Management Alert: EXIM Did Not Appropriately Safeguard Personally Identifiable Information

OIG-O-25-02
January 2025

Office of Inspector General
Export-Import Bank of the United States

MANAGEMENT ALERT

To: Howard Spira, Senior Vice President, Chief Information Officer, and Senior Agency Official for Privacy

Darren Death, Chief Information Security Officer/Chief Privacy Officer

From: Ami Schaefer, Deputy Assistant Inspector General for Special Reviews AMI SCHAEFER Digitally signed by AMI SCHAEFER Date: 2025.01.02 13:39:01 -05'00'

Subject: Management Alert: EXIM Did Not Appropriately Safeguard Personally Identifiable Information (OIG-O-25-02)

Date: January 2, 2025

During the course of an oversight project, the Office of Inspector General (OIG) for the Export-Import Bank of the United States (EXIM) found that EXIM did not appropriately limit access to copies of protected or restricted documents maintained on a shared network drive.[1] OIG is informing EXIM of this incident—and potential breach[2]—because it risks unauthorized disclosure or unauthorized access to sensitive information, including information EXIM is obligated to protect under the Privacy Act of 1974 (Privacy Act).[3]

OIG believes that the evidence obtained provides a reasonable basis for the findings and recommendations outlined below. OIG conducted this work in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Federal Offices of Inspector General*.[4] OIG issued four recommendations to improve EXIM's compliance with applicable information security requirements. In its comments on the draft report, EXIM concurred with all four recommendations. OIG considers the four recommendations resolved. EXIM's formal response to this management alert is reprinted in its entirety in Appendix A. In advance of publishing this report, OIG made the agency aware of the findings so that they could take appropriate action. At the time of publication, the Office of Information

[1] OIG did not complete a comprehensive review of all records stored on the shared network drive; OIG's findings are based upon a high-level review of document file names. OIG's review of these documents confirmed that they contained information that should be protected and/or restricted in their distribution.

[2] The Office of Management and Budget defines a "breach" as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an 'other than authorized purpose.' See Office of Management and Budget, *Preparing for and Responding to a Breach of Personally Identifiable Information* (M-17-12; January 3, 2017).

[3] 5 U.S.C. § 552a.

[4] Council of the Inspectors General on Integrity and Efficiency, *Quality Standards for Federal Offices of Inspector General* (August 2012).

Management and Technology had initiated actions to protect the documents, report the incident, and notify EXIM staff of their responsibilities to safeguard confidential information.

EXIM Did Not Safeguard Files Containing Protected or Restricted Information

OIG found that EXIM did not appropriately safeguard multiple files that contained protected or restricted information stored on an EXIM shared network drive that was made available to all EXIM information technology (IT) systems users. Specifically, OIG identified the following types of protected or restricted documents that EXIM made available to all users: reimbursement forms (some of which included social security numbers and home addresses); employee performance evaluations and ratings; employee performance improvement plans and performance reprimands; a job applicant assessment and rating; Standard Form (SF)-50s and SF-52s, which outline various, agency personnel actions; outside employment request forms; an employee timesheet; and other documents that could contain personally identifiable information (PII).[5] For example, OIG identified two examples in which documentation included the name, address, and social security number for the individual(s) involved, information that is expressly governed by the Privacy Act. In addition, OIG found documents that reference ongoing litigation or potentially law enforcement sensitive[6] information.

EXIM maintains a shared network drive on its IT network that all EXIM users can access, unless additional permission restrictions have been programmed. OIG recognizes that EXIM operations may benefit from using a shared network drive to allow users to work collaboratively. However, having a shared network drive adds risk that users may inappropriately or inadvertently save or store protected or restricted-access PII and/or other restricted documentation to those folders—thus, taking protected documents out of their authorized storage structure. EXIM's IT Rules of Behavior[7] state that authorized users must take approved measures to protect PII, business sensitive information, or controlled unclassified information[8] from disclosure and report breaches to the IT Help Desk immediately. Some of the documentation OIG identified date from 2017 and 2018, indicating that EXIM did not conduct regular monitoring of the shared network drive for improper records or that such monitoring efforts were ineffective.

---

[5] Personally identifiable information is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual, such as a name, address, and social security number.

[6] Law enforcement sensitive information refers to unclassified information originated by agencies with law enforcement missions that may be used in criminal prosecution and requires protection against unauthorized disclosure to protect sources and methods, investigative activity, evidence, or the integrity of pretrial investigative reports.

[7] Export-Import Bank of the United States, *Rules of Behavior for User of EXIM Bank's Information Systems*; updated June 2024.

[8] Controlled unclassified information is sensitive information that does not meet the criteria for classification but must still be protected. It is Government-created or owned unclassified information that allows for, or requires, safeguarding and dissemination controls in accordance with laws, regulations, or Government-wide policies.

EXIM Required to Safeguard Privacy Act Information, Report Breaches

The Privacy Act prohibits the disclosure of covered records to unauthorized persons. Many of the records identified in OIG's review are governed by system of records notices,[9] which limit the authorized releases of covered documents and identify the safeguards to be applied to those records. This includes maintaining paper records in locked files and electronic records in password protected systems which may only be accessed by individuals whose official duties require access. Furthermore, the Office of Management and Budget identifies an agency's Senior Agency Official for Privacy as the primary official for preparing for and responding to a breach.[10] Once the Senior Agency Official for Privacy has been notified of a breach, they must determine whether there is a requirement to report the breach, and develop and implement a breach response plan.[11] Finally, as outlined in EXIM's *Security Incident Handling Policy,*[12] EXIM's Chief Information Officer and the Chief Information Security Officer must develop a report regarding the circumstances that led to the incident and the lessons learned that will prevent future incidents and/or improve agency response.

Recommendations

OIG is making the agency aware of this incident and is issuing four recommendations to address the incident and mitigate the risk of Privacy Act-covered documentation being accessible to those without a need to know. OIG's FY 2025 Oversight Work Plan[13] includes an audit of EXIM's implementation of the Privacy Act; OIG reserves the right to alter the timing of this planned audit and/or modify the audit objectives based on the actions taken by EXIM in response to the below recommendations.

> **Recommendation 1:** The Office of Information Management and Technology should immediately restrict access to documents containing Privacy Act information, or any other protected or restricted documentation stored on EXIM's Information Technology (IT) systems, ensuring that only individuals with a need to know have access.
>
> **Management Response:** In its December 26, 2024, response, EXIM concurred with this recommendation.

---

[9] The Privacy Act requires that each agency that maintains a system of records must publish a notice in the Federal Register that identifies the purpose for which information about an individual is collected, from whom and what type of information is collected, how the information is shared with individuals and organizations outside/external to the agency (routine uses), and what an individual must do if they want to access and/or correct any records the agency maintains about them. These notices are commonly referred to as "systems of records notices" or "SORNs."

[10] Office of Management and Budget, *Preparing for and Responding to a Breach of Personally Identifiable Information* (M-17-12, January 3, 2017).

[11] *Ibid.*

[12] Export-Import Bank of the United States, *Security Incident Handling Policy*; updated May 2025.

[13] OIG, *FY 2025 Oversight Work Plan* (OIG-O-24-13, September 30, 2024).

OIG Reply: OIG considers this recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation that the Office of Management and Technology immediately restricted access documents containing Privacy Act information, or any other protected or restricted documentation stored on EXIM's Information Technology (IT) systems, ensuring that only individuals with a need to know have access.

Recommendation 2: The Senior Agency Official for Privacy, in coordination with the Office of General Counsel, should assess within the Office of Management and Budget guidance whether there is a requirement to report the incident, and potential breach, and determine if any of the files were inappropriately accessed by individuals without a need to know.

Management Response: In its December 26, 2024, response, EXIM concurred with this recommendation.

OIG Reply: OIG considers this recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation that the Senior Agency Official for Privacy, in coordination with the Office of General Counsel, assessed within the Office of Management and Budget guidance whether there was a requirement to report the incident, and potential breach, and determined if any of the files were inappropriately accessed by individuals without a need to know.

Recommendation 3: The Chief Information Officer and the Chief Information Security Officer should develop a report regarding the circumstances that led to the incident and the lessons learned that will prevent future incidents and/or improve agency response, as required by EXIM's *Security Incident Handling Policy*.

Management Response: In its December 26, 2024, response, EXIM concurred with this recommendation.

OIG Reply: OIG considers this recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation that the Chief Information Officer and the Chief Information Security Officer developed a report regarding the circumstances that led to the incident and the lessons learned that will prevent future incidents and/or improve agency response, as required by EXIM's *Security Incident Handling Policy*.

Recommendation 4: The Office of Information Management and Technology should implement any changes or lessons learned identified in the incident report, to include policy changes or updated training that address the production, maintenance, and disposal of non-record copies of official documents.

Management Response: In its December 26, 2024, response, EXIM concurred with this recommendation.

OIG Reply: OIG considers this recommendation resolved. The recommendation can be closed when OIG receives and accepts documentation that the Office of Information

Management and Technology implemented any changes or lessons learned identified in the incident report, to include policy changes or updated training that address the production, maintenance, and disposal of non-record copies of official documents.

APPENDIX A: MANAGEMENT RESPONSE

EXIM
EXPORT-IMPORT BANK
OF THE UNITED STATES

Helping American Businesses Win the Future

DATE: December 26, 2024

TO: Ms. Ami Schaefer, Acting Assistant Inspector General for Special Reviews

THROUGH: Ravi Singh, Acting Senior Vice President and Chief Financial Officer

FROM: Howard Spira, Senior Vice President and Chief Information Officer HOWARD SPIRA Digitally signed by HOWARD SPIRA Date: 2024.12.26 08:31:36 -05'00'

SUBJECT: EXIM Management Response to the Draft Report *Management Alert: EXIM Did Not Appropriately Safeguard Personally Identifiable Information*

Dear Ms. Schaefer,

Thank you for providing the Export-Import Bank of the United States ("EXIM" or "EXIM Bank") management with the Office of Inspector General's ("OIG") *Management Alert: EXIM Did Not Appropriately Safeguard Personally Identifiable Information (Report No. OIG-O-25-01),* dated December 23, 2024 (the "Report"). EXIM's leadership and management continue to fully support the OIG's work, which we believe complements and enhances EXIM's efforts to continually improve its processes. EXIM Bank is proud of the strong and cooperative relationship it has with the OIG.

EXIM Bank appreciates the OIG's alert of EXIM's management of data covered by the Privacy Act and the recommendations made around appropriately restricting, reporting and managing such data.

EXIM's response to the recommendation in this report is as follows:

Recommendation 1: The Office of Information Management and Technology should immediately restrict access to documents containing Privacy Act information, or any other protected or restricted documentation stored on EXIM's Information Technology (IT) systems, ensuring that only individuals with a need to know have access.

Management response: EXIM concurs with this recommendation. EXIM's Office of Information Management and Technology immediately restricted access to documents containing Privacy Act information, or any other protected or restricted documentation stored on EXIM's Information Technology (IT) systems.

Recommendation 2: The Senior Agency Official for Privacy, in coordination with the Office of General Counsel, should assess within the Office of Management and Budget guidance whether there is a requirement to report the incident, and potential breach, and determine if any of the files were inappropriately accessed by individuals without a need to know.

Management response: EXIM concurs with this recommendation. EXIM's Senior Agency Official for Privacy, in coordination with the Office of General Counsel, will assess within the Office of Management and Budget guidance whether there is a requirement to report the incident, and potential breach, and determine if any of the files were inappropriately accessed by individuals without a need to know.

Recommendation 3: The Chief Information Officer and the Chief Information Security Officer should develop a report regarding the circumstances that led to the incident and the lessons learned that will prevent future incidents and/or improve agency response, as required by EXIM's *Security Incident Handling Policy*.

Management response: EXIM concurs with this recommendation. EXIM's Chief Information Officer and the Chief Information Security Officer will develop a report regarding the circumstances that led to the incident and the lessons learned that will prevent future incidents and/or improve agency response, as required by EXIM's *Security Incident Handling Policy*.

Recommendation 4: The Office of Information Management and Technology should implement any changes or lessons learned identified in the incident report, to include policy changes or updated training that address the production, maintenance, and disposal of non-record copies of official documents.

Management response: EXIM concurs with this recommendation. EXIM's Office of Information Management and Technology will implement any changes or lessons learned identified in the incident report, to include policy changes or updated training that address the production, maintenance, and disposal of non-record copies of official documents.

We look forward to our continued strengthening of our working relationship and working closely with the Office of the Inspector General.

CC:

The Honorable Reta Jo Lewis, President and Chair of the Board of Directors
Brad Belzak, Senior Vice President and Chief of Staff
Hazeen Ashby, Deputy Chief of Staff and White House Liaison
Larry Decker, Senior Advisor to the President and Chair of the Board of Directors
Michaela Smith, Director of Audit and Internal Controls Programs
James Coughlan, Senior Vice President and General Counsel

Office of Inspector General
Export-Import Bank of the United States

811 Vermont Avenue, NW
Washington, DC 20571

Telephone 202-565-3908
Facsimile 202-565-3988

HELP FIGHT

FRAUD, WASTE, AND ABUSE

1- 888-OIG-EXIM
(1-888-644-3946)

https://eximoig.oversight.gov/contact-us

https://eximoig.oversight.gov/hotline

If you fear reprisal, contact EXIM OIG's Whistleblower Protection Coordinator at oig.whistleblower@exim.gov

For additional resources and information about whistleblower protections and unlawful retaliation, please visit the whistleblower's resource page at oversight.gov.