U.S. International Trade Commission
OFFICE OF INSPECTOR GENERAL

Management Letter – Inadequate Oversight of the Interagency Agreement for Building and Security Services

OIG-ML-26-05

June 29, 2026

THE INSPECTOR GENERAL

UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

June 29, 2026

IG-YY-006
OIG-ML-26-05

Chairman Johanson:

The OIG is currently conducting an audit to examine whether the U.S. International Trade Commission (USITC or Commission) has badge access controls in place to protect facilities, provide access to authorized individuals, and perform timely monitoring and updates. During the audit, we identified conditions that warrant prompt management action. The purpose of this management letter is to bring immediate attention to significant internal control weaknesses in the Commission's oversight of an Interagency Agreement (IA) with the Federal Protective Service[1] (FPS) for basic building and security services. This management letter was not performed in accordance with generally accepted government auditing standards and does not present any conclusions or recommendations.

The mission of the USITC Office of Security Services (OSS) includes implementing, coordinating, and executing programs at the USITC that support physical security, safety, and asset protection. OSS is responsible for overseeing the USITC's physical security and accomplishes this through USITC staff and an IA with FPS. The OIG found that the OSS staff and managers were unable to verify or provide general information about basic building and security services performed through the IA with FPS. The USITC Physical Security Officer assigned to monitor the IA could not accurately describe FPS activities or confirm that services

[1] The Federal Protective Service (FPS) within the Department of Homeland Security (DHS) is responsible for protecting more than 9,000 federal buildings and ensuring the safety of the people within them—federal employees, contractors, and visitors, including members of the public. From https://www.gao.gov/assets/gao-21-311r.pdf

were delivered in accordance with applicable agreements and security requirements at the USITC building. The IA between the FPS and the Commission and the associated General Terms and Conditions document do not contain specific details on the level and type of security services provided.

Monitoring Gaps

The USITC has not documented any procedures for monitoring the FPS activities or provided any analysis of the documents reviewed, despite the approximately $2.4 million IA for basic building and security services in Fiscal Year 2025. OSS personnel initially told the OIG that the underlying contract[2] between FPS and the security firm assigned to the USITC building, as well as the Post Orders, prohibited certain monitoring activities, such as reviewing logs. However, the OIG discovered that the Commission had never reviewed or possessed the contract.

We met with FPS leadership, who told us that the USITC does not receive any reports from FPS regarding access control at the building. They explained that all information is noted in the Post Orders. The FPS confirmed that there is no Memorandum of Understanding or Agreement related to USITC and FPS roles and responsibilities, and no such language exists in the IA. FPS said the contract security officers created an internal ITC log to manage tracking of individuals who did not have a working badge for USITC space for accountability, and that the USITC did not have a system in place.

The USITC Physical Security Officer stated that monitoring of the IA for basic building and security services was conducted. As evidence of this, the Physical Security Officer and the FPS gave us logs in June, despite OSS stating it did not have access to logs used by the guards at USITC. OSS demonstrated that visitor and employee sign-in sheets existed, but the OIG could not determine what level of monitoring had occurred.

Credibility Issues with OSS Staff

During the OIG's audit, the explanations provided by OSS staff were inconsistent with the available evidence, to the point of raising serious credibility issues. The audit team found that explanations provided by OSS regarding the identified deficiencies and oversight activities

[2] FPS contracts with a private security company to provide Protective Security Officer services at various locations throughout Washington, DC, including at the USITC leased building.

conducted were not supported by contemporaneous documentation, could not be independently verified, and, in several instances, were inconsistent with other evidence obtained during the audit. For example, the OSS stated that it reviewed Post Orders at the guard desk as part of its monitoring. When we asked to see what had been reviewed, OSS shared an FPS email with the OIG stating that the documents are restricted and may not be shared outside authorized personnel.

The OIG arranged with FPS to view the Post Orders at the guard desk. When the OIG went to the desk, the officers and the on-site supervising officer could not find the Post Orders and stated they had been told the document had been removed for "updating." The OIG then contacted FPS leadership directly and learned that the Post Orders were to be maintained at the USITC and should still be there. Although FPS made another effort to locate the Post Orders at USITC, they subsequently informed the OIG that the Post Orders had been removed and shredded, which was not known by the Commission.

Passive Oversight

An administrative approach to oversight may be sufficient for lower-risk functions where compliance with contractual requirements can be demonstrated through reports, invoices, and routine performance metrics. Security operations, however, present fundamentally different risks. The Commission relies on the OSS and the IA with FPS to provide physical security services at the leased building where the USITC staff conduct mission-related activities and operations. Effective oversight of the agreement with FPS requires Commission personnel to understand the IA, monitor performance, verify that services are delivered as expected, maintain supporting documentation, take responsibility for the outcomes, and ensure that security expenditures are supported by evidence of performance. After interviewing OSS staff, reviewing email correspondence, and reviewing available USITC and FPS documents, the OIG could not determine whether OSS had:

- demonstrated the knowledge, experience, and ability to oversee the IA effectively;
- reviewed reports or other evidence demonstrating FPS's fulfillment of IA responsibilities;
- established basic protocols or procedures to assess whether the services provided by the IA with FPS meet the USITC's needs and applicable federal requirements; and
- received all services described in the General Terms and Conditions document.

Summary

Given the potentially serious impact on the Commission's physical security posture and the need for efficient and effective stewardship of federal resources, the OIG believes management's prompt attention to this matter is warranted to address a culture of minimal engagement. In the current threat environment characterized by persistent and evolving risks to federal operations, facilities, information, and personnel, robust oversight is critical in preserving USITC's ability to prevent, detect, and respond to security incidents. We are providing this alert to facilitate the review of current OSS personnel performance and practices, identification of any gaps in IA oversight, establishment of a monitoring regimen, and implementation of improvements while our audit work continues.

If a serious security incident at the USITC-leased building were to occur, the resulting scrutiny would appropriately extend beyond the IA and contractor performance to the adequacy of the Commission's oversight. The OIG's concerns extend beyond the documentation of monitoring activities to the performance of OSS personnel and managers. The deficiencies observed by the OIG during our ongoing audit raise questions about whether the Commission has personnel with the expertise, analytical skills, and commitment necessary to oversee the IA for basic building and security services that is vital to protecting USITC personnel and visitors, facilities, operations, and assets.

Sincerely,

Rashmi Bartlett
Inspector General

CC: Erin Joffre, Chief of Staff
David Fishberg, Deputy Chief of Staff and Audit Liaison
Kate Higginbothom, Chief Administrative Officer

U.S. International Trade Commission
Office of Inspector General
500 E Street, SW Washington, DC 20436

REPORT WASTE, FRAUD, ABUSE, OR MISMANAGEMENT

Hotline: 202-205-6542
OIGHotline@usitcoig.gov
https://usitcoig.oversight.gov/report-fraud-waste-or-abuse