



Office of Inspector General
United States Department of State

Inspector General Statement on
the U.S. Agency for Global Media's

Major Management and Performance Challenges

FISCAL YEAR 2024



Contents

Introduction	1
Information Security and Management	2
Contract and Grant Management.....	3
Appendix A: Response From U.S. Agency For Global Media	4

Introduction

Each year, in accordance with the Reports Consolidation Act of 2000,¹ the Office of Inspector General (OIG) for the U.S. Agency for Global Media (USAGM) identifies the most significant management and performance challenges facing the agency and briefly assesses progress in addressing those challenges. The resulting report is included in the agency's annual performance and accountability report.

OIG identified the following two management challenges in FY 2024:

- Information Security and Management
- Contract and Grant Management

These were also identified as major management challenge in our FY 2023 report. Continued attention to these concerns will improve USAGM's operations and, accordingly, its ability to fulfill its underlying mission. This document includes examples of OIG reports and findings completed in FY 2024 that illustrate these challenge areas.

¹ The Reports Consolidation Act of 2000, § 3, Pub. L. 106-531 (amending 31 U.S.C. § 3516).

Information Security and Management



As a result of the annual audit of USAGM’s information security program,² OIG reported that USAGM continued efforts to implement an organization-wide program. However, additional steps are needed to fully implement an effective program. This conclusion was based on evidence of deficiencies identified in seven of nine domains—supply chain risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, and contingency planning. The information security standards that form the criteria of this audit represent foundational guidelines for managing and reducing cyber risk by protecting networks and data. USAGM’s persistent inability to comply with those standards will continue to be a focus of our work.

² OIG, *Audit of the U.S. Agency for Global Media FY 2024 Information Security Program* (AUD-IT-IB-24-25, July 2024).



Contract and Grant Management

An independent external auditor, working on OIG's behalf, has identified deficiencies with USAGM's grant monitoring efforts annually since the audit of USAGM's FY 2013 financial statements. USAGM has four grantees that it funds through annual grant agreements: Radio Free Europe/Radio Liberty (RFE/RL), Radio Free Asia, the Middle East Broadcasting Networks, and the Open Technology Fund. The auditor noted that USAGM made progress in strengthening its grants monitoring program. However, the program had not been fully implemented during FY 2023. Because USAGM continued to lack effective grantee oversight related to grant closeout requirements and financial audit requirements, there was an increased risk of waste, fraud, and abuse of federal funds.³

³ OIG, *Management Letter Related to the Audit of the U.S. Agency for Global Media FY 2023 Financial Statements* (AUD-FM-IB-24-22, February 2024).

Appendix A: Response From U.S. Agency For Global Media



U.S. AGENCY FOR
GLOBAL MEDIA

330 Independence Avenue SW | Washington, DC 20237 | usagm.gov

November 6, 2024

The Honorable Cardell K. Richardson, Sr.
Inspector General
Office of Inspector General
U.S. Department of State

Dear Mr. Richardson:

Thank you for the opportunity to respond to the Office of Inspector General's (OIG) *Statement on the U.S. Agency for Global Media's (USAGM) Major Management and Performance Challenges* for Fiscal Year (FY) 2024. I appreciate the OIG identifying challenges to agency operations, including those related to information security and management, and contract and grant management. I am pleased to highlight USAGM's progress on these issues, as well as plans for further improvement.

Information Security and Management

In FY24, USAGM has been hard at work to improve its cybersecurity program and investments, which have helped significantly mature the agency's IT security posture. Some key focus areas where the agency has made significant progress are the following: USAGM's continuous monitoring program, configuration management and vulnerability management, maturing and automating its identity governance and Identity-as-a-Service workflows, improving device protection for remote workers, and full implementation of Role-Based Access Control, which has helped improve secure access to cloud-based IT services and implement data loss protection to protect sensitive information and the integrity of USAGM content.

Notable accomplishments include:

- Significant progress in the agency's Information Security Continuous Monitoring program. The agency improved its management oversight processes and realigned some of the Federal Information Security Modernization Act systems boundaries, which have helped achieve greater visibility, accountability, oversight, and clear reporting structures, increasing its protection against cyber threats.
- USAGM has also made significant progress in our Supply Chain Risk Management (SCRM) program by compiling all the vendor software attestations for the agency. USAGM now fully complies with the Office of Management and Budget's (OMB)



SCRM Memorandum M-22-18.

- USAGM made significant improvements with the implementation of a new cloud-based IT service management “Ivanti Change Management” module for better management of its IT Change Advisory Board activities. This has significantly improved the documenting, monitoring, testing, approving and communication of IT changes across the enterprise.
- USAGM has continued to make progress with the implementation of its software and hardware assets management program with Ivanti Assets Management modules.
- USAGM has continued to make progress with implementing its software baseline on workstations and mobile devices to allow and disallow certain software applications to better protect the agency from ever-changing risks.
- USAGM has made progress in its efforts to implement Zero Trust Architecture, the cybersecurity mandated by Executive Order 14028, by creating a clear strategic roadmap and work plan for activities needed to implement the Zero Trust with architecture within the IT enterprise.
- USAGM has made significant progress enforcing multi-factor authentication, data encryption, and personal identity verification (PIV) card authentication. USAGM is now 92% PIV login compliant for all agency devices and users accessing the agency’s network.

Contract and Grant Management

USAGM is continuing to implement a robust grants management program and continues to implement key grants monitoring activities. During FY24, USAGM’s Grant Monitoring Program consisted of working to formally adopt OMB’s revised regulations at 2 CFR Part 200 and updating policies and workflow processes in response to OMB Memorandum 24-11 *Reducing Burden in the Administration of Federal Financial Assistance*; desk and on-site reviews; reviving the use of the Treasury Collateral Management and Monitoring system of securing collateral for advanced cash; annual grants management training provided to the recipients; technical assistance to the recipients as needed; annual risk assessments for all five grant recipients; and the closing out of completed grants.

Again, thank you for the opportunity to respond to OIG’s statement on USAGM’s FY24 management and performance challenges. I look forward to a positive and productive relationship with the OIG.

Sincerely,



Amanda Bennett
Chief Executive Officer



HELP FIGHT FRAUD, WASTE, AND ABUSE

1-800-409-9926

[Stateoig.gov/HOTLINE](https://stateoig.gov/HOTLINE)

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

WPEAOmbuds@stateoig.gov