Office of Inspector General
United States Department of State

ISP-I-24-21 | Office of Inspections | June 2024

Targeted Review of the Bureau of Diplomatic Technology's Cloud Services Program Management

TARGETED REVIEW

Summary of Review

OIG reviewed the Bureau of Information Resource Management's (IRM)[1] enterprise cloud computing services program management. The two primary enterprise cloud service providers in IRM are the Cloud Program Management Office (CPMO) and the Systems Integration Office (SIO). Together, the two offices offer seven enterprise-level[2] (or enterprise) cloud services to help Department of State (Department) bureaus and offices efficiently and securely transition their systems and applications from on-premises data centers to modernized cloud environments, in accordance with IRM's stated goal of enabling modernization. Due to the self-service capabilities inherent in cloud computing environments and the ability to rapidly provision and release cloud resources with minimal management involvement, there are cost, configuration, and security control risks unique to cloud computing that organizations managing these environments must address. Through this review, OIG sought to determine whether (1) enterprise-level cloud systems complied with federal and Department security requirements; (2) CPMO and SIO implemented required product management and customer engagement processes and procedures; (3) IRM established internal controls to govern the use of enterprise cloud systems in the Department; and (4) enterprise cloud systems complied with federal and Department contracting and procurement requirements.

OIG found IRM's cloud computing policies and guidelines have not kept pace with the quickly evolving cloud computing landscape and the rollout of enterprise cloud services in the Department. OIG's review determined IRM established processes and procedures to meet most federal and Department security requirements and to monitor and control costs associated with the enterprise cloud services. However, the policies and guidelines IRM established to govern the procurement, implementation, configuration, and use of cloud services in the Department were outdated and obsolete. Additionally, OIG found the customer engagement processes IRM used to promote awareness of the enterprise cloud services required improvement.

This review includes 11 recommendations to improve IRM's cloud services program management. In its comments on the draft review, the bureau concurred with all 11 recommendations. OIG considers all 11 recommendations resolved. The bureau's response to each recommendation and OIG's reply can be found in the Recommendations section of this review. The bureau's formal written response is reprinted in its entirety in Appendix B.

[1] In May 2024, after OIG issued the draft targeted review, the Department changed the name of the bureau to the Bureau of Diplomatic Technology (DT). Throughout this targeted review, except for the report title and recommendations, the bureau is still referred to as IRM.

[2] An enterprise-level service is defined as a solution designed to integrate multiple facets of an organization's business.

BACKGROUND

The National Institute of Standards and Technology defines cloud computing as a "model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management involvement or service provider interaction." In February 2011, the federal government released the first federal cloud computing strategy, commonly referred to as "Cloud First," to accelerate the pace at which the federal government adopted cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making any new investments. The latest version of the strategy, commonly referred to as "Cloud Smart," was released in June 2019, and was intended to offer implementation guidance for government agencies to fully realize the potential of cloud computing technologies.[3] Additionally, in 2011, the federal government established the Federal Risk and Authorization Management Program (FedRAMP), which is a government-wide program that provides a standardized approach to security assessment and authorization for cloud products and services.

The Department's IT strategic plan for FY 2011-2013 was the first Department IT strategic plan to mention cloud computing. Goal 2 of that plan stated the Department would take maximum advantage of advances in networking, virtualization, storage, and application services offered by cloud computing technologies. The Department's first cloud computing policies and guidelines were released in the Foreign Affairs Manual (FAM) and Foreign Affairs Handbook (FAH) in October 2015 to provide Department-wide direction, policy, and governance requirements for the use of cloud services. IRM released the Department's first enterprise cloud strategy in July 2018 to provide enterprise-level direction for achieving the full benefits of cloud computing and drive Department-wide cloud adoption through a shared service model.

OIG first inspected the Department's cloud computing efforts in a 2012 report titled *Inspection of the Bureau of Information Resource Management, Systems Integration Office*.[4] At that time, IRM had no central office to coordinate cloud computing initiatives Department-wide. The report discussed SIO's efforts to establish a private cloud environment for the Department. Although SIO existed prior to the advent of cloud computing technology in the Department and was not primarily focused on cloud computing, the office initially took the lead on implementing enterprise cloud services for the Department.

Mission and Organization

In 2018, the Department's then-Chief Information Officer identified the need for a central office in IRM to assist the Department in taking a more strategic, enterprise-level approach to cloud services delivery and established CPMO. The intent was for CPMO to manage the architecture planning and delivery of a secure enterprise multi-cloud ecosystem. When the office was first created, the CPMO leadership team described the Department's cloud computing landscape as

[3] U.S. Federal Chief Information Officer, "Federal Cloud Computing Strategy," June 24, 2019.

[4] OIG, *Inspection of the Bureau of Information Resource Management, Systems Integration Office* (ISP-I-12-30, June 2012).

a host of uncoordinated efforts spread across the Department's bureaus and offices that were early adopters of the new cloud computing technologies, which made it difficult for offices with information assurance responsibilities to track, monitor, and secure the Department's data in the cloud. Part of CPMO's initial implementation plan was to consolidate duplicative services and track and monitor the Department's cloud data.

At the time of this review, CPMO and SIO were the two primary cloud service providers in the Department offering enterprise-level cloud services. Although CPMO's mission is not codified in 1 FAM 270,[5] the office's stated mission is to select enterprise cloud services, engineer them to meet Department requirements, obtain an authorization to operate, and continually develop and release updates to the enterprise offerings. CPMO offers five "State Enterprise" cloud services in its portfolio of services.[6] SIO's mandate in the FAM does not explicitly state it has cloud computing management responsibilities, but the office advertises two enterprise-level cloud services as leading products offered in its portfolio of services.[7] The total cost for the enterprise-level cloud services at the time of OIG's review was $533 million.[8]

IRM Reorganization

At the time of this review, IRM was in the process of a multi-year reorganization effort. Several offices were being subsumed, renamed, or consolidated under the reorganization effort, including CPMO and SIO. The enterprise cloud services offered by CPMO and SIO were transitioning to two new directorates established in IRM under the reorganization: Enterprise Infrastructure and Enterprise Services. When the reorganization effort is complete, the CPMO and SIO offices will no longer exist, but the enterprise cloud services they operate and maintain will continue under the two new directorates. As part of the reorganization, IRM was also in the process of revising the policies established in 5 FAM and 5 FAH, including the cloud computing policies. Both the reorganization and policy revision efforts were ongoing at the time of OIG's review.

Despite the ongoing IRM reorganization, providing enterprise cloud services remains a bureau priority. Goal 2, "Enable Modernization," of the Department's IT strategic plan for FY 2024-2026 identifies leveraging and continuing to implement enterprise cloud solutions as a guiding priority.[9] Goal 3, "Innovation – Mission effectiveness and modernization," in IRM's most recent Functional Bureau Strategy, identifies leveraging a shared, secure cloud environment as a key

[5] IRM's authority, responsibility, and organization are defined in 1 FAM 270.

[6] Enterprise cloud services offered by CPMO include State Enterprise-Amazon Web Services, State Enterprise-Azure, State Enterprise-Google Cloud Platform, State Enterprise-ServiceNow, and State Enterprise-Google Workspace.

[7] Enterprise cloud services offered by SIO include Enterprise Azure Cloud Services (EACS) and Microsoft Office 365 (O365).

[8] The $533 million total does not include labor contract costs. Additionally, the total includes costs for some Microsoft services that are not part of O365, but due to the structure of the contract, the additional Microsoft service costs could not be separated from the O365 costs.

[9] Department of State's Information Technology Strategic Plan (ITSP), Fiscal Year 2024-2026, December 2023.

objective.[10] Additionally, IRM's most recent Budget Resource Request submission identifies cloud computing as a priority area.

FINDINGS

OIG reviewed IRM's enterprise cloud services program management, including compliance with federal and Department security requirements, contract management and procurement requirements, product management[11] requirements, customer engagement and feedback processes, cost monitoring and cost control process, and the processes and controls used to govern the use of enterprise cloud services in the Department. The review did not include the Department's entire cloud portfolio, and it did not cover bureau- and office-level cloud systems and applications that IRM hosts in the enterprise cloud environments.

In accordance with IRM's stated goal of enabling modernization, OIG found IRM developed and deployed several enterprise-level cloud environments to help the Department's bureaus and offices efficiently and securely transition their systems and applications from on-premises data centers to cloud environments. However, OIG also determined IRM's enterprise cloud services program management required management attention in several areas. As described below, those areas are governance, security management, customer engagement, and contract and procurement management. Finally, OIG also found IRM's enterprise cloud service product management was done in accordance with Department guidelines.

Enterprise Cloud Service Governance

Cloud service governance is the process for ensuring effective, efficient, and compliant use of cloud computing resources in an organization. OIG reviewed IRM's governance processes related to cloud policy development and maintenance; coordination among IRM offices involved with managing and overseeing cloud services; tracking of alignment with Office of Management and Budget (OMB) and other federal cloud-related mandates; and tracking of cloud procurement requests and implementations to reduce the duplication of cloud services. OIG determined IRM's processes for updating Department cloud computing policies, the coordination among the enterprise cloud service providers and other IRM offices performing cloud-related functions, and the policies and guidelines for procuring cloud services in the Department require improvement, as described below.

IRM Did Not Establish Organizational Structure, Responsibility, and Authority for Cloud Services Management in Accordance With Federal Standards

The organizational structure and responsibilities for managing the enterprise cloud services in IRM did not comply with federal standards for internal controls. The Government

[10] Bureau of Information Management, Functional Bureau Strategy, Revised April 26, 2023.

[11] The National Institute of Standards and Technology defines product management as a set of processes for the development, modification, operation, and/or final disposition of software or hardware used in an information system.

Accountability Office's *Standards for Internal Control in the Federal Government*, Principle 3.03, requires agencies to develop an organizational structure with an understanding of the overall responsibilities and assign those responsibilities to offices to enable the organization to operate in an efficient and effective manner, comply with applicable laws and regulations, and reliably report quality information.[12]

OIG found that the offices in IRM performing work related to cloud computing did not always understand or were not aware of the cloud-related responsibilities other offices in IRM were assigned. Staff in some IRM offices believed other IRM offices were responsible for areas of cloud service management for which they were not assigned responsibility. Additionally, because roles and responsibilities were unclear, OIG found the IRM enterprise cloud service providers (e.g., CPMO and SIO) were making changes to the enterprise cloud environments but were not coordinating with offices that have a role in monitoring changes to enterprise cloud environments such as the Office of the Chief Architect and the Enterprise Chief Information Security Officer. OIG determined general and widespread lack of awareness of responsibilities occurred because cloud-related responsibilities assigned to IRM offices were not always codified in the FAM and FAH. Inadequate and poorly defined organizational structure and responsibilities can lead to inefficient and ineffective business processes and increase the risk of introducing new vulnerabilities to the Department's networks due to inadequate oversight.

> **Recommendation 1:** The Bureau of Diplomatic Technology should update the Foreign Affairs Manual and Foreign Affairs Handbook to define its organizational structure and assign the associated cloud-related responsibilities to the responsible offices in its organizational structure. (Action: DT)

Department Cloud Computing Policies Were Not Up To Date

The Department's cloud computing policies established in the FAM and FAH were not updated in accordance with Department standards. Department standard 18 FAM 201.1-3(A)(2) requires program offices to review directives for which they have substantive and coordinating responsibility annually and make changes to maintain the FAM's completeness and accuracy. OIG found IRM has not updated most of the cloud computing policies since 2015. Additionally, several of the policies contained references to processes, boards, and guidelines that no longer existed or were no longer in use. For example, 5 FAH-8 H-350, titled "Cloud Computing," primarily covers details about the Department's Cloud Computing Governance Board (CCGB), which no longer exists. Furthermore, 5 FAM 1110, titled "Cloud Computing Policy," references the federal "Cloud First" policy, which was superseded in 2019 by the updated federal "Cloud Smart" policy previously mentioned in this report.

IRM officials told OIG the bureau had not reviewed and updated the policies because they were waiting to revise all the policies the bureau is responsible for, including the cloud policies, as part of the ongoing reorganization effort. OIG also determined IRM did not assign responsibility

[12] Government Accountability Office, *Standards for Internal Control in the Federal Government*, pages 27-28 (GAO-14-704G, September 2014).

for updating the cloud policies, which contributed to the policies not being kept current. Outdated and obsolete policies that do not reflect actual business practices and organizational needs can result in wasted time and resources, increased operational costs, and failure to incorporate new systems or technology.

Recommendation 2: The Bureau of Diplomatic Technology should update its cloud computing policies in accordance with Department standards. (Action: DT)

IRM Did Not Communicate Changes to the Cloud Procurement Guidelines in Accordance With Federal Standards

IRM did not communicate changes to the policies and guidelines for procuring cloud computing services in accordance with federal standards. The Government Accountability Office's *Standards for Internal Control in the Federal Government*, Principle 14.03, requires federal agencies to communicate information down and across reporting lines to enable personnel to perform key roles in achieving objectives, addressing risks, and supporting established internal controls.[13] IRM established cloud procurement guidelines in 2015 in 5 FAH-8 H-350, which required the Department's CCGB to review each cloud procurement request and issue a recommendation to the Authorizing Official for adjudication. However, IRM officials told OIG the CCGB no longer existed, and the cloud procurement guidelines established in the FAH were no longer followed. At the time of this review, cloud procurements in the Department followed the general IT acquisition process.

In a 2018 Department cable,[14] IRM communicated the transition from the CCGB review and recommendation process to the Department's capital planning process and stated that the Cloud Computing Policy in the FAM and FAH would be updated to reflect these changes. OIG found the FAH was never updated to reflect the changes and it was unclear whether there was still an established process for Department offices and bureaus to follow when seeking to procure cloud services, or whether there were any Department-level approvals required before submitting cloud procurement requests. IRM officials told OIG when they disbanded the CCGB and its business processes, the bureau did not establish a replacement cloud procurement process and therefore could not communicate a new process to the Department. Unclear or absent policies and guidelines for procuring cloud services increase the risk cloud services could be duplicated across the Department leading to wasted funds or inefficient use of government resources.

Recommendation 3: The Bureau of Diplomatic Technology should update its cloud service procurement policies and guidelines and communicate the changes to the Department. (Action: DT)

[13] Government Accountability Office, *Standards for Internal Control in the Federal Government*, page 60 (GAO-14-704G, September 2014).

[14] Cable 18 STATE 105736, "Transition of the Cloud Computing Governance Board and Approval Process," October 18, 2018.

Enterprise Cloud Service Security Management

OIG reviewed the security requirements for the Department's enterprise cloud services by verifying each system had an authorization to operate, defined system security plans and assessments, information system contingency plans, plans of action and milestones documents, change control processes, notifications of changes, security management processes, system logging and monitoring, and incident response procedures.

Although cloud system security governance policies in the FAM and FAH were outdated and obsolete, OIG found IRM established internal cyber procedures to meet federal requirements included in the National Institute of Standards and Technology Risk Management Framework,[15] OMB Circular A-130,[16] OMB Memoranda M-22-09,[17] and M-21-31,[18] and Cybersecurity and Infrastructure Security Agency[19] recommendations. For example, the enterprise cloud offerings OIG reviewed all went through the Department's Assessment and Authorization process, in addition to being FedRAMP approved. OIG determined enterprise cloud systems and services generally met the Department's day-to-day computing and communications security requirements, with the exceptions described below.

Department Configuration Management Standards Were Inconsistent for Enterprise Cloud Services

The Department's configuration management standards were inconsistent for enterprise cloud services. Department standards in 5 FAM 862.3a state applications which function outside the local area network, such as OpenNet,[20] must obtain IT Configuration Control Board (IT CCB) approval prior to use. Additionally, 5 FAH-8 H-351.3 requires the CCGB to review all cloud systems and applications. OIG found not all cloud applications/services and baseline configurations were approved through the IT CCB or reviewed by the now disbanded CCGB. For example, CPMO did not obtain IT CCB approval for cloud applications or services in Azure Commercial Cloud, Amazon Web Services, Google Workspace, or Google Cloud Platform. Instead, CPMO approved cloud service offerings through its own local configuration board, allowed by 5 FAM 861.1f,[21] but contrary to the policy established in 5 FAM 862.3a.

[15] The Risk Management Framework, presented in NIST SP 800-37, provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle.

[16] OMB Circular A-130, "Managing Information as a Strategic Resource" (July 28, 2016).

[17] OMB Memorandum, M-22-09 "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles" (January 26, 2022).

[18] OMB Memorandum M-21-31 "Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents" (August 27, 2021).

[19] The Cybersecurity and Infrastructure Security Agency is the operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience. See www.cisa.gov/about.

[20] OpenNet is the Department's Sensitive But Unclassified network.

[21] For those systems which do not fall under the OpenNet or ClassNet authorization boundaries, system owners must develop and maintain Department configuration management plans for systems under their authority as part of the systems security documents required for authorization and accreditation.

Furthermore, SIO maintained a standard operating environment[22] for the Enterprise Azure Cloud System without IT CCB approval, contrary to 5 FAM 861.2.d(4) and (8).[23] Staff told OIG Department policy was outdated and did not keep up with the nuances of cloud computing, as described earlier in this report. Additionally, because cloud systems and applications were accessed through an approved internet browser on OpenNet workstations, IRM staff considered these systems and applications to fall outside OpenNet and therefore, not subject to IT CCB approval. Inconsistent configuration management policies pose a risk to the confidentiality, integrity, or accessibility of Department systems and data.

Recommendation 4: The Bureau of Diplomatic Technology should review Department configuration management policies for inconsistencies and update them to align with federal cloud policies. (Action: DT)

Cloud Security Guidelines Did Not Follow Department Standards

The Department did not maintain cloud security principles referenced in 5 FAH-8 H-354.2b(3). The Department published cloud security principles in 2015 but withdrew them in 2017 without providing a replacement. Additionally, the Department has not published cloud security configuration settings for systems owners to follow, as required by 12-FAH-10 H-222.5. Following federal risk management guidelines, SIO established configuration guidelines for its Enterprise Azure Cloud Services customers and coordinated those guidelines through the Bureau of Diplomatic Security.[24] However, those guidelines only applied to SIO customers and not to the entire Department. IRM and the Bureau of Diplomatic Security staff both told OIG the implementation of cloud computing services in the Department was moving faster than the policies to support them. Inconsistent policies and misconfigured systems may result in a loss of confidentiality, integrity, or accessibility of Department systems and data.

Recommendation 5: The Bureau of Diplomatic Technology, in coordination with the Bureau of Diplomatic Security, should follow Department standards for cloud security guidelines. (Action: DT, in coordination with DS)

Enterprise Cloud Systems Encryption Did Not Comply With Department Standards

Enterprise cloud systems encryption key management did not comply with Department standards. According to 5 FAH-8 H-354.2b(4), Department data centers are required to maintain, generate, and control encryption keys. Instead, OIG found the Department enterprise cloud systems used the cloud service providers' encryption keys. Cloud system staff said some

[22] Per 5 FAM 861.2, a standard operating environment is a specification for using a standard architecture and applications within a Department information system. It supports the development of strong configuration management plans for the computing environments commonly used throughout the Department.

[23] Guidance in 5 FAM 861.2.d(4) and (8) requires the standard operating environments to be approved by the IT CCB.

[24] Guidance in 1 FAM 262.9-4.1 designates the Bureau of Diplomatic Security's Emerging Technologies Division (DS/CTS/TIE/ET) with the responsibility to research, develop, and maintain security configuration standards and principles for Departmental implementation of IT hardware, operating systems, and applications.

cloud systems did not support external encryption key management, and therefore, thought this requirement should be reassessed. Without using Department encryption keys for cloud encryption, cloud data could be at risk of compromise.

Recommendation 6: The Bureau of Diplomatic Technology should comply with Department encryption key management requirements for enterprise cloud systems. (Action: DT)

Enterprise Cloud Service Product Management

Product Owners Performed Cloud Responsibilities According to Department Guidelines

OIG found product owners performed their cloud responsibilities according to Department guidelines. For example, product owners followed systems development lifecycle methodologies for their respective cloud platform development and maintenance activities as described in 12 FAH-10 H-342.2 and 5 FAH-5 H-211. Product owners told OIG they used an agile methodology[25] for cloud development and maintenance. OIG reviewed the documented methodology and found the process included recurring meetings with developers, technical staff, information security staff, and system owners to discuss progress and next steps for systems review. OIG also determined the respective cloud teams properly maintained systems development documentation in document repositories. Furthermore, OIG found product owners were participants in the change management process for cloud platforms, with appropriate approvals by government personnel in accordance with 12 FAH-10 H-222.2-1. Specifically, CPMO deployed an automated approval process for changes to cloud products and services which included required approvals by both the information systems security officer and the system owner.

Enterprise Cloud Service Customer Engagement

Teams in both CPMO and SIO handled customer engagement. Both customer engagement teams focused on providing services to customers to help determine which cloud platform would best suit their business and technical needs. The customer engagement teams' services included overseeing all cloud subscription acquisition, customer consumption monitoring and cost optimization, customer financial on-boarding and off-boarding, and cloud agreements facilitation. OIG's review of customer engagement found deficiencies in the areas below.

Bureau Lacked Communication Plan to Explain Cloud Responsibilities and Available Cloud Products and Services to Customers

According to OIG interviews, customers told OIG they were unclear on cloud responsibilities between them and IRM, as well as details on what cloud products and services are available. Specifically, customers were not clear on cloud responsibilities concerning billing, cost structure, monitoring, application development, and security controls. Also, they were

[25] The agile methodology is a project management approach that involves breaking the project into phases and emphasizes continuous collaboration and improvement. Teams follow a cycle of planning, executing, and evaluating.

uncertain on updates and changes to cloud environments and how that would impact cloud responsibilities. Additionally, OIG found both CPMO and SIO did not communicate consistently with their domestic and overseas users about what cloud products and services were available. Customers told OIG they learned of available cloud products and services via word of mouth from other Department personnel. In some cases, customers conducted their own research to gather information on cloud products and services because they did not know where to locate such information and guidance.

IRM staff told OIG they provided customers with a terms and conditions agreement outlining both parties' cloud responsibilities; however, OIG found some customers did not receive that documentation. Furthermore, IRM staff acknowledged to OIG that they could reach out more proactively to customers about their cloud products and services, noting increased contact with customers would help IRM meet the Department's modernization goals.

In accordance with the Government Accountability Office's S*tandards for Internal Control in the Federal Government*, Principles 14.08 and 15.01, management should communicate with external customers the necessary information to achieve the entity's objectives.[26] Those standards also state management should periodically evaluate the method of communication to ensure the organization has the appropriate tools to communicate in a timely manner. Without adequate communication with its customers, there is potential risk IRM will not meet its cloud management goals.

> **Recommendation 7:** The Bureau of Diplomatic Technology should implement a communication plan for its domestic and overseas customers to include details on cloud responsibilities and available cloud products and services. (Action: DT)

Bureau Lacked a Formal Process for Gathering Customer Feedback

OIG found IRM lacked a formal process for gathering routine feedback from customers on IRM's cloud services and platforms. Customers told OIG they provided feedback and asked questions during informal meetings with cloud teams or at meetings with IRM that they requested. In lieu of a formal process, product owners provided their personal contact information to customers as a way to communicate if issues arose. IRM staff told OIG they recognized the importance of feedback and were working on establishing a formal process. According to 18 FAM 301.1-4b, monitoring and data collection efforts should be integrated through the life cycle of a program, project, or process as they inform ongoing adjustments and improvements. Furthermore, 18 FAM 301.4-3b states all bureaus and offices must develop a monitoring plan for their programs and projects including ongoing data collection to assess whether the programs are achieving the expected results. Without a formal process for gathering regular customer feedback, IRM is unable to track trends, identify recurring issues, and ensure customer needs are being met.

[26] Government Accountability Office, *Standards for Internal Control in the Federal Government*, pages 61-62 (GAO-14-704G, September 2014).

Recommendation 8: The Bureau of Diplomatic Technology should implement a formal process for gathering regular customer feedback on its cloud products and services. (Action: DT)

Enterprise Cloud Contract and Procurement Management

CPMO and SIO had seven Department enterprise-level cloud services awards with a total cost of $533 million. OIG reviewed the files and documentation for all seven awards in the Integrated Logistics Management System (ILMS),[27] the Contractor Performance Assessment Reporting System (CPARS),[28] as well as documentation from Bureau of Administration, Office of Acquisitions Management (AQM), and IRM SharePoint files. AQM provided IRM with two contracting officers (COs) and one contract specialist, who managed these awards. Additionally, three IRM staff served as contracting officer's representatives (CORs). There were no assistant CORs or government technical monitors for any of the awards. OIG met with the COs, CORs, and the contract specialist for these awards.

OIG determined the Department's processes and procedures for managing enterprise-level cloud service procurements generally followed applicable laws, policies, and standards, with the exceptions noted below.

Contract File Management Did Not Fully Comply With Department Standards

OIG reviewed contract files and documentation for all seven enterprise-level cloud services awards and found contract file management did not fully comply with Department and federal standards. Specifically, OIG found the files did not include some key documents, which IRM and AQM staff were unable to provide, or they had documents that were not properly executed. Specifically,

- The CORs and COs did not complete any of the 12 mandatory annual contractor performance assessments[29] in CPARS.gov, the federal system of record for contractor performance assessments (14 FAH-2 H-572a, c, and d, and Federal Acquisition Regulation (FAR) 42.1502(a) and (b)).
- Four of the seven awards were missing National Defense Authorization Act Section 889 documentation from vendors stating they were not using equipment or services from

[27] 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, according to 14 FAM 121c.

[28] CPARS is the government-wide evaluation reporting tool for all past performance reports on contracts and orders. An annual performance assessment must be completed in the system for each contract above the simplified acquisition threshold of $250,000, according to Federal Acquisition Regulation (FAR) 42.1502(a) and (b).

[29] Five of the Department's seven enterprise-level cloud services contracts required annual CPARS performance assessments, some for multiple years, for a total of 12 CPARS assessments. Performance assessments are to be completed in the CPARS.gov system by CORs and COs within 120 days of the end of the performance period. None of the 12 required assessments were in the system. Any copies outside the CPARS.gov system would not comply with FAR or Department standards.

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) and 52.204-25(b)(1)-(2)).

- Five of the seven awards were sole source awards and not competed. These awards each required a fully approved justification document prior to the start of the award. Only one of the five had a fully approved justification. The other four were signed by the COR but not by the CO or Department competition advocate as required (FAR 6.303 and FAR 6.304).
- Two of the seven awards were missing Statements of Work (5 FAM 1114f).
- Six of the seven awards were missing acquisition plans, or they were not signed by the required parties. Acquisition plans are important because they specify the type of award to be used, cost, period of performance, and other important information. FAR 7.104(c) requires CO concurrence with acquisition plans. Three of the seven awards did not have acquisition plans. The other three had acquisition plans that were only signed by the COR, but not by the CO.
- Five of the seven awards were missing required copies of COR letters of designation in contract files (FAR 1.604(a), 14 FAH-2 H-517a(1)).
- CORs only maintained COR files for three of the seven awards in ILMS's COR e-Filing module as required (14 FAH-2 H-142b(16)(b)).
- One of the seven awards did not have any documentation in ILMS, the Department's system of record for procurement, or in CPARS.gov due to technical issues[30] (14 FAH-2 H-572a, c, and d, and FAR 42.1502(a) and (b)).

Despite these issues, OIG's interviews with IRM CORs and AQM contracting staff and reviews of other documentation showed the Department monitored the enterprise-level cloud services contracts, received the goods and services for which it had contracted, and addressed contractor performance when issues arose.

IRM and AQM staff told OIG they were unfamiliar with some requirements, had technical issues using some systems due to understaffing for acquisition staff and other full-time duties for CORs, which took precedence over file management. Non-compliance with contract file and COR file requirements increases the risk of contract mismanagement.

Recommendation 9: The Bureau of Diplomatic Technology, in coordination with the Bureau of Administration, should bring its enterprise-level cloud services contract and contracting officer's representative files into compliance with Department and federal requirements. (Action: DT, in coordination with A)

[30] Key contract documents usually transfer automatically to ILMS from the Bureau of the Comptroller and Global Financial Services' Financial Management System, but they did not for this contract. At the time of the inspection, the CO was working to get the problem corrected.

Contracting Officer's Representative Program Did Not Fully Comply With Department Standards

IRM's enterprise-level cloud services COR program did not fully comply with Department standards. OIG reviewed the COR program and found deficiencies in COR training and other related COR issues. OIG found none of the three staff serving as CORs were fully qualified, due to the following issues:

- One of the three staff serving as a COR lacked certification issued by the Department's Office of the Procurement Executive (14 FAH-2 H-143.1h).
- Two of the three CORs were missing COR delegation letters for five of the seven awards they were overseeing (14 FAH-2 H-143.2). Delegation letters are important because they instruct CORs on their duties and any restrictions on their activities.
- Two of the three CORs did not have COR training or had expired COR training (14 FAH-2 H-143.1), and one COR had not completed the required annual ethics training (13 FAM 301.2-3a).[31]
- One of the three CORs could not provide documentation that they had submitted the required OGE-450 annual financial disclosure statement (14 FAH-2 H-151c).[32]

IRM and AQM staff told OIG these problems occurred because COR and contracting staff did not believe some of the awards required formal COR oversight, and the other full-time duties of the CORs made it difficult for CORs to find the time to complete COR program requirements. A non-compliant COR program increases the risk of contract mismanagement and required annual contractor performance assessments not being completed.

Recommendation 10: The Bureau of Diplomatic Technology should bring the enterprise-level cloud services contracting officer's representative program into compliance with Department standards. (Action: DT)

Contracting Personnel Did Not Follow All Cloud Services Procurement Requirements

The COs, CORs, and contract specialist responsible for the Department's enterprise cloud services awards told OIG they did not follow all cloud services procurement requirements. Although some of these were related to IRM policies, which needed to be updated, others were requirements found in the Department's acquisition regulation and OMB guidance. OIG found the following cloud services procurement specific requirements were not being implemented.

- An IT security plan must be submitted to the CO and COR within the first 30 days (Department of State Acquisition Regulation 652.239-71(c)).

[31] Department guidance in 13 FAM 301.2-3a states all staff who are required to complete annual financial disclosure reports must also complete annual ethics training. According to 14 FAH-2 H-151c, all CORs and government technical monitors are required to file an annual financial disclosure report.

[32] According to 14 FAH-2 H-151c, FAR 3.104 and the Department of State Acquisition Regulation Part 603 also prescribe procedures applicable to Department employees regarding standards of conduct and prohibited business practices.

- All Department cloud services procurements must have Federal Risk and Authorization Management Program authorizations. OIG found two of the seven awards did not have the required authorization (OMB Memorandum for Chief Information Officers, "Security Authorization of Information Systems in Cloud Computing" (December 8, 2011)).
- An incident response and mitigation capability for security and privacy incidents for cloud services must be established (OMB Memorandum for Chief Information Officers (December 8, 2011)).
- The provider must route their traffic through a service that meets the requirements of the Trusted Internet Connection program (OMB Memorandum for Chief Information Officers (December 8, 2011)).

IRM and AQM staff told OIG they were unfamiliar with these requirements or where to find them, and acknowledged they were not implementing them. Non-compliance with cloud services procurement specific requirements increases risks to IT security and reduces the Department's ability to identify and mitigate those risks.

Recommendation 11: The Bureau of Diplomatic Technology, in coordination with the Bureau of Administration, should develop and communicate guidance specifying what cloud services procurement requirements staff need to implement, which staff are responsible for implementing them, and how the requirements should be implemented. (Action: DT, in coordination with A)

RECOMMENDATIONS

OIG provided a draft of this targeted review to Department stakeholders for their review and comment on the findings and recommendations. OIG issued the following recommendations to the Bureau of Diplomatic Technology. The complete responses can be found in Appendix B.

Recommendation 1: The Bureau of Diplomatic Technology should update the Foreign Affairs Manual and Foreign Affairs Handbook to define its organizational structure and assign the associated cloud-related responsibilities to the responsible offices in its organizational structure. (Action: DT)

Management Response: In its May 28, 2024, response, the Bureau of Diplomatic Technology 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 Diplomatic Technology updated the Foreign Affairs Manual and Foreign Affairs Handbook to define its organizational structure and assigned the associated cloud-related responsibilities to the responsible offices in its organizational structure.

Recommendation 2: The Bureau of Diplomatic Technology should update its cloud computing policies in accordance with Department standards. (Action: DT)

Management Response: In its May 28, 2024, response, the Bureau of Diplomatic Technology 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 Diplomatic Technology updated its cloud computing policies in accordance with Department standards.

Recommendation 3: The Bureau of Diplomatic Technology should update its cloud service procurement policies and guidelines and communicate the changes to the Department. (Action: DT)

Management Response: In its May 28, 2024, response, the Bureau of Diplomatic Technology 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 Diplomatic Technology updated its cloud service procurement policies and guidelines and communicated the changes to the Department.

Recommendation 4: The Bureau of Diplomatic Technology should review Department configuration management policies for inconsistencies and update them to align with federal cloud policies. (Action: DT)

Management Response: In its May 28, 2024, response, the Bureau of Diplomatic Technology 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 Diplomatic Technology reviewed Department configuration management policies for inconsistencies and updated them to align with federal cloud policies.

Recommendation 5: The Bureau of Diplomatic Technology, in coordination with the Bureau of Diplomatic Security, should follow Department standards for cloud security guidelines. (Action: DT, in coordination with DS)

Management Response: In its May 28, 2024, response, the Bureau of Diplomatic Technology 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 Diplomatic Technology followed Department standards for cloud security guidelines.

Recommendation 6: The Bureau of Diplomatic Technology should comply with Department encryption key management requirements for enterprise cloud systems. (Action: DT)

Management Response: In its May 28, 2024, response, the Bureau of Diplomatic Technology 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 Diplomatic Technology complied with Department encryption key management requirements for enterprise cloud systems.

Recommendation 7: The Bureau of Diplomatic Technology should implement a communication plan for its domestic and overseas customers to include details on cloud responsibilities and available cloud products and services. (Action: DT)

Management Response: In its May 28, 2024, response, the Bureau of Diplomatic Technology 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 Diplomatic Technology implemented a communication plan for its domestic and overseas customers to include details on cloud responsibilities and available cloud products and services.

Recommendation 8: The Bureau of Diplomatic Technology should implement a formal process for gathering regular customer feedback on its cloud products and services. (Action: DT)

Management Response: In its May 28, 2024, response, the Bureau of Diplomatic Technology 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 Diplomatic Technology implemented a formal process for gathering regular customer feedback on its cloud products and services.

Recommendation 9: The Bureau of Diplomatic Technology, in coordination with the Bureau of Administration, should bring its enterprise-level cloud services contract and contracting officer's representative files into compliance with Department and federal requirements. (Action: DT, in coordination with A)

Management Response: In its May 28, 2024, response, the Bureau of Diplomatic Technology 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 Diplomatic Technology's enterprise-level cloud services contract and contracting officer's representative files complied with Department and federal requirements.

Recommendation 10: The Bureau of Diplomatic Technology should bring the enterprise-level cloud services contracting officer's representative program into compliance with Department standards. (Action: DT)

Management Response: In its May 28, 2024, response, the Bureau of Diplomatic Technology 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 Diplomatic Technology's enterprise-level cloud services contracting officer's representative program complied with Department standards.

Recommendation 11: The Bureau of Diplomatic Technology, in coordination with the Bureau of Administration, should develop and communicate guidance specifying what cloud services procurement requirements staff need to implement, which staff are responsible for implementing them, and how the requirements should be implemented. (Action: DT, in coordination with A)

Management Response: In its May 28, 2024, response, the Bureau of Diplomatic Technology 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 Diplomatic Technology developed and communicated guidance specifying what cloud services procurement requirements staff need to implement, which staff are responsible for implementing them, and how the requirements should be implemented.

APPENDIX A: OBJECTIVES, SCOPE, AND METHODOLOGY

This review was conducted from January 2 to March 18, 2024, 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).

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, this review focused on the Bureau of Information Resource Management's (IRM) cloud services program management. OIG's specific objectives were to determine whether:

- Enterprise cloud systems complied with federal and Department security requirements.
- IRM offices responsible for managing the enterprise cloud systems implemented required product management and customer engagement processes and procedures.
- IRM established internal controls to govern the use of enterprise cloud systems in the Department.
- Enterprise cloud systems complied with federal and Department contracting and procurement requirements.

OIG used a risk-based approach to prepare for this review. OIG conducted portions of the review 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, such as established standard operating procedures, policy and strategy documents, internal controls related to governing the use of cloud systems, communication with enterprise cloud system stakeholders, and security plans and assessments.

At the conclusion of this review, OIG shared 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.

Team Leader Brett Fegley, Jay Biddulph, Vandana Patel, Paul Sanders, and Brian Smith conducted this review. Other report contributors included Leslie Gerson.

APPENDIX B: MANAGEMENT RESPONSE

United States Department of State

Washington, DC 20520

UNCLASSIFIED

May 28, 2024

NOTE FOR UNITED ACTING ASSISTANT INSPECTOR GENERAL FOR INSPECTIONS ARNE B. BAKER

FROM: DT – Kelly E. Fletcher

SUBJECT: Response to Draft OIG Report: Targeted Review of the Bureau of Information Resource Management's Cloud Services Program Management

Diplomatic Technology has reviewed the draft OIG inspection report. We provide the following comments in response to the recommendations provided by OIG.

Recommendation 1: The Bureau of Information Resource Management should update the Foreign Affairs Manual and Foreign Affairs Handbook to define its organizational structure and assign the associated cloud-related responsibilities to the responsible offices in its organizational structure.

Management Response: Diplomatic Technology concurs with this recommendation. DT will update the 1 FAM 270 and the Foreign Affairs Handbook defining organizational structure and assigning cloud related responsibilities.

Recommendation 2: The Bureau of Information Resource Management should update its cloud computing policies in accordance with Department standards. (Action: IRM)

Management Response: Diplomatic Technology concurs with this recommendation. DT will update its Cloud Computing policies 5 FAH-8 H-350 and 5 FAM 1110 to align with Department standards.

Recommendation 3: The Bureau of Information Resource Management should update its cloud service procurement policies and guidelines and communicate the changes to the Department. (Action: IRM)

Management Response: Diplomatic Technology concurs with this recommendation. DT provides the link to the newly published 5 FAM 910 Information Technology (IT) Acquisition Policies 5 FAM 910 Information Technology (IT) Acquisition Policies. (Also see Tab 1, DTM 24-004)

Recommendation 4: The Bureau of Information Resource Management should review Department configuration management policies for inconsistencies and update them to align with federal cloud policies. (Action: IRM)

Management Response: Diplomatic Technology concurs with this recommendation. DT will review Department configuration management policies for inconsistencies and update them to align with federal cloud policies.

Recommendation 5: The Bureau of Information Resource Management, in coordination with the Bureau of Diplomatic Security, should follow Department standards for cloud security guidelines. (Action: IRM, in coordination with DS)

Management Response: Diplomatic Technology concurs with this recommendation. DT will review Department standards for cloud security guidelines and ensure they are being followed.

Recommendation 6: The Bureau of Information Resource Management should comply with Department encryption key management requirements for enterprise cloud systems. (Action: IRM)

Management Response: Diplomatic Technology concurs with this recommendation. DT will review Department standards and update policy

for encryption key management requirements for enterprise cloud systems as appropriate.

Recommendation 7: The Bureau of Information Resource Management should implement a communication plan for its domestic and overseas customers to include details on cloud responsibilities and available cloud products and services. (Action: IRM)

Management Response: Diplomatic Technology concurs with this recommendation. DT will implement a communication plan for its domestic and overseas customers that details cloud responsibilities and available products and services.

Recommendation 8: The Bureau of Information Resource Management should implement a formal process for gathering regular customer feedback on its cloud products and services. (Action: IRM)

Management Response: Diplomatic Technology concurs with this recommendation. DT will implement a formal process for gathering regular customer feedback.

Recommendation 9: The Bureau of Information Resource Management, in coordination with the Bureau of Administration, should bring its enterprise-level cloud services contract and contracting officer's representative files into compliance with Department and federal requirements. (Action: IRM, in coordination with A)

Management Response: Diplomatic Technology concurs with this recommendation. DT, in coordination with A-bureau, will work to bring its enterprise-level cloud services contract and contracting officer's representative files into compliance.

Recommendation 10: The Bureau of Information Resource Management should bring the enterprise-level cloud services contracting officer's

representative program into compliance with Department standards. (Action: IRM)

Management Response: Diplomatic Technology concurs with this recommendation. DT will bring the enterprise-level cloud services contracting officer's representative program into compliance.

Recommendation 11: The Bureau of Information Resource Management, in coordination with the Bureau of Administration, should develop and communicate guidance specifying what cloud services procurement requirements staff need to implement, which staff are responsible for implementing them, and how the requirements should be implemented. (Action: IRM, in coordination with A)

Management Response: Diplomatic Technology concurs with this recommendation. DT provides the link to the newly published 5 FAM 910 Information Technology (IT) Acquisition Policies 5 FAM 910 INFORMATION TECHNOLOGY (IT) ACQUISITION POLICIES.

If you have any questions or concerns, please contact Craig Hootselle.

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