# 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.