
Office of Inspector General
United States Department of State

ISP-I-23-23 | Office of Inspections | June 2023

# Inspection of the Bureau of Information Resource Management's Mobile and Remote Access Division

DOMESTIC OPERATIONS

# HIGHLIGHTS
Office of Inspector General
United States Department of State

ISP-I-23-23

**What OIG Inspected**

OIG inspected the Bureau of Information Resource Management's Mobile and Remote Access Division's services, specifically the management of mobile and remote access services systems security; customer service delivery; mobile devices and subscription services; and contracts.

**What OIG Recommends**

OIG made 7 recommendations to the Bureau of Information Resource Management. In its comments on the draft report, the bureau concurred with 5 recommendations, neither agreed nor disagreed with 1 recommendation, and disagreed with 1 recommendation. OIG considers 5 recommendations resolved and 2 recommendations unresolved. The bureau's response to each recommendation, and OIG's reply, can be found in the Recommendations section of this report. The bureau's formal response is reprinted in its entirety in Appendix B.

**June 2023**
**OFFICE OF INSPECTIONS**
DOMESTIC OPERATIONS

## Inspection of the Bureau of Information Resource Management's Mobile and Remote Access Division

**What OIG Found**

- Department of State stakeholders praised the Mobile and Remote Access Division's swift response to support the increased remote access demand during the COVID-19 pandemic.
- The Department did not monitor and control the usage and costs of mobile device services, and the division did not issue guidance to Department employees responsible for managing usage and costs. This resulted in more than $7.2 million in expenditures in 2022 that could have been put to better use. OIG estimated that these expenditures represented 24.4 percent of the Department's $29.5 million total annual cost for mobile device services.
- The division did not perform all information systems security officer duties for its own systems or for the enterprise mobile devices it managed for the Department, placing at risk IT security for approximately 83,000 mobile devices worldwide.
- The division did not communicate and enforce the enterprise mobile device system user groups access requirements in the GO Desktop system security plan. As a result, Department managers issued enterprise mobile devices to users overseas without considering the security requirements in the plan.

# CONTENTS

# CONTEXT

The Bureau of Information Resource Management's (IRM) Mobile and Remote Access Division (MRA) administers, maintains, and provides Tiers II and III[1] service desk support for mobile and remote access capabilities and wireless provisioning services[2] for the Department of State (Department). MRA's remote access capabilities include:

1. *GO[3] Mobile*: Mobile solution which allows users to securely access Department resources via personal or government-furnished equipment mobile devices.
2. *GO Virtual:* Remote access solution which allows users to access OpenNet from a virtual client using their personal devices.
3. *GO Desktop*: Remote solution which allows users to remotely access OpenNet via the Department's IT Configuration Control Board-approved Windows 10 devices, also known as enterprise mobile devices.

MRA also is responsible for GO Manager, which includes an enterprise telecom expense management system.

MRA's four goals, as outlined in its FY 2023 and FY 2024 Mobile Program Strategy, are to:

- Improve the customer experience and end-user satisfaction of MRA's mobile programs, services, and support.
- Maintain the capabilities to provide robust mobile solutions efficiently and effectively.
- Ensure the Department is equipped with the right tools and technology to complete its diplomatic mission from any location and at any time.
- Drive the Mobile Strategy for the Department and provide key insights into mobile solutions, technologies, and capabilities.

A Deputy Division Chief, who also is serving as the acting Division Chief, and two Branch Chiefs lead MRA and its two branches: Mobile Operations and Mobile Strategies. The Mobile Operations Branch is responsible for planning, implementing, operating, and improving IT services and the systems for managing IT service operations. The Mobile Strategies Branch focuses on advancing IRM's mobile and remote access strategies and planning the division's

[1] Tier II support requires personnel with deep knowledge of the product or service but does not include the engineer or programmer who designed and created the product. Tier III support requires personnel with expert product and service knowledge, such as engineers and programmers.

[2] Wireless provisioning services include procuring mobile devices, activating commercial carrier services (AT&T, Verizon, T-Mobile), Subscriber Identity Module provisioning, making wireless service changes, assisting with carrier service issues, and operating a billing management application.

[3] GO is Global OpenNet, the name used for the Department's Sensitive But Unclassified network when accessed remotely.

budget. MRA has maintained ISO[4]/IEC 20000-10(ISO 20K) certification—a standard for IT service providers around the world—since 2016.

MRA receives its budget from the Department's Working Capital Fund (WCF) and appropriations. The WCF is a revolving fund through which Department customers transfer appropriated funds to MRA as payment for IT services. In FY 2022, MRA's budget was $71 million; of that, $58 million was from the WCF and $13 million was appropriated funding. For FY 2023, the projected budget was $65 million from the WCF and $12 million from appropriations.

At the time of the inspection, MRA's staffing comprised 10 full-time Civil Service and 4 Foreign Service specialists as well as 134 contractor personnel. Additionally, as of January 2023, three full-time positions in the division were vacant—two Civil Service positions and one Foreign Service specialist position.

Consistent with Section 209 of the Foreign Service Act of 1980, OIG reviewed MRA's leadership and the division's overall delivery of services. Additionally, OIG evaluated the division's management of systems security, customer service delivery, mobile device services, and contract management.[5]

## LEADERSHIP AND OVERALL DELIVERY OF SERVICES

Based on staff responses to OIG questionnaires, OIG determined that the MRA acting Division Chief and the two Branch Chiefs set a positive tone and led the division consistent with the Department's leadership and management principles contained in 3 Foreign Affairs Manual (FAM) 1214b.[6] OIG also found that the division collaborated with the Bureau of Diplomatic Security and IRM stakeholders to expand mobile and remote access capabilities to Department users at the onset of the COVID-19 pandemic in March 2020. Prior to the pandemic, MRA supported 32,000 GO Mobile and GO Desktop devices. As of November 28, 2022, MRA supported 95,000 devices worldwide, tripling its mobile and remote access services. Department stakeholders praised MRA's swift response to support the increased remote access demands during the pandemic. Finally, OIG concluded that MRA's overall delivery of services generally complied with Department standards and guidelines although, as discussed in the next four sections of this report, OIG found some issues that require management attention.

[4] International Organization for Standardization (ISO) 20000 is a service management standard for IT service providers around the world.

[5] See Appendix A.

[6] The Department's leadership and management principles outlined in 3 FAM 1214b include (1) model integrity, (2) plan strategically, (3) be decisive and take responsibility, (4) communicate, (5) learn and innovate constantly, (6) be self-aware, (7) collaborate, (8) value and develop people, (9) manage conflict, and (10) foster resilience.

# MANAGEMENT OF SYSTEMS SECURITY

### *Division's Information Systems Security Officer Program Needed Improvement*

OIG found MRA did not perform all information systems security officer (ISSO) duties for its systems or the enterprise mobile devices (EMD)[7] under its purview. According to 12 FAM 613.4 and 5 Foreign Affairs Handbook (FAH)-11 H-116a(1), ISSOs are responsible for implementing cybersecurity policies and procedures for information systems and for using the ISSO checklist to document all required duties. Although MRA handled systems authorizations, an ISSO duty, OIG found MRA did not have ISSO accounts to monitor MRA's systems and EMDs, which included more than 20,000 laptops and 63,000 mobile phones. Furthermore, the division restricted ISSO access for the EMDs to its own staff. This meant that bureau and overseas post ISSOs were unable to monitor the EMDs issued to their users, as required in 12 FAH-10 H-163.3(8).

OIG also found that MRA ISSOs did not consistently participate in the review and approval of changes to its systems, such as GO Manager, to ensure the changes did not affect security controls. OIG determined that the lack of full-time ISSO staff led to these issues. OIG issued two management assistance reports, one in May 2017 and the other in December 2020,[8] that highlighted widespread Department failures to perform ISSO duties. Failure to perform required ISSO responsibilities leaves Department networks vulnerable to potential unauthorized access and malicious activity, an especially serious concern in light of the office's Department-wide IT security responsibilities for more than 83,000 enterprise mobile devices.

> **Recommendation 1:** The Bureau of Information Resource Management should implement an information systems security officer program for systems and enterprise mobile devices that complies with Department standards. (Action: IRM)

### *Lack of Communication and Enforcement Led to the Issuance of Enterprise Mobile Devices to Unauthorized Systems User Groups*

OIG found MRA did not communicate and enforce EMD user group requirements outlined in the GO Desktop system security plan.[9] According to 5 FAM 842a, a system security plan provides all the information necessary to secure an IT system throughout the system's lifecycle.

[7] Enterprise mobile devices are unclassified Department-owned mobile devices that are approved to connect to the Sensitive But Unclassified enterprise network.

[8] OIG, *Management Assistance Report: Non-Performance of Information Systems Security Officer Duties by Overseas Personnel* (ISP-17-24, May 2017); OIG, *Management Assistance Report: Continued Deficiencies in Performance of Information Systems Security Officer Responsibilities at Overseas Posts* (ISP-21-07, December 2020).

[9] A system security plan, also called security plan, is a formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned to meet those requirements. See the National Institute of Standards and Technology (NIST) Special Publication 800-53A Revision 5—Security and Privacy Controls for Federal Information Systems and Organizations (at Appendix A).

In this instance, the GO Desktop system security plan also was used to obtain authorization to operate[10] from IRM. The plan states that user groups with U.S. direct hire and contractor employees with minimum Secret clearances are authorized to use GO Desktop. However, because MRA did not communicate and enforce this user group requirement, at the time of the inspection more than 5,000 potential prohibited users[11] had been issued EMDs. In discussions with MRA about this issue, division managers told OIG that MRA planned to address this issue with IRM's Cyber Operations Directorate. Not communicating and enforcing security requirements weakens the information security stance of the Department and its EMDs.

> **Recommendation 2:** The Bureau of Information Resource Management should require the Mobile and Remote Access Division to communicate and enforce the Global OpenNet Desktop system user group access requirements outlined in the GO Desktop system security plan. (Action: IRM)

### *Division's Change Management Procedures Did Not Fully Comply With Department Standards*

MRA's change management procedures did not fully comply with Department standards. Department policy in 5 FAM 861c requires that changes to information systems take place in an identifiable and controlled fashion. OIG determined that MRA staff documented changes to one of the information systems it owned and operated using weekly meeting minutes, as required by MRA's change management procedures. However, OIG's review of the meeting minutes found it difficult to identify which items in the minutes were actual changes, when the changes were scheduled to take place, or whether a change was successfully implemented.

Additionally, 12 FAH-10 H-222.5-3 requires responsible ISSOs to ensure that system security settings are not modified when a system's configuration is changed. MRA's documented change management procedures state, as required, that the ISSO is responsible for evaluating changes submitted to IRM's Change Advisory Board to ensure controls are not modified, and that the ISSO is a member of the MRA Local Change Advisory Board. However, OIG found that the responsible ISSO did not review all changes to MRA systems and was not a participating member of the division's Change Advisory Board. The failure to document changes in an identifiable and detailed manner and to review those changes with explicit consideration for security increases the risk of compromising the confidentiality, integrity, and availability of sensitive information systems.

[10] An authorization to operate is the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operation (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security controls. See the National Institute of Standards and Technology Special Publication 800-53A Revision 5—Security and Privacy Controls for Federal Information Systems and Organizations (at Appendix A).

[11] Prohibited users are not allowed system access in the system security plan.

**Recommendation 3:** The Bureau of Information Resource Management should require the Mobile and Remote Access Division to bring its change management procedures into compliance with Department standards. (Action: IRM)

## CUSTOMER SERVICE DELIVERY

### *Separate Laptop Programs With the Same Name Led to Customer Confusion and Misconfigured Devices*

IRM operated two separate laptop programs with the same name, leading to end-user confusion and inefficient use of government resources. Both MRA and IRM's Office of Consolidated Customer Support titled their OpenNet laptop programs GO Desktop. Despite the identical names, the two programs are separate, are managed by different organizations within IRM, and are supported by different service desks.

OIG found instances of GO Desktop service requests being routed back and forth between the two program service desks because it was unclear which program was responsible for supporting the end user. Additionally, OIG observed instances of GO Desktop devices that were configured incorrectly because of the duplicate naming convention. The Office of Management and Budget's Circular A-130, Section 5,[12] requires federal agencies to perform information resource management activities in an efficient and effective manner. The Office of Consolidated Customer Support's GO Desktop program was established to help manage the increased use of laptops in the Department due to the COVID-19 pandemic, but a lack of coordination and communication from IRM led to the duplicate naming convention and end-user confusion. Failure to clarify the responsibilities of the two offices to end users creates confusion for Department end users and causes inefficiencies and delays with the support they receive.

**Recommendation 4:** The Bureau of Information Resource Management should take steps to eliminate the confusion between its two GO Desktop programs. (Action: IRM)

## MOBILE DEVICE SERVICES

### *Department Did Not Monitor and Control the Usage and Costs of Mobile Device Services*

OIG determined that the Department did not monitor and control the usage and costs of mobile device services despite guidance in 5 FAM 527a and c requiring domestic bureaus and offices and overseas posts to review telephone service costs monthly to maintain management control over Department telephone expenses.[13] This problem first was identified in an audit

[12] The Office of Management and Budget Circular A-130, "Managing Information as a Strategic Resource," July 28, 2016.

[13] The Department issued 5 FAM 527 on August 9, 2013, when IRM's Telephone, Wireless, and Data Services Division was responsible for overseeing the Department's telephone expenses. MRA assumed this responsibility on January 26, 2014.

conducted by the Government Accountability Office (GAO) in 2015,[14] in which GAO sampled records from the Bureaus of Diplomatic Security and African Affairs and concluded that the Department lacked effective processes and procedures to monitor and control spending on mobile devices and wireless services. GAO recommended that the Department establish Department-wide procedures to monitor and control spending on its mobile devices and services. The Department tasked MRA with addressing the recommendation.

During this inspection, OIG found that MRA drafted a Mobile Service Oversight Guidance Policy in November 2018, but never finalized it.[15] The policy would have provided guidance to Department staff responsible for managing usage and costs of mobile device services—cost center managers and systems administrators in domestic bureaus and offices and overseas posts—on how to review Telecom Expense Management System (TEMS)[16] reports to identify possible cost savings and take action to realize the savings. MRA told OIG that even though it did not finalize the policy, it sent TEMS reports to domestic bureaus and offices and overseas missions each month. However, OIG identified several problems with MRA's approach. Specifically,

- The reports were not sent to all cost center managers. MRA staff told OIG they only send monthly TEMS reports to the 104 cost center managers who requested them. MRA was unable to provide to OIG the total number of cost center managers or systems administrators in the Department, with estimates differing greatly. MRA staff told OIG the guidance they had received from IRM management was to send the TEMS reports only to those cost centers that requested them.
- There was no enforcement mechanism. The reports, for example, show potential savings that could be achieved by suspending or deactivating unused lines. MRA staff said they could not compel managers to act on the information, nor did MRA have the authority to suspend or deactivate unused lines themselves. The average active mobile line costs $69 per month; a suspended line costs $10 per month. Additionally, there was no requirement for cost center managers to tell MRA what actions they took based on the information in the reports.
- The TEMS reports were difficult to understand without additional guidance. MRA staff said they received feedback from some cost center managers that the data in the

[14] GAO, TELECOMMUNICATIONS: Agencies Need Better Controls to Achieve Significant Savings on Mobile Devices and Services (GAO-15-431, May 21, 2015).

[15] Upon OIG bringing this to MRA's attention, division staff responded that they would begin working to finalize the policy. MRA staff also informed OIG of three additional sets of guidance for cost center managers and systems administrators. However, two of them did not include information on mobile device services. The third set of guidance contained updated directions on using TEMS, but did not include a mechanism to ensure, or specify procedures for ensuring, that cost center managers act upon recommended savings. Finally, all three sets of guidance could be accessed only on MRA's internal SharePoint site, which is only available to MRA staff. Thus, it was unclear how many, if any, cost center managers and system administrators had seen the three sets of guidance.

[16] The monthly TEMS reports specify the mobile phone lines and users under each cost center, and what type of action is needed. The reports include an attachment listing unused lines that could be suspended or deactivated as well as an attachment listing high expense lines that have exceeded voice or data limits.

reports was unclear or hard to understand. In January 2023, MRA staff told OIG they were working on an update "in the next 1 or 2 months" to address this problem and that any changes would be communicated to cost center managers.

Because MRA never finalized and issued its Mobile Service Oversight Guidance Policy and because of the problems enumerated above with MRA's approach of sending TEMS reports to some cost center managers and not knowing whether the information was being acted on, OIG set out to determine whether the problem identified by GAO in 2015 still existed. To start, OIG sampled documentation from the same two bureaus the GAO had reviewed—the Bureaus of Diplomatic Security and African Affairs—and identified a total of $355,392 in potential savings during a 10-month period from March through December 2022. OIG then expanded its review to sample documentation Department-wide and in doing so, identified $7,216,203 in potential savings in mobile device services for calendar year 2022. This included unused or inactive cellular lines for which the Department was still paying, as well as voice, data, and roaming usage that exceeded the contracted amounts.[17] These potential savings represented 24.4 percent of the Department's $29.5 million total annual cost for mobile device services.

Without a clear policy or adequate procedures in place to monitor and control the usage and costs of mobile device services, the Department is continuing to spend more than is necessary for its mobile device services as evidenced by the more than $7.2 million in potential savings in 2022 that could have been put to better use.

**Recommendation 5:** The Bureau of Information Resource Management, in coordination with the Bureau of Administration, should implement policies and procedures to monitor and control the usage and costs of mobile device services in accordance with Department standards and put potential savings of up to $7,216,203 to better use. (Action: IRM, in coordination with A)

## CONTRACT MANAGEMENT

### *Contract File Management Did Not Comply With Department Standards*

OIG reviewed contract files and documentation for all 13 MRA contracts (total value approximately $45 million) and found contract file management did not comply with Department standards. OIG found the files did not include key documents, which MRA staff were unable to provide, despite multiple requests. Specifically,

- Three time and materials contracts did not have signed determination and finding documents approving the use of that type of contract. This is significant because the Federal Acquisition Regulation (FAR) discourages the use of time and materials contracts

[17] Cost center managers request mobile services from one of three carriers and a specific plan under that carrier for each line. Not all plans have unlimited voice and data. Monthly TEMS reports identify when lines have excessive voice or data overages, and costs that could be reduced with use of another plan. It is the responsibility of cost center managers to request plan changes to achieve recommended cost savings.

and states they only can be used if the contracting officer prepares a determination and finding document stating that no other contract type is suitable, and the head of contracting activity, or their designee, approves its use prior to the issuance of the contract (FAR 16.601(d)(1)).

- One contract was missing a National Defense Authorization Act Section 889 representation from the vendor stating that they did not use equipment or services from any prohibited sources. If they were using such equipment or services, the Department would have been prohibited from entering into a contract. Contracting with a vendor found to be using equipment or services from a prohibited source could represent an IT security risk. (FAR 4.2102(a)(1)-(2), FAR 52.204(b)(1)-(2))
- Eight contract files were missing required copies of modifications to the contracts (FAR 4.803(a)(26)(ii)).

Despite these issues, OIG's interviews with staff in MRA, IRM's IT Acquisition Contract Management, and the Bureau of Administration's Office of Acquisitions Management[18] and reviews of other documentation showed that staff responsible for overseeing MRA awards monitored contracts, received goods and services for which it had contracted, and addressed contractor's performance when issues arose.

Contracting officer and contracting officer's representative (COR) staff told OIG they were unable to locate some documents because they were completed by staff who had left MRA and were no longer responsible for those contracts. In addition, other documents were unavailable due to administrative mistakes. MRA contracting staff told OIG the division kept contract files and documentation in both the Integrated Logistics Management System, the Department's system of record for procurement,[19] and in one of several Teams channels and SharePoint sites. However, OIG reviewed these locations and was unable to locate the missing documents. Non-compliance with contract and COR file requirements increases the risk of contract mismanagement.

**Recommendation 6:** The Bureau of Information Resource Management, in coordination with the Bureau of Administration, should bring the Mobile and Remote Access Division's contract and contracting officer's representative files into compliance with Department and federal guidance. (Action: IRM, in coordination with A)

[18] The Bureau of Administration's Office of Acquisitions Management provides all contracting officer and contract specialist staff to manage MRA's contracts. IRM's Division of IT Acquisitions Contract Management provides full time contracting officer's representatives to manage some MRA contracts.

[19] The Integrated Logistics Management System (ILMS) is an integrated web-based system that encompasses all Department supply chain functions in one system. ILMS is designed to upgrade Department supply chain management by improving operations in areas such as purchasing, procurement, warehousing, transportation, property management, personal effects, and diplomatic pouch and mail.

### *Contracting Officer's Representative and Government Technical Monitor Programs Did Not Fully Comply With Department Standards*

MRA's COR and government technical monitor (GTM)[20] programs did not fully comply with Department standards. MRA had five CORs assigned to 13 MRA contracts worth approximately $45 million and three staff members serving as GTMs. OIG interviewed the CORs and GTMs, and reviewed the files and documentation provided for all MRA contracts and found that:

- Two CORs and all three GTMs lacked current delegation letters (14 FAH-2 H-143.2).
- Two CORs and the three GTMs lacked current OGE-450 financial disclosure statements (14 FAH-2 H-151c).
- None of the GTMs had current certifications issued by the Department's Office of the Procurement Executive (14 FAH-2 H-143a) nor had they completed all the required training (14 FAH-2 H-143.1).
- Only two of the three GTMs completed the required bi-weekly vendor performance assessments (MRA Service Monitoring Plan, Sections 3.2 and 7.3.4.1).

Despite these issues, OIG's interviews with staff in MRA, IT Acquisitions Contract Management, the Office of Acquisitions Management and reviews of other documentation showed that staff responsible for overseeing MRA's contracts monitored the contracts, received goods and services for which it had contracted, and addressed contractor performance when issues arose.

Staff told OIG the issues with the COR and GTM programs occurred because they had limited time for those duties. Four of the eight CORs and GTMs said these were ancillary duties in addition to their other work. The four full-time CORs said they oversaw multiple contracts. Non-compliant COR and GTM programs increase the risk of contract mismanagement.

**Recommendation 7:** The Bureau of Information Resource Management should bring the Mobile and Remote Access Division's contracting officer's representative and government technical monitor programs into compliance with Department standards. (Action: IRM)

[20] Department of State Acquisition Regulation (DOSAR) 642.271 states a contracting officer may appoint a government technical monitor to assist a COR in monitoring a contractor's performance. This may be because the GTM has special skills or knowledge necessary for monitoring the contractor's work. According to contracting officer and COR staff, CORs and GTMs have the same requirements for training and certification.

# RECOMMENDATIONS

OIG provided a draft of this report to Department stakeholders for their review and comment on the findings and recommendations. OIG issued the following recommendations to the Bureau of Information Resource Management. The bureau's complete response can be found in Appendix B.

**Recommendation 1:** The Bureau of Information Resource Management should implement an information systems security officer program for systems and enterprise mobile devices that complies with Department standards. (Action: IRM)

**Management Response:** In its May 25, 2023, response, the Bureau of Information Resource Management concurred with this recommendation.

**OIG Reply:** OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation that the Bureau of Information Resource Management implemented an information systems security officer program for systems and enterprise mobile devices that complies with Department standards.

**Recommendation 2:** The Bureau of Information Resource Management should require the Mobile and Remote Access Division to communicate and enforce the Global OpenNet Desktop system user group access requirements outlined in the GO Desktop system security plan. (Action: IRM)

**Management Response:** In its May 25, 2023, response, the Bureau of Information Resource Management disagreed with this recommendation. The bureau requested that the recommendation be rewritten to require the Mobile and Remote Access Division (MRA) to update the Global OpenNet (GO) Desktop system user group access requirements outlined in the GO Desktop system security plan.

**OIG Reply:** OIG considers the recommendation unresolved. OIG acknowledges that the Bureau of Information Resource Management is considering updating the GO Desktop system user group access requirements as part of its efforts to implement this recommendation. However, any potential changes will still need to be communicated to overseas posts and enforced; therefore, OIG did not revise this recommendation. As noted in the report, OIG determined that the bureau did not communicate and enforce the current requirements. As a result, more than 5,000 users who were not U.S. direct-hire or contractor personnel with the minimum Secret clearances—contrary to the requirements set forth in the system security plan—had been issued enterprise mobile devices to access the GO Desktop system. The recommendation can be closed when OIG receives and accepts documentation that the Bureau of Information Resource Management communicated and enforced the GO Desktop system user group access requirements outlined in the system security plan.

**Recommendation 3:** The Bureau of Information Resource Management should require the Mobile and Remote Access Division to bring its change management procedures into compliance with Department standards. (Action: IRM)

**Management Response:** In its May 25, 2023, response, the Bureau of Information Resource Management concurred with this recommendation.

**OIG Reply:** OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation that the MRA's change management procedures comply with Department standards.

**Recommendation 4:** The Bureau of Information Resource Management should take steps to eliminate the confusion between its two GO Desktop programs. (Action: IRM)

**Management Response:** In its May 25, 2023, response, the Bureau of Information Resource Management neither agreed nor disagreed with this recommendation. The bureau noted it addressed the customer confusion by consolidating the two helpdesks, as of July 19, 2021, into the single helpdesk run by the bureau's Office of Consolidated Customer Support.

**OIG Reply:** OIG considers the recommendation unresolved. OIG acknowledges that the Office of Consolidated Customer Support's (CCS) GO Desktop program was established to help manage the increased use of laptops in the Department due to the COVID-19 pandemic and that, in 2021, the Bureau of Information Resource Management intended to have a single helpdesk run by CCS. However, at the time of the inspection nearly 2 years later, OIG found that both MRA and CCS had laptop programs referred to as GO Desktop, with separate service desks, leading to confusion for Department end users. OIG determined that the two laptop programs with the same name was a result of the bureau's lack of coordination and communication. The recommendation can be closed when OIG receives and accepts documentation that the Bureau of Information Resource Management took steps to eliminate the confusion between its two GO Desktop programs.

**Recommendation 5:** The Bureau of Information Resource Management, in coordination with the Bureau of Administration, should implement policies and procedures to monitor and control the usage and costs of mobile device services in accordance with Department standards and put potential savings of up to $7,216,203 to better use. (Action: IRM, in coordination with A)

**Management Response:** In its May 25, 2023, response, the Bureau of Information Resource Management concurred with this recommendation.

**OIG Reply:** OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation that the Bureau of Information Resource Management implemented policies and procedures to monitor and control the usage and costs of mobile device services in accordance with Department standards and put potential savings of up to $7,216,203 to better use.

**Recommendation 6:** The Bureau of Information Resource Management, in coordination with the Bureau of Administration, should bring the Mobile and Remote Access Division's contract and contracting officer's representative files into compliance with Department and federal guidance. (Action: IRM, in coordination with A)

**Management Response:** In its May 25, 2023, response, the Bureau of Information Resource Management concurred with this recommendation. Additionally, the bureau noted that it discussed the recommendation with the Bureau of Administration, and both parties agreed that this recommendation should be assigned to the Bureau of Administration.

**OIG Reply:** OIG considers the recommendation resolved. OIG acknowledges that the Bureau of Administration's Office of Acquisitions Management provides contracting officers to manage MRA's contracts and will be involved in the implementation of the recommendation. However, because the contracts belong to the MRA, the Bureau of Information Resource Management will need to initiate action and request assistance from the Bureau of Administration to bring the contract files into compliance. The recommendation can be closed when OIG receives and accepts documentation that MRA's contract and contracting officer's representative files comply with Department and federal guidance.

**Recommendation 7:** The Bureau of Information Resource Management should bring the Mobile and Remote Access Division's contracting officer's representative and government technical monitor programs into compliance with Department standards. (Action: IRM)

**Management Response:** In its May 25, 2023, response, the Bureau of Information Resource Management concurred with this recommendation.

**OIG Reply:** OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation that MRA's contracting officer's representative and government technical monitor programs comply with Department standards.

# PRINCIPAL OFFICIALS

| Title | Name | Arrival Date |
|---|---|---|
| | | |
| Division Chief | Billy McGowan[a] | 7/2022 |
| Deputy Division Chief | Billy McGowan | 7/2022 |
| **Branch Chiefs** | | |
| Mobile Operations | Tonya Wood-Griffin | 5/2014 |
| Mobile Strategies | Colin McCannon | 8/2021 |

[a] At the time of the inspection, Billy McGowan was serving as the acting Division Chief.

**Source:** Generated by OIG from data provided by the Mobile and Remote Access Division.

# APPENDIX A: OBJECTIVES, SCOPE, AND METHODOLOGY

This inspection was conducted from January 3 to March 13, 2023, in accordance with the Quality Standards for Inspection and Evaluation, as issued in 2020 by the Council of the Inspectors General on Integrity and Efficiency, and the Inspections Handbook, as issued by the Office of Inspector General (OIG) for the Department and the U.S. Agency for Global Media (USAGM).

## Objectives and Scope

The Office of Inspections provides the Secretary of State, the Chief Executive Officer of USAGM, and Congress with systematic and independent evaluations of the operations of the Department and USAGM. Consistent with Section 209 of the Foreign Service Act of 1980, OIG's specific objectives for this inspection of the Bureau of Information Resource Management's Mobile and Remote Access (MRA) Division were to determine whether MRA:

- Established processes and procedures for innovating, developing, securing, operating, and maintaining the Department's mobile and remote access systems in accordance with federal and Department standards.
- Established procedures to ensure mobile devices complied with Bureau of Diplomatic Security configuration standards.
- Established procedures for monitoring and controlling wireless devices and services usage in accordance with federal requirements and Department standards.
- Established policies and procedures for managing Tiers II and III mobile and remote access service requests in accordance with service level agreements.
- Established the capability to monitor customer service metrics and complied with service level agreement requirements related to mobile and remote access services.
- Had adequate internal controls in place for managing and monitoring its contracts in accordance with federal requirements and Department standards.

## Methodology

OIG used a risk-based approach to prepare for this inspection. OIG conducted portions of the inspection remotely and relied on audio- and video-conferencing tools in addition to in-person interviews with Department and other personnel. OIG also reviewed pertinent records; circulated surveys and compiled the results; and reviewed the substance of this report and its findings and recommendations with offices, individuals, and organizations affected by the review. OIG used professional judgment and analyzed physical, documentary, and testimonial evidence to develop its findings, conclusions, and actionable recommendations.

# APPENDIX B: MANAGEMENT RESPONSE

**United States Department of State**

***Washington, D.C. 20520***

UNCLASSIFIED May 25, 2023

o Read by _____

**NOTE FOR ASSISTANT INSPECTOR GENERAL FOR INSPECTIONS LEWIS**

FROM: IRM – Kelly E. Fletcher (Signed)

SUBJECT: (U) Draft Report - Inspection of the Bureau of Information Resource Management's Mobile and Remote Access Division

The Bureau of Information Resource Management (IRM) provides the following responses to the recommendations issued in the draft report of the Inspection of the Bureau of Information Resource Management's Mobile and Remote Access Division.

**Recommendation 1:** The Bureau of Information Resource Management should implement an Information Systems Security Officer (ISSO) program for systems and enterprise mobile devices that complies with Department standards. (Action: IRM)

**Management Response (Draft Report):** IRM concurs with this recommendation. We have an ISSO program and are following Department guidance on filling the MRA vacancy to comply with Department standards

**Recommendation 2:** The Bureau of Information Resource Management should require the Mobile and Remote Access Division to communicate and

enforce the Global OpenNet Desktop system user group access requirements outlined in the GO Desktop system security plan. (Action: IRM)

**Management Response (Draft Report):** IRM non-concurs and requests that the recommendation is re-written as follows:

- The Bureau of Information Resource Management should require the Mobile and Remote Access Division to update the Global OpenNet Desktop system user group access requirements outlined in the GO Desktop System Security Plan (SSP).

**Recommendation 3:** The Bureau of Information Resource Management should require the Mobile and Remote Access Division to bring its change management procedures into compliance with Department standards. (Action: IRM)

**Management Response (Draft Report):** IRM concurs with this recommendation. IRM will review and upate the change management procedures to bring them into compliance with Department standards.

**Recommendation 4:** The Bureau of Information Resource Management should take steps to eliminate the confusion between its two GO Desktop programs. (Action: IRM)

**Management Response (Draft Report):** IRM has addressed the customer confusion by consolidating the two helpdesks as of July 19, 2021 into the single helpdesk run by the Office of Consolidated Customer Support (CCS). IRM requests that this finding is closed.

**Recommendation 5:** The Bureau of Information Resource Management, in coordination with the Bureau of Administration, should implement policies and procedures to monitor and control the usage and costs of mobile device services in accordance with Department standards and put potential savings of up to $7,216,203 to better use. (Action: IRM, in coordination with A)

**Management Response (Draft Report).** IRM concurs with this recommendation. MRA provides monthly line status reports to the Cost Center System Administrators and Managers. In addition, MRA provides MobiChord Generated Customer Reports, on demand. IRM is working on updating and finalizing the mobile service oversight guidance policy.

MobiChord Telecom Expense Reports: High Usage & Unused Lines (Sys Admin, FMO, & GSO Guidance)

**Recommendation 6:** The Bureau of Information Resource Management, in coordination with the Bureau of Administration, should bring the Mobile and Remote Access Division's contract and contracting officer's representative files into compliance with Department and federal guidance. (Action: IRM, in coordination with A)

**Management Response (Draft Report).** IRM concurs with this recommendation. IRM discussed with A Bureau and both parties agree that this recommendation should be assigned to A-bureau as the Action Office with IRM as coordinating entity.

**Recommendation 7:** The Bureau of Information Resource Management should bring the Mobile and Remote Access Division's contracting officer's representative and government technical monitor programs into compliance with Department standards. (Action: IRM)

**Management Response (Draft Report):** IRM concurs with this recommendation. IRM will work the Bureau of Administration to address and bring the contracting officer's representative and government technical monitor programs into compliance with Department standards.

# ABBREVIATIONS

| | |
|---|---|
| COR | Contracting Officer's Representative |
| EMD | Enterprise Mobile Device |
| FAH | Foreign Affairs Handbook |
| FAM | Foreign Affairs Manual |
| FAR | Federal Acquisition Regulation |
| GAO | Government Accountability Office |
| GTM | Government Technical Monitor |
| IRM | Information Resource Management |
| ISSO | Information Systems Security Officer |
| MRA | Mobile and Remote Access Division |
| TEMS | Telecom Expense Management System |
| WCF | Working Capital Fund |

# OIG INSPECTION TEAM MEMBERS

Martha Fikru, Team Leader
Brett Fegley
Paul Sanders
Brian Smith

**Other Contributors**
Ellen Engels
Caroline Mangelsdorf

# HELP FIGHT

## FRAUD, WASTE, AND ABUSE

1-800-409-9926
**www.stateoig.gov/HOTLINE**

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