



Office of Inspector General
United States Department of State

ISP-I-22-07

Office of Inspections

January 2022

**Inspection of the Bureau
of Administration,
Office of the Executive Director**

DOMESTIC OPERATIONS



HIGHLIGHTS

Office of Inspector General
United States Department of State

ISP-I-22-07

What OIG Inspected

OIG inspected information technology services, evaluation report tracking, and resource management operations of the Bureau of Administration, Office of the Executive Director.

What OIG Recommends

OIG made 12 recommendations to the Bureau of Administration.

In its comments on the draft report, the Bureau of Administration concurred with all 12 recommendations. OIG considers all 12 recommendations resolved. 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.

January 2022

OFFICE OF INSPECTIONS
DOMESTIC OPERATIONS

Inspection of the Bureau of Administration, Office of the Executive Director

What OIG Found

- Overall, the Bureau of Administration's Office of the Executive Director was fulfilling its mission in compliance with Department of State requirements. However, there were some significant information technology challenges that required management attention.
- The Information Technology Services Division had expanded its roles and responsibilities beyond those outlined in the Foreign Affairs Manual due to lack of internal controls. As a result of its expanded scope of functions without a commensurate increase in resources, the staff was unable to maintain routine, daily information management operations and maintenance, which contributed to information technology security vulnerabilities.
- Although the office met and sometimes exceeded the requirement to conduct annual evaluations of its programs and operations, it did not implement a system to track recommendations made in its evaluation reports which weakened the positive impact of the bureau's otherwise robust evaluation process, including the identification of possible cost savings.
- The Human Resources Division was unable to meet its customer service standards as a result of a 43 percent vacancy rate in U.S. direct-hire positions.
- The office had approximately \$8 million in unliquidated obligations with no activity for more than 1 year.

CONTENTS

| | |
|--|----|
| CONTEXT | 1 |
| OVERVIEW | 2 |
| EXECUTIVE OFFICE OPERATIONS..... | 3 |
| Information Management | 3 |
| Collaborative Strategy and Management | 9 |
| Resource Management | 11 |
| RECOMMENDATIONS..... | 14 |
| PRINCIPAL OFFICIALS | 18 |
| APPENDIX A: OBJECTIVES, SCOPE, AND METHODOLOGY | 19 |
| APPENDIX B: MANAGEMENT RESPONSE..... | 21 |
| ABBREVIATIONS | 26 |
| OIG INSPECTION TEAM MEMBERS..... | 27 |

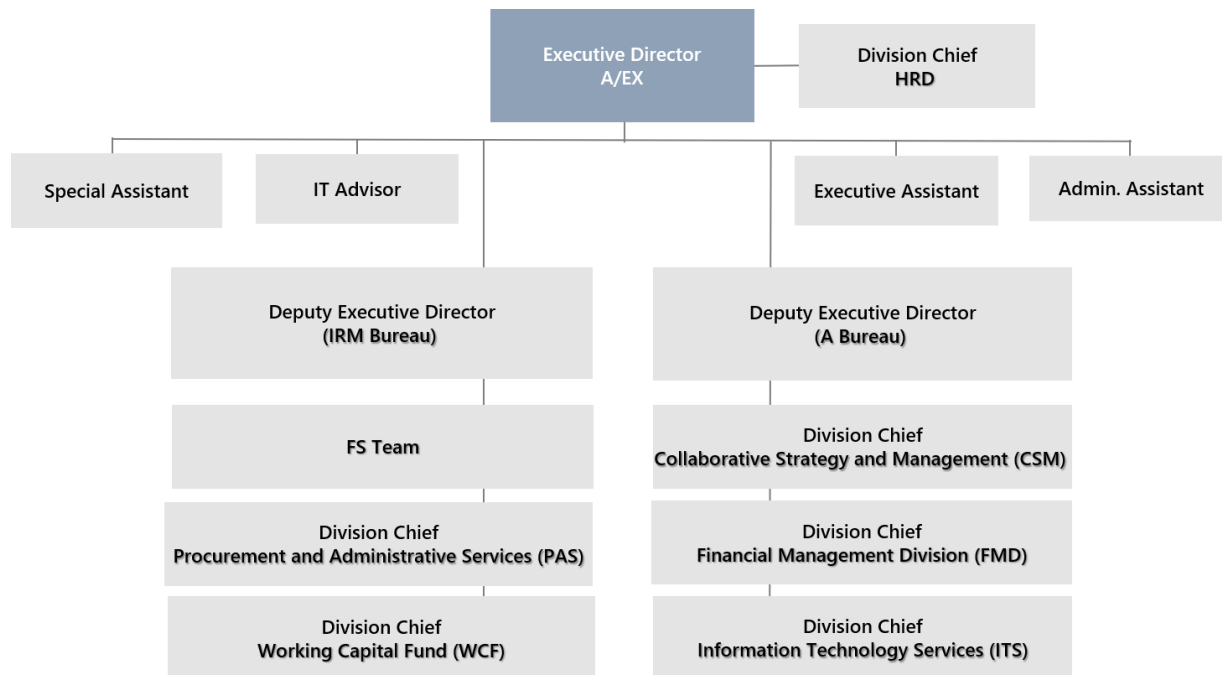
CONTEXT

The Bureau of Administration (A Bureau), Office of the Executive Director (A/EX) supports the Assistant Secretary for Administration and the Under Secretary for Management through the provision of executive management and administrative services, including management analysis, financial management, human resources management, information resources management, and general services. A/EX also serves as the Executive Office for the Bureau of Information Resource Management (IRM) and provides management support to two smaller offices: the Office of Fine Arts and the Office of Small and Disadvantaged Business Utilization. Additionally, A/EX provides Presidential and Vice-Presidential travel support services for White House international travel. A/EX serves approximately 2,500 employees in the A Bureau and IRM—its two largest customers.

Although A/EX is authorized a total of 104 U.S. direct-hire positions, it had 68 direct-hire employees at the time of the inspection. The 36 unfilled positions represented a vacancy rate of approximately 35 percent. The Human Resources Division had the highest number of vacancies, with 23 of 40 U.S. direct-hire positions filled (43 percent vacancy rate). A/EX also is staffed by 91 third-party contractors, the majority of whom work in the Information Technology Services Division.

OIG evaluated the bureau's information management, collaborative strategy and management, and resource management operations consistent with Section 209 of the Foreign Service Act of 1980.¹

¹ See Appendix A. Evaluation of the A/EX Division of the Working Capital Fund was not included within the scope of this inspection. Working Capital Fund operations are reviewed by the OIG Office of Audits.

Figure 1: Office of the Executive Director Organization Chart

Source: OIG generated from information provided by A/EX.

OVERVIEW

Based on a variety of OIG questionnaires, including a customer service survey of A Bureau and IRM users of A/EX services, staff interviews, and document reviews, OIG determined that A/EX generally fulfilled its mission in compliance with the responsibilities outlined in 1 Foreign Affairs Manual (FAM) 212.1. As stated in 1 FAM 212.1a and d, A/EX's mission is broader than supporting only the A Bureau. A/EX also provides services to other bureaus and offices, as discussed above and in the Information Management section of this report.

As part of its 1 FAM 212.1 mandate, A/EX coordinates strategic planning for A Bureau.² OIG reviewed A/EX's Functional Bureau Strategy (FBS) process and found it conformed with Department of State (Department) guidance in 18 FAM 301.2-4(B)b(1)(c) and 18 FAM 301.2-4(D)c on assessing progress toward achieving goals and objectives and having a regular review strategy.³ A/EX's commitment to the FBS process was noteworthy in its sustainability and thoroughness. A/EX staff maintained, regularly updated, and posted an online FBS tracker and master spreadsheet showing FBS goals by category, associated Bureau Resource Requests, alignment with the Joint Strategic Plan, and steps the bureau was taking to meet its goals. In addition, A/EX hosted robust quarterly FBS reviews which informed senior leadership's strategic

² Within A/EX, the Collaborative Strategy and Management Division led the Functional Bureau Strategy development and tracking process.

³ FBS is a 4-year strategic plan that outlines the bureau's priority setting and resource allocation in support of the administration's priorities in the Joint Department of State-USAID Strategic Plan.

decision-making. A/EX also undertook evaluations of A Bureau-specific programs and processes as part of the FBS process. Program evaluations are discussed later in this report.

A/EX was led by a Senior Executive Service Executive Director who, at the time of the inspection, had been in the position for less than 1 year. Previously, she served in the operations and oversight function of the Bureau of Intelligence and Research. In A/EX, she was assisted by two Deputy Executive Directors, both of whom assumed their positions in 2019. One Deputy Executive Director had served in A/EX since 2002 and therefore brought institutional knowledge and continuity to the leadership team.

EXECUTIVE OFFICE OPERATIONS

OIG reviewed A/EX's programs and responsibilities in several areas, including information technology (IT); strategic planning and program administration; human resources; financial management; and procurement and support. A/EX's performance in those areas generally met Department standards, with the exceptions noted below regarding IT services, program evaluation, and resource management.

Information Management

According to 1 FAM 212.1-5, the A/EX Information Technology Services Division (ITS) is responsible for providing the bureau's information management leadership and IT services, establishing bureau IT policies, and conducting IT security oversight for the bureau's information systems. At the time of the inspection, the division consisted of 12 direct-hire employees and 42 contract personnel. This staff operated and maintained more than 100 information systems⁴ and one network that support both bureau and Department⁵ operations. During the inspection, OIG reviewed the effectiveness of the division's management and the Information Systems Security Officer (ISSO) program, including implementation of the system development lifecycle, its assessment, and its authorization; configuration management; contingency planning; system operations and maintenance; and knowledge management processes.

Information Technology Services Division Took Steps to Improve Operations, But Challenges Remain

At the time of the inspection, ITS faced significant challenges related to funding and staffing resources which led to program management issues and, in some cases, to increased IT security risks. The division implemented several changes to address some of these challenges. For instance, the ITS Division Director created a program management office to help with financial management and project oversight, increased the focus on standardizing and documenting ITS

⁴ Forty-six of these systems are subsystems of the cloud platform known as Myapps, which ITS operates.

⁵ ITS provides the following services to the Department: video streaming services, employee data and knowledge management, Government form submission and management services, and cloud application hosting and management support.

processes and procedures, established an intake review board to review proposed work and to make decisions considering resource availability and bureau mission alignment, and updated ITS cost models to better project and account for the full cost of the services it was providing. At the time of the inspection, however, 7 of the division's 19 direct-hire staff positions were vacant, which created challenges for assigning work and supervising staff. Despite the steps taken by ITS to improve its operations, OIG identified the issues described below.

Division Roles and Services Did Not Align With Roles Outlined in the Foreign Affairs Manual

ITS delivered IT services to bureaus and offices outside the A Bureau, a role that was inconsistent with its responsibilities outlined in Department guidance. Specifically, guidance in 1 FAM 212.1-5 states that ITS should provide IT leadership, management, policy, and security oversight for the Bureau of Administration. However, OIG found that ITS provided services beyond this mandate and acted as a service provider to the entire Department.

OIG found that ITS provided direct support to 21 Department bureaus in addition to the A Bureau. ITS acted as a service provider for cloud computing hosting and development efforts and directly supported development projects for the Department's Sensitive But Unclassified network for bureaus in addition to the A Bureau. For example, ITS procured a cloud computing⁶ product and offered the product's services to bureaus that had yet to establish similar capabilities. This expanded mission scope occurred because A/EX leadership, over at least 5 years prior to this inspection, did not establish internal controls to limit the ITS mission to the scope detailed in 1 FAM 212.1-5. ITS employees could not provide OIG with documentation tracing the history of this expansion.

The division's stagnant base budget, which had not changed significantly in more than 19 years, did not align with its expanded scope of responsibilities beyond the A Bureau.⁷ Therefore, ITS relied on non-recurring, competitively allocated funding sources such as the IT Central Investment Fund⁸ and reimbursements from its customers to fund its services. During the inspection, the A Bureau's acting Assistant Secretary did not approve ITS' request for an increase to its base budget for FY 2023 because of competing priorities for bureau resources. Dependence on non-recurring and uncertain funding sources created long-term and strategic IT planning challenges and increased the risk of funding shortages if Central Investment Funds were not awarded, reimbursement from customers was not forthcoming, or the cost of services provided was not correctly calculated. Although sharing the cloud platform was a cost-saving approach for the Department as a whole, OIG observed instances where ITS did not fully factor in the financial and staffing impacts associated with extending services outside its mandated roles and responsibilities. At the time of the inspection, OIG also observed potential ITS funding

⁶ Cloud computing is the delivery of computing services over the internet to offer faster innovation, flexible resources, and economies of scale.

⁷ In FY 2020, the ITS base budget was \$2,835,500, and the total projected costs for ITS operations were \$15,088,000.

⁸ The IT Central Investment Fund is a Department-wide central funding source for IT investments and is part of the IT capital investment planning process. Funding is managed through the Information Technology Program Board.

shortages of \$298,000 for FY 2021 because of uncertainty as to whether customers would reimburse ITS for services it provided.

ITS staff explained, and OIG confirmed, that the expanded mission scope, in part, created challenges for the division in implementing required information security procedures and governance processes. Rather, ITS focused on meeting the business requirements for its expanded customer base and lacked the staffing and funding resources to manage and govern the day-to-day security and operations functions for the systems in its own mandated portfolio of services, as outlined in 1 FAM 212.1-5. The details of those challenges are described below.

Recommendation 1: The Bureau of Administration should review the role defined for the Information Technology Services Division in the Foreign Affairs Manual and the services that the Information Technology Services Division is providing and bring them into alignment. (Action: A)

Information Systems Security Officers Did Not Perform All Required Duties

OIG found that A/EX did not fully implement the Department's ISSO program as required by 5 FAM 824, which seeks to ensure information security oversight to meet Department standards. ITS designated an ISSO and an alternate ISSO to oversee and monitor the security of its information systems, as directed in 12 Foreign Affairs Handbook (FAH)-10 H-352(1) and 12 FAH-10 H-352(2). However, the ISSOs did not perform the required security functions to ensure systems were configured, operated, maintained, and disposed of in accordance with all relevant security guidelines issued by IRM and the Bureau of Diplomatic Security, per 5 FAM 824(1). For example, the ISSOs did not consistently review and monitor the systems under their purview, including ITS networks and applications that supported the bureau and Department. As discussed in more detail below, ITS applications operated without security assessments; servers ran unsupported and unsecured operating systems; and Active Directory⁹ security groups did not follow the least privileged principles.¹⁰ These issues could be mitigated if ISSOs regularly monitored security controls as required by 12 FAH-10 H-312.5-3 and reviewed Active Directory accounts, as called for in 12 FAH-10 H-112.1-3. The ISSOs told OIG they did not perform all ISSO duties due to a lack of time and resources. Not performing these duties put the security of the Department's computer systems and information at risk of compromise.

Recommendation 2: The Bureau of Administration should require the Information Systems Security Officers to perform their duties in accordance with Department guidance. (Action: A)

⁹ The Department used Active Directory, a Microsoft technology, to manage users, computers, and other devices on its networks and assign permissions to access Department resources.

¹⁰ The principle of least privilege allows only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks. See NIST Special Publication 800-53A, Rev. 5, "AC-6 Least Privilege," at 36.

Information Technology Services Division Did Not Implement Standardized and Documented Systems Development Life Cycle Procedures

ITS did not implement standardized and documented systems development life cycle (SDLC) procedures to manage its systems, as required in 12 FAH-10 H-342.2-1. According to 5 FAM 693, SDLC is a framework for developing, maintaining, and replacing IT systems. This framework ensures systems operate in accordance with security policies. Until A/EX established the ITS Program Management Office in January 2020, ITS staff focused on meeting customers' business needs rather than on SDLC processes. As a result, systems did not undergo security reviews, as discussed above, and lacked background documentation to show life cycle plans. Furthermore, a key Department-wide system operated by ITS used unsupported and unsecured operating systems due to lack of replacement planning. Although the Program Management Office had started to institute SDLC frameworks, it had yet to fully document and implement key steps for integrating the Department's risk management process into SDLC activities, as described in 12 FAH-10 H-342.2-1(5). In the absence of standardized and documented SDLC procedures, ITS could not ensure its systems fully met security and maintenance requirements to protect the Department's information and manage the systems in a cost-effective manner.

Recommendation 3: The Bureau of Administration should implement standardized systems development life cycle procedures to manage the systems in the Information Technology Services Division in accordance with Department standards. (Action: A)

Systems Lacked Risk Assessments and Authorizations to Operate

ITS operated systems without conducting risk assessments and obtaining authorizations to operate (ATO)¹¹ from IRM, as required in 12 FAH-10 H-332.2-1b and 5 FAM 619c. Risk assessment involves conducting and documenting assessments of risk, including the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of information the systems process and store. To manage risk, the outcomes from the risk assessment are used to apply security controls proportional to the determined magnitude of harm. The ATO process validates that the required security controls are properly implemented for applications that are reportable under the Federal Information Security Modernization Act of 2014.¹²

OIG found that 11 of the division's 55 systems had expired ATOs and 41 had not undergone initial or subsequent risk assessments as systems were modified. These applications support the A Bureau, as well as the Department, in real property management, translation services,

¹¹ 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. NIST Special Publication 800-53A, Rev. 5, "Security and Privacy Controls for Federal Information Systems and Organizations," Appendix A, at 396.

¹² The Federal Information Security Modernization Act of 2014 provides enhanced access to Government information and services in a manner consistent with laws regarding protection of personal privacy and national security.

emergency notifications, and knowledge management platforms. A lack of funding, staffing, and procedures for planning systems life cycles led to the applications being released without risk assessments and authorizations or to continue to operate with expired ATOs. Developing and maintaining applications without conducting risk assessments and obtaining ATOs increases the risk of the Department's information being compromised or operations disrupted due to inadequate security controls. At the time of the inspection, ITS was in the process of developing procedures to ensure risk management steps were planned in systems life cycle to address these deficiencies.

Recommendation 4: The Bureau of Administration should conduct risk assessments for the applications in the Information Technology Services Division and obtain authorizations to operate from the Bureau of Information Resource Management. (Action: A)

Recommendation 5: The Bureau of Administration should implement procedures to conduct risk assessments and obtain authorizations for applications in the Information Technology Services Division prior to production releases and expiration of the systems' authorizations to operate. (Action: A)

Information Technology Operations Did Not Comply With System Inventory Tracking Standards

ITS operations did not comply with the Department's system inventory tracking standards, which require maintaining accurate systems inventory documentation. According to 5 FAM 864d and 5 FAM 639.1b, all systems need to be listed in the Department's IT portfolio management tool known as the Integrated Management, Analytics, and Technology Resource for Information Exchange (iMatrix),¹³ and updated on a regular basis. OIG reviewed iMatrix system inventory documentation and compared it to the system inventory lists generated by ITS staff and the Department's Risk Management Framework management tool Xacta.¹⁴ The three lists did not align. Additionally, ITS staff stated that a recent cybersecurity scorecard¹⁵ released by IRM did not incorporate all ITS systems in the assessment because IRM was unaware of some ITS systems. ITS staff told OIG that they did not have the time and resources to establish a process for reviewing and updating iMatrix or its internal system inventory documents when developing or updating systems. The failure to maintain accurate system inventory documents and configuration data can result in unprotected or improperly protected information systems.

Recommendation 6: The Bureau of Administration should implement a process for reviewing and updating iMatrix and internal system inventory documents to accurately

¹³ iMatrix is the Department's official system of record for information on all IT investments, programs, projects, and assets.

¹⁴ Xacta is the software suite chosen by the Department to automate the assessment and authorization process and implement the Risk Management Framework outlined by NIST SP 800-37 Rev. 2, "Risk Management Framework for Information Systems and Organizations" (December 20, 2018).

¹⁵ The cybersecurity scorecard is a monthly IRM report that provides a snapshot of bureau efforts in addressing the cybersecurity responsibilities and ranks the bureaus according to the score they receive.

reflect the status of the Information Technology Services Division's information systems.
(Action: A)

Division Ran Unsupported, Unapproved Operating System on the Department's Network

OIG found that ITS ran an operating system that was no longer approved for Department networks. The Department's IT Configuration Control Board¹⁶ change request CR1-20191470 states that installations of Windows Server 2008 R2¹⁷ and below must be upgraded or removed from production systems because the vendor would no longer support and update it. During the inspection, OIG found four ITS servers running Windows Server 2008 R2 on the Department's Sensitive But Unclassified network. ITS operations staff were aware of this issue. The division planned to replace the servers with an approved system, but ITS failed to plan far enough in advance to release the system before Windows Server 2008 R2 was removed from the Department's approved products list. During the inspection, ITS was attempting to release the new system and remove the unapproved servers from the Sensitive But Unclassified network, but configuration issues caused delays. Additionally, ITS staff was informed during the inspection that funding for the new system would not be renewed for FY 2022 and, as a result, ITS would need to continue running the unsupported operating system. Running unsupported and unsecured operating systems on production networks introduces cybersecurity vulnerabilities to the Department's networks and increases the potential risk that ITS information systems could be compromised.

Recommendation 7: The Bureau of Administration should review its existing operating systems and remove all unsupported operating systems from Department networks.
(Action: A)

Division Did Not Conduct Contingency Plan Testing for Information Technology Systems

ITS did not conduct IT contingency plan testing for its information systems. Guidance in 12 FAH-10 H-232.3-1a states that bureaus, in coordination with application or information system owners, must conduct annual contingency plan testing. OIG reviews found ITS systems with IT contingency plan test due dates that were more than 5 years old and that most ITS systems had never been tested. Personnel responsible for planning and conducting IT contingency plan tests told OIG that a lack of time and resources led to the lapse in testing. The failure to test IT contingency plan tests increases the risk of system and service disruption.

Recommendation 8: The Bureau of Administration should conduct information technology contingency plan tests for the information systems in the Information Technology Services Division in accordance with Department standards. (Action: A)

¹⁶ The IT Change Control Board manages standardization of the Department's global IT environment and addresses issues of configuration tracking, change control, and network planning and operations.

¹⁷ Windows Server 2008 R2 is a server operating system developed by Microsoft, which builds on the enhancements built into Windows Server 2008.

Office Lacked Records Management Policy and Procedures

A/EX did not manage its digital records in accordance with Department guidelines. According to Department cable 20 STATE 124322,¹⁸ offices must ensure they can locate, retrieve, access, and use the digitized versions for the records' entire retention period. Additional Department guidance¹⁹ states that offices should develop and maintain office-level policies and procedures that govern the use of shared computer drives. During the inspection, OIG found a lack of standardization among A/EX divisions regarding organizing shared drives and storing digital files. A/EX staff told OIG there were occasions when knowledge transfer activities between employees did not occur because digital files could not be located. Some divisions in A/EX were working on standardizing their knowledge management processes, but the office did not have an office-level policy or procedures that governed the use of shared drives and digital records. The failure to effectively manage office shared drives and digital records can result in the loss of institutional knowledge and adversely affect continuity of operations.

Recommendation 9: The Bureau of Administration should develop and implement a policy for organizing and managing electronic records in the Office of the Executive Director.
(Action: A)

Collaborative Strategy and Management

Created in 2013,²⁰ A/EX's Collaborative Strategy and Management (CSM) Division provides management analysis, policy guidance, and advisory services to the A Bureau's Assistant Secretary and Executive Director. The seven-person division also is responsible for a range of disparate activities in the A Bureau: OIG liaison;²¹ coordination of changes to 1 FAM and 6 FAM;²² oversight of Balanced Workforce and FAIR Act activities;²³ management of the emergency preparedness program;²⁴ development of the FBS and other planning documents; coordination of management control issues; and management of program evaluations and special studies to identify and resolve operational deficiencies and improve processes. OIG

¹⁸ Cable 20 STATE 124322, "Updated recordkeeping guidance for managing shared drives on OpenNet and ClassNet and for digitizing temporary paper records," December 28, 2020.

¹⁹ Bureau of Administration, Global Information Services, *Guide to Organizing and Managing Electronic Records on OpenNet and ClassNet* (December 2020).

²⁰ CSM was created following the 2013 merger of the Office of Commercial Services Management with A/EX.

²¹ Coordination of A Bureau responses to recommendations and hotline referrals from OIG.

²² Coordination of A Bureau's changes to volume 1 of the FAM (Authority, Responsibility, and Organization) and all changes to volume 6 of the FAM (General Services) as well as clearance of all FAM changes that are referred to A/EX.

²³ Balanced Workforce studies determine the appropriate mix of Federal employees and contractor skills, experience, and expertise necessary to achieve the Department's mission. The Federal Activities Inventory Reform (FAIR) Act of 1998, P.L. 105-270, along with Office of Management and Budget Circular A-76, requires agencies to prepare inventories of the commercial and inherently governmental activities performed by Federal employees.

²⁴ Includes updating and distributing the A Bureau's Emergency Action Plan, maintaining information on the bureau's emergency personnel, and assisting in the coordination of emergency drills affecting the bureau's several organizations.

determined, through interviews and document reviews, that CSM generally fulfilled its 1 FAM 212.1-1 mandate in these areas, except for program evaluation follow-up, as discussed below.

Bureau Did Not Track Implementation of Program Evaluation Recommendations

OIG found A/EX did not have a mechanism to track implementation of A Bureau program evaluations. According to 1 FAM 212.1-1c, CSM has primary responsibility for managing all bureau program evaluations. CSM met and sometimes exceeded the number of annual program evaluations per bureau required in 18 FAM 301.4-4b. In addition to the five program evaluations CSM completed²⁵ between FY 2018 and FY 2021, other A Bureau offices initiated at least six program evaluations during that same timeframe.²⁶ According to 18 FAM 301.4-4(F)b, bureaus are required to track progress on program evaluation recommendations through a document such as a recommendation tracker until they are implemented.

Although evaluations were vetted and discussed at A Bureau quarterly FBS meetings²⁷ and CSM was aware of the evaluations being done by other bureau offices, OIG determined through interviews and documentary reviews that neither CSM nor any other part of the bureau played a role in tracking the implementation of recommendations once the evaluations—both CSM-managed and non-CSM-managed—were completed. Furthermore, CSM staff told OIG they usually learned about an office’s reaction to one of their evaluations or about corrective action incidentally, such as in meetings or in informal discussions. Only occasionally did offices respond to evaluation findings in writing. For example, the bureau’s Privacy Office provided a written memo and an action plan after their CSM-led evaluation, and the Global Publishing Solutions Office requested a future CSM evaluation to build on an earlier one. However, CSM did not require this type of written feedback.

Division staff told OIG that due to its desire to maintain a bureau-wide collegial relationship on the full range of CSM responsibilities, as well as its small staff, CSM viewed its role as a consultant on bureau program evaluations. However, the lack of a tracking mechanism on implementation of A Bureau program evaluation recommendations—both those conducted by CSM and its partners and those conducted by other bureau offices—weakened the positive impact of the bureau’s otherwise robust evaluation process, including the identification of possible cost savings.

Recommendation 10: The Bureau of Administration should implement a procedure to track implementation of all bureau program evaluation recommendations. (Action: A)

²⁵ At the time of the inspection, CSM also had two evaluations in progress and planned an additional two evaluations for FY 2021.

²⁶ CSM partnered with subject matter experts from other bureau offices on some of its evaluations, while some other non-CSM-managed evaluations were conducted by contract evaluators.

²⁷ Guidance in 18 FAM 301.4-4a requires bureaus to examine the performance and outcomes of programs, projects, and processes through bureau evaluations.

Resource Management

A/EX provides human resources, financial management, and administrative and procurement support services to customers in the A Bureau and IRM. OIG reviewed internal controls in the Human Resources, Financial Management, and Procurement and Administrative Services Divisions and found they generally implemented required processes and procedures in accordance with applicable Department standards, with the exceptions noted below.

Human Resources Division Was Taking Steps to Address Staffing Shortages and Communication Issues

OIG found the Human Resources Division (HRD) generally provided effective support to its customers. However, HRD did not meet its staffing and recruitment customer service standard²⁸ of completing 90 percent of hiring actions within the Federal Government's 80-day target.²⁹ At the time of the inspection, the Human Resources Division had a 43 percent vacancy rate. OIG determined that the staffing shortages³⁰ affected the division's ability to fully meet its customer service standards directly leading to the bureau's overall vacancy rate of 35 percent. At the time of the inspection, in an effort to complement its staffing and recruitment team, the division issued a job announcement and planned to hire five additional full-time employees.

Additionally, staff told OIG that communication within HRD needed improvement. For example, the division did not have regular staff meetings, even virtual ones during the COVID pandemic, which hindered information sharing and coordination among division employees. In addition, CSM, in a FY 2020 organizational health assessment, identified poor internal communication among the five HRD teams as affecting division cohesion, an issue that OIG also identified during the inspection. HRD leadership recognized the need to improve communication among the five teams and reaffirmed its commitment to implement the communication elements of the strategic improvement plan that grew out of CSM's 2020 program evaluation.

Bureau Did Not Review \$8 Million in Unliquidated Obligations in a Timely Manner

OIG found that, as of May 2021, the A Bureau had \$8 million in unliquidated obligations with no activity in more than 1 year. OIG's review of data in the Department's Global Business Intelligence³¹ repository showed, for example, that 1,450 unliquidated obligations related to

²⁸ The Human Resources Division established a staffing and recruitment standard to measure its performance against Federal Government hiring standards.

²⁹ The 80-day hiring standard is a target hiring timeframe defined in the End-to-End Hiring Initiative. This initiative was launched in February 2008 as a partnership between the Office of Personnel Management and the Chief Human Capital Officers Council to improve the overall experience for applicants and hiring officials in the Federal hiring process. After a pilot phase, the Office of Personnel Management issued a government-wide standard in September 2008.

³⁰ The Human Resources Division was authorized 40 full-time positions, but only had 23 positions filled at the time of the inspection—a 43 percent vacancy rate.

³¹ The Global Business Intelligence, or Global BI, is the Bureau of the Comptroller and Global Financial Services' consolidated resource management reporting repository, which provides a single source of financial reporting for

official travel that took place from FY 2017 through FY 2019, valued at approximately \$2.7 million, had not been targeted for de-obligation. According to Department standards in 4 FAM 225d, unliquidated obligations with no activity in more than 1 year must be targeted and de-obligated if they cannot be documented as valid obligations. Financial management staff told OIG this situation occurred because some of the offices to which the funds were allotted were slow in responding to queries about the status of these unliquidated obligations. In addition, financial management officials told OIG that staffing shortages in the division hindered the division's ability to complete thorough monthly reviews of unliquidated obligations, in accordance with 4 FAM 225a. Failure to review and de-obligate unliquidated obligations in a timely manner, results in an accumulation of funds that could be put to better use.

Recommendation 11: The Bureau of Administration should review and de-obligate all invalid unliquidated obligations without activity for more than 1 year, in accordance with Department standards, so funds of up to \$8 million can be put to better use. (Action: A)

Contracting Officer's Representatives Did Not Administer Contracts in Accordance With Department Standards

OIG found that A/EX's three contracting officer's representatives (COR) did not administer assigned contracts in accordance with Department standards. The three CORs oversaw 19 contracts worth approximately \$133 million. OIG reviewed 7 of the 19 COR contract files³² (total value of approximately \$53 million) and found the files did not comply with Department standards in 14 FAH-2 H-517a. For example, two COR files did not include a copy of the contracting officer's letter of designation as required in 14 FAH-2 H-517a(1), and four files did not include technical and cost proposal documentation submitted by the contractor required by 14 FAH-2 H-517a(4).

In addition, CORs did not systematically document the contractors' annual performance in the Contractor Performance Assessment Reporting System,³³ as required by 14 FAH-2 H-572d³⁴ and 48 Code of Federal Regulations 42.1502a and the contracting officer's letter of designation. Despite these issues, OIG's discussions with the CORs and its review of other documentation in the files showed the CORs monitored the contracts, received the contracted services, and addressed contract issues when they arose. The CORs told OIG these issues occurred because they were unaware of some of the requirements and because their workload did not allow them to dedicate sufficient time to their COR duties. Failure to comply with COR requirements

the Department. Global BI includes a suite of reports and analytical tools that allows users to analyze large volumes of data sourced from the Department's various financial systems.

³² OIG reviewed the COR file for the highest value contract, worth \$36.1 million. OIG randomly selected the remaining six contracts, ensuring at least one file for each COR was reviewed.

³³ The Contractor Performance Assessment Reporting System, or CPARS, is the Government-wide evaluation reporting tool for all past performance reports on contracts and orders.

³⁴ The contracting officer is responsible for ensuring that the evaluation takes place, but the COR may be tasked with evaluating contractor performance. See 14 FAH-2 H-572e, "Final Evaluation."

increases the risk of contract mismanagement, misuse of Government resources, and substandard contractor performance.

Recommendation 12: The Bureau of Administration should bring its contract administration into compliance with Department standards. (Action: A)

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 Administration. The bureau's complete response can be found in Appendix B.¹ The bureau also provided technical comments that were incorporated into the report, as appropriate.

Recommendation 1: The Bureau of Administration should review the role defined for the Information Technology Services Division in the Foreign Affairs Manual and the services that the Information Technology Services Division is providing and bring them into alignment. (Action: A)

Management Response: In its December 8, 2021, response, the Bureau of Administration 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 Administration reviewed the role defined for the Information Technology Services Division in the Foreign Affairs Manual and the services that the division is providing and brought them into alignment.

Recommendation 2: The Bureau of Administration should require the Information Systems Security Officers to perform their duties in accordance with Department guidance. (Action: A)

Management Response: In its December 8, 2021, response, the Bureau of Administration 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 Administration required the Information Systems Security Officers to perform their duties in accordance with Department guidance.

Recommendation 3: The Bureau of Administration should implement standardized systems development life cycle procedures to manage the systems in the Information Technology Services Division in accordance with Department standards. (Action: A)

Management Response: In its December 8, 2021, response, the Bureau of Administration concurred with this recommendation.

¹ OIG faced delays in completing this work because of the COVID-19 pandemic and resulting operational challenges. These challenges included the inability to conduct most in-person meetings, limitations on our presence at the workplace, difficulty accessing certain information, prohibitions on travel, and related difficulties within the agencies we oversee, which also affected their ability to respond to our requests.

OIG Reply: OIG considers the recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation that the Bureau of Administration implemented standardized systems development life cycle procedures to manage the systems in the Information Technology Services Division in accordance with Department standards.

Recommendation 4: The Bureau of Administration should conduct risk assessments for the applications in the Information Technology Services Division and obtain authorizations to operate from the Bureau of Information Resource Management. (Action: A)

Management Response: In its December 8, 2021, response, the Bureau of Administration 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 Administration conducted risk assessments for the applications in the Information Technology Services Division and obtained authorizations to operate from the Bureau of Information Resource Management.

Recommendation 5: The Bureau of Administration should implement procedures to conduct risk assessments and obtain authorizations for applications in the Information Technology Services Division prior to production releases and expiration of the systems' authorizations to operate. (Action: A)

Management Response: In its December 8, 2021, response, the Bureau of Administration 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 Administration implemented procedures to conduct risk assessments and obtain authorizations for applications in the Information Technology Services Division prior to production releases and expiration of the systems' authorizations to operate.

Recommendation 6: The Bureau of Administration should implement a process for reviewing and updating iMatrix and internal system inventory documents to accurately reflect the status of the Information Technology Services Division's information systems. (Action: A)

Management Response: In its December 8, 2021, response, the Bureau of Administration 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 Administration implemented a process for reviewing and updating iMatrix and internal system inventory documents to accurately reflect the status of the Information Technology Services Division's information systems.

Recommendation 7: The Bureau of Administration should review its existing operating systems and remove all unsupported operating systems from Department networks. (Action: A)

Management Response: In its December 8, 2021, response, the Bureau of Administration 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 Administration reviewed its existing operating systems and removed all unsupported operating systems from Department networks.

Recommendation 8: The Bureau of Administration should conduct information technology contingency plan tests for the information systems in the Information Technology Services Division in accordance with Department standards. (Action: A)

Management Response: In its December 8, 2021, response, the Bureau of Administration 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 Administration conducted information technology contingency plan tests for the information systems in the Information Technology Services Division in accordance with Department standards.

Recommendation 9: The Bureau of Administration should develop and implement a policy for organizing and managing electronic records in the Office of the Executive Director. (Action: A)

Management Response: In its December 8, 2021, response, the Bureau of Administration 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 Administration developed and implemented a policy for organizing and managing electronic records in the Office of the Executive Director.

Recommendation 10: The Bureau of Administration should implement a procedure to track implementation of all bureau program evaluation recommendations. (Action: A)

Management Response: In its December 8, 2021, response, the Bureau of Administration 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 Administration implemented a procedure to track implementation of all bureau program evaluation recommendations.

Recommendation 11: The Bureau of Administration should review and de-obligate all invalid unliquidated obligations without activity for more than 1 year, in accordance with Department standards, so funds of up to \$8 million can be put to better use. (Action: A)

Management Response: In its December 8, 2021, response, the Bureau of Administration 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 Administration reviewed and de-obligated all invalid unliquidated obligations without activity for more than 1 year, in accordance with Department standards, so funds of up to \$8 million can be put to better use.

Recommendation 12: The Bureau of Administration should bring its contract administration into compliance with Department standards. (Action: A)

Management Response: In its December 8, 2021, response, the Bureau of Administration 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 Administration brought its contract administration into compliance with Department standards.

PRINCIPAL OFFICIALS

| Title | Name | Arrival Date |
|-----------------------------------|-----------------|---------------------|
| Executive Director | Elissa Pitterle | 7/2020 |
| Deputy Executive Directors | | |
| | Michael Capozzi | 4/2019* |
| | John L. Nave | 12/2019 |

*Michael Capozzi joined the Office of the Executive Director (A/EX) in 2002 in another position.

Source: Generated by OIG from information provided by A/EX.

APPENDIX A: OBJECTIVES, SCOPE, AND METHODOLOGY

This inspection was conducted from March 15, 2021, to August 31, 2021, in accordance with the Quality Standards for Inspection and Evaluation, as issued in 2012 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. Inspections cover three broad areas, consistent with Section 209 of the Foreign Service Act of 1980:

- **Policy Implementation:** whether policy goals and objectives are being effectively achieved and U.S. interests are accurately and effectively represented; and whether all elements of an office or mission are being adequately coordinated.
- **Resource Management:** whether resources are being used and managed with maximum efficiency, effectiveness, and economy; and whether financial transactions and accounts are properly conducted, maintained, and reported.
- **Management Controls:** whether the administration of activities and operations meets the requirements of applicable laws and regulations; whether internal management controls have been instituted to ensure quality of performance and reduce the likelihood of mismanagement; and whether instances of fraud, waste, or abuse exist and whether adequate steps for detection, correction, and prevention have been taken.

OIG's objectives for this inspection were to assess whether the Bureau of Administration, Office of the Executive Director (A/EX):

- Followed applicable information technology security and systems development standards for its information management systems.
- Tracked recommendations made in program evaluations according to applicable standards.
- Managed contracting, financial, and human resources functions efficiently and in compliance with applicable standards.

Methodology

OIG used a risk-based approach to prepare for this inspection. Due to the COVID-19 pandemic and taking into consideration relevant guidance, OIG conducted the inspection remotely and relied on audio- and video-conferencing tools in lieu of 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,

along with physical, documentary, testimonial, and analytical evidence collected or generated, to develop its findings, conclusions, and actionable recommendations.

This inspection did not include in its scope the operations of the A/EX Division of the Working Capital Fund. Studies of those operations fall under the purview of the OIG Office of Audits.

APPENDIX B: MANAGEMENT RESPONSE




United States Department of State

Washington, D.C. 20520

12/8/2021

UNCLASSIFIED

TO: OIG – Sandra Lewis, Assistant Inspector General for Inspections

FROM: A-IRM/EX – Elissa G. Pitterle, Executive Director 

SUBJECT: Response to Draft OIG Report – Inspection of the Bureau of
Administration, Office of the Executive Director

A-IRM/EX appreciates the opportunity to comment on the draft A-IRM/EX Inspection report. While we concur with the recommendations in principle, we do not agree with the summary statement on page 1 that indicates a “lack of internal controls” was responsible for the A-IRM/EX Information Technology Services (ITS) Division expanding its roles and responsibilities beyond those outlined in the Foreign Affairs Manual (FAM). While the expansion of ITS services beyond the A Bureau took place prior to the arrival of the current A-IRM/EX management team, it was done with the approval and full support of senior Bureau of Administration (A) and Bureau of Information Resource Management (IRM) leadership. The funding used to develop and expand ServiceNow technology to customers external to the A Bureau was provided through the Department’s IT Central Investment Fund and was reviewed and approved by A, IRM, BP and OMB. Further, this approach was directly related to a Department led initiative to save costs through shared IT services and support. Consequently, a lack of internal controls was not a factor in the expansion of ITS services. We respectfully request that OIG eliminate the phrase “lack of internal controls” as the cause for this condition.

Footnote number two on page 2 should not reference the Financial Management Division. Please eliminate.

UNCLASSIFIED

UNCLASSIFIED

-2-

Footnote number 20 on page 9 should eliminate “Office of Procurement Executive” on line one and the entire 2nd sentence.

We offer the following comments in response to the specific recommendations provided by OIG:

OIG Recommendation 1: The Bureau of Administration should review the role defined for the Information Technology Services Division in the Foreign Affairs Manual and the services that the Information Technology Services Division is providing and bring them into alignment. (Action: A)

Management Response: A-IRM/EX concurs with the recommendation.

OIG Recommendation 2: The Bureau of Administration should require the Information Systems Security Officers to perform their duties in accordance with Department guidance. (Action: A)

Management Response: A-IRM/EX concurs with the recommendation. A-IRM/EX is in the process of filling three GS-14 team leads in the ITS Division that will allow the ISSO to concentrate full-time on information security duties. Additionally, one contract security specialist has recently joined the ITS division.

OIG Recommendation 3: The Bureau of Administration should implement standardized systems development life cycle procedures to manage the systems in the Information Technology Services division in accordance with Department standards. (Action: A)

Management Response: A-IRM/EX concurs with the recommendation. Full implementation of this recommendation will be dependent on receiving additional resources.

OIG Recommendation 4: The Bureau of Administration should conduct risk assessments for the applications in the Information Technology Services division and obtain authorizations to operate from the Bureau of Information Resource Management. (Action: A)

UNCLASSIFIED

UNCLASSIFIED

-3-

Management Response: A-IRM/EX concurs with the recommendation. Full implementation of this recommendation will be dependent on receiving additional resources.

OIG Recommendation 5: The Bureau of Administration should implement procedures to conduct risk assessments and obtain authorizations for applications in the Information Technology Services division prior to production releases and expiration of the systems authorization to operate. (Action: A).

Management Response: A-IRM/EX concurs with the recommendation. The ITS division is developing procedures to comply with the recommendation but requires additional resources, such as a properly staffed development, change management and testing environment for full implementation.

OIG Recommendation 6: The Bureau of Administration should implement a process for reviewing and updating iMatrix and internal system inventory documents to accurately reflect the status of the Information Technology Services Division's information systems. (Action: A)

Management Response: A-IRM/EX concurs with the recommendation and has begun working more closely with the two other A Bureau IT offices located within Global Information Services (A/GIS) and Logistics Management (A/LM) to ensure iMatrix is properly updated for the entire A Bureau.

OIG Recommendation 7: The Bureau of Administration should review its existing operating systems and remove all unsupported systems from Department networks. (Action: A)

Management Response: A-IRM/EX concurs with the recommendation. The 2008 servers have been removed from the network and 2012 servers are in the process of being migrated to the 2018 platform. Full implementation of this recommendation will require modernizing legacy systems, which is dependent on receiving additional funding.

UNCLASSIFIED

UNCLASSIFIED

-4-

OIG Recommendation 8: The Bureau of Administration should conduct information technology contingency plan tests for the information systems in the Information Technology Services division in accordance with Department standards. (Action: A)

Management Response: A-IRM/EX concurs with the recommendation. Full implementation of this recommendation will be dependent on receiving additional resources as the ITS division is not properly staffed to design and perform these tests.

OIG Recommendation 9: The Bureau of Administration should develop and implement a policy for organizing and managing electronic records in the Office of the Executive Director. (Action: A)

Management Response: A-IRM/EX concurs with the recommendation and will work to develop a cost-effective solution.

OIG Recommendation 10: The Bureau of Administration should implement a procedure to track implementation of all bureau program evaluation recommendations. (Action: A).

Management Response: A-IRM/EX agrees with the recommendation and will develop a tracking system to monitor the implementation of recommendations.

OIG Recommendation 11: The Bureau of Administration should review and deobligate all invalid unliquidated obligations without activity for more than 1 year, in accordance with Department standards, so funds of up to \$8 million can be put to better use. (Action: A)

Management Response: A-IRM/EX concurs with the recommendation and has begun to reduce unliquidated obligations (ULOs) over twelve months old.

OIG Recommendation 12: The Bureau of Administration should bring its contract administration into compliance with Department standards. (Action: A)

UNCLASSIFIED

UNCLASSIFIED

-5-

Management Response: A-IRM/EX concurs with the recommendation and is taking steps to ensure contract administration is in compliance with the Office of Procurement Executive's 10/1/2020 PIB NO 2020-04 which outlines responsibilities and requirements for all contracting personnel.

UNCLASSIFIED

ABBREVIATIONS

| | |
|----------|--|
| A Bureau | Bureau of Administration |
| A/EX | Office of the Executive Director |
| ATO | Authorization to Operate |
| COR | Contracting Officer's Representative |
| CSM | Collaborative Strategy and Management Division |
| FAH | Foreign Affairs Handbook |
| FAM | Foreign Affairs Manual |
| FBS | Functional Bureau Strategy |
| HRD | Human Resources Division |
| IRM | Bureau of Information Resource Management |
| ISSO | Information Systems Security Officer |
| ITS | Information Technology Services Division |
| SDLC | Systems Development Life Cycle |

OIG INSPECTION TEAM MEMBERS

Peter Prahar, Team Leader
Iris Rosenfeld, Team Manager
Wilma Bodden-Raffucci
Brett Fegley
Martha Fikru
Leo Hession
Sergio Lagares
Matthew Lunn
Jessica McTigue

Other Contributors

Dolores Adams
Leslie Gerson
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