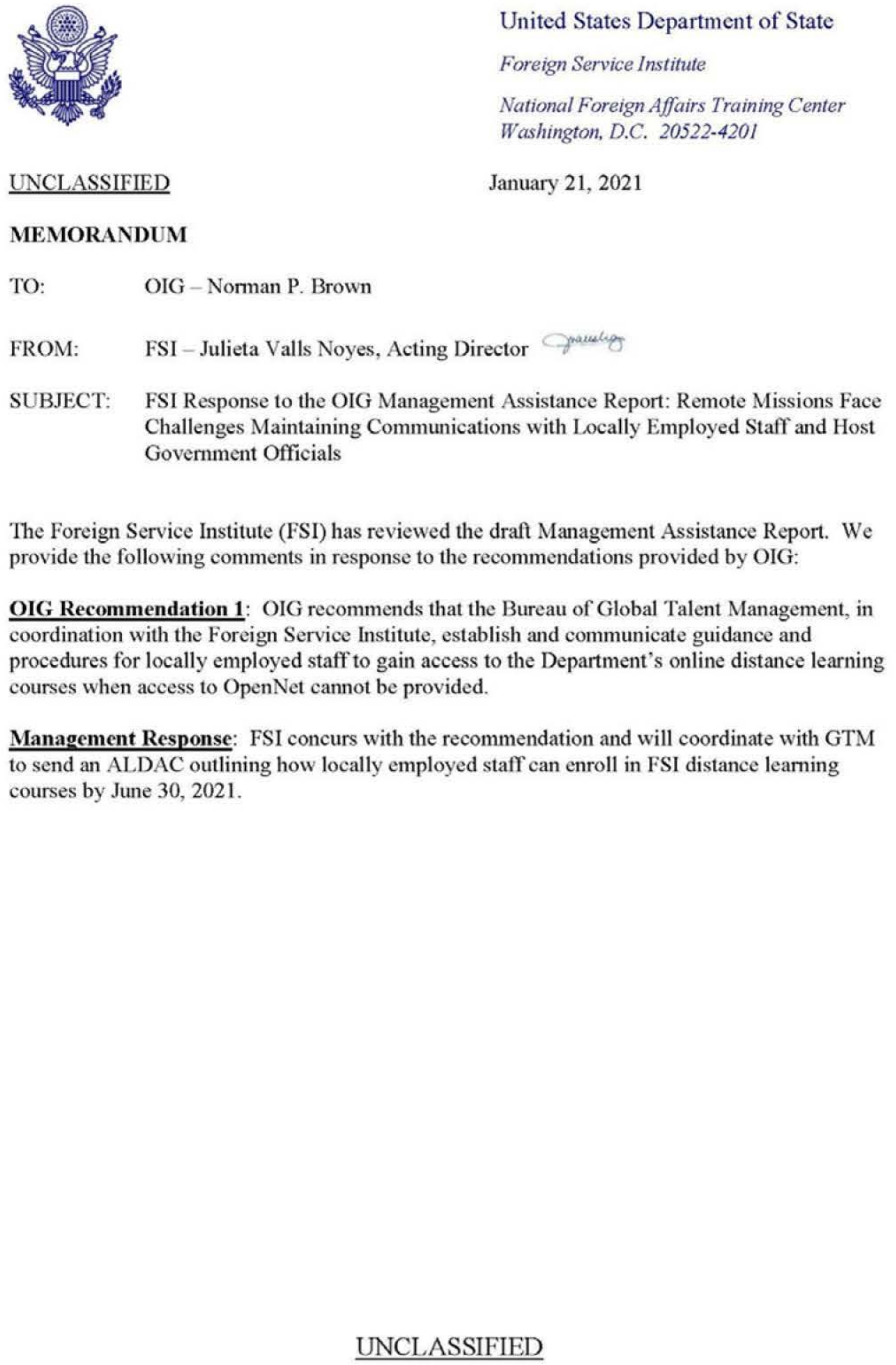
- Rendering LE Staff more vulnerable to foreign intelligence entities
- The likelihood of foreign counterintelligence elements (FIE) collecting information directly from LE Staff employees (e.g., FIE physically with the employee accessing the device) or by gaining unauthorized access to devices that have less protection than a U.S. government facility desktop.
- The increased incentive and opportunity for FIE to approach LE Staff to acquire protected U.S. government information.
- The likelihood that LE Staff may feel more vulnerable having OpenNet access outside of a U.S. government facility.

Rather, the Department first needs to perform a fully coordinated in-depth risk assessment to properly identify and gauge the actual necessity and benefits of providing remote, OpenNet access to LE Staff and whether adequate and affordable security controls and counterintelligence countermeasures are available to pursue such an option. Should off-site access be deemed necessary, at a minimum, Regional Security Officer counterintelligence awareness/cyber briefing should accompany each OpenNet remote access approval for LE Staff.

UNCLASSIFIED

Approved:	DS – Todd J. Brown, Acting	[ ]
Analyst:	DS/MGT/PPD – Peggy Brown	
Cleared:	DS/DSS – CMatus	(OK)
	DS/EX – WTerrini	(OK)
	DS/EX/MGT – JSchools	(OK)
	DS/MGT/PPD – ARanly	(OK)
	DS/MGT/PPD – THouser	(OK)
	DS/HTP - GSherman	(OK)
	M: BPeracchio	(OK)
	M/SS: SCimino	(OK)
	GTM: JMeeks	(OK)

(U) APPENDIX B: FOREIGN SERVICE INSTITUTE RESPONSE



United States Department of State

Foreign Service Institute

National Foreign Affairs Training Center
Washington, D.C. 20522-4201

UNCLASSIFIED

January 21, 2021

MEMORANDUM

TO: OIG – Norman P. Brown

FROM: FSI – Julieta Valls Noyes, Acting Director

SUBJECT: FSI Response to the OIG Management Assistance Report: Remote Missions Face Challenges Maintaining Communications with Locally Employed Staff and Host Government Officials

The Foreign Service Institute (FSI) has reviewed the draft Management Assistance Report. We provide the following comments in response to the recommendations provided by OIG:

OIG Recommendation 1: OIG recommends that the Bureau of Global Talent Management, in coordination with the Foreign Service Institute, establish and communicate guidance and procedures for locally employed staff to gain access to the Department's online distance learning courses when access to OpenNet cannot be provided.

Management Response: FSI concurs with the recommendation and will coordinate with GTM to send an ALDAC outlining how locally employed staff can enroll in FSI distance learning courses by June 30, 2021.

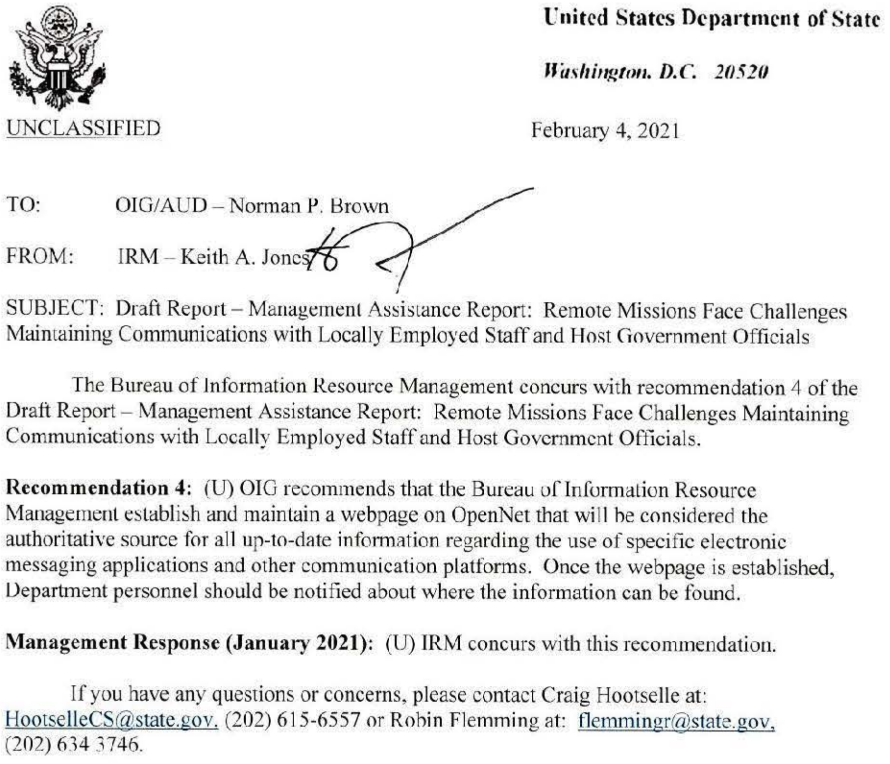
UNCLASSIFIED

Approved: FSI – Joan Polaschik, Acting (JP)

Drafted: Linda Eduful – Edufully@state.gov
Kelly Ozolek Cella – OzolekCellaKR@state.gov

Cleared: FSI/EX – Dominica Gutierrez (OK)
FSI/SPAS – Monique Ramgoolie (OK)
GTM/OE – Anita Brown (OK)

(U) APPENDIX C: BUREAU OF INFORMATION RESOURCE MANAGEMENT RESPONSE



United States Department of State

Washington, D.C. 20520

UNCLASSIFIED

February 4, 2021

TO: OIG/AUD – Norman P. Brown

FROM: IRM – Keith A. Jones

SUBJECT: Draft Report – Management Assistance Report: Remote Missions Face Challenges Maintaining Communications with Locally Employed Staff and Host Government Officials

The Bureau of Information Resource Management concurs with recommendation 4 of the Draft Report – Management Assistance Report: Remote Missions Face Challenges Maintaining Communications with Locally Employed Staff and Host Government Officials.

Recommendation 4: (U) OIG recommends that the Bureau of Information Resource Management establish and maintain a webpage on OpenNet that will be considered the authoritative source for all up-to-date information regarding the use of specific electronic messaging applications and other communication platforms. Once the webpage is established, Department personnel should be notified about where the information can be found.

Management Response (January 2021): (U) IRM concurs with this recommendation.

If you have any questions or concerns, please contact Craig Hootselle at: HootselleCS@state.gov, (202) 615-6557 or Robin Flemming at: flemmingr@state.gov, (202) 634 3746.

(U) OIG AUDIT TEAM MEMBERS

Tinh Nguyen, Division Director
Middle East Region Operations
Office of Audits

Samantha Carter, Audit Manager
Middle East Region Operations
Office of Audits

Angelo Arpaia, Senior Auditor
Middle East Region Operations
Office of Audits

Areeba Hasan, Management Analyst
Middle East Region Operations
Office of Audits

Nina Lin, Senior Auditor
Middle East Region Operations
Office of Audits

Malea Martin, Management Analyst
Middle East Region Operations
Office of Audits

HELP FIGHT

FRAUD, WASTE, AND ABUSE

1-800-409-9926
Stateoig.gov/HOTLINE

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