



Management Advisory: Implementation of Watch List Program Presents Potential Legal Risks and Limits Effectiveness



OIG-O-25-04
February 4, 2025

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



MANAGEMENT ADVISORY

To: Victoria Coleman
Deputy General Counsel

From: Eric Rivera
Assistant Inspector General for Audits

Subject: Management Advisory: Implementation of Watch List Program Presents
Potential Legal Risks and Limits Effectiveness (OIG-O-25-04)

Date: February 4, 2025

Executive Summary

The Office of Inspector General (OIG) for Export-Import Bank of the United States (EXIM) found that the agency's implementation of its Watch List program presents potential legal risks to the agency and limits the effectiveness of the program. EXIM's Watch List is a central repository of names of parties for which EXIM personnel have identified concerns. Parties are added to the Watch List when there is a reasonable basis to believe that the party engaged in, or associated with persons that engaged in, criminal conduct or conduct that could adversely affect EXIM.¹

OIG determined that EXIM needs to clarify its Watch List procedures and improve processes to ensure consistent and appropriate treatment of applicants for EXIM financing. OIG found that EXIM's Watch List procedures lack clear requirements for how to manage concerns with applicants that could adversely affect EXIM and how the agency should coordinate with OIG on fraud-related matters. OIG also found that the agency did not provide links to the Watch List system of record notice² (SORN) on its website and identified potential concerns with the legal sufficiency of the Watch List program. Specifically, vagueness regarding the standard for placing

¹ Federal Register Vol. 87, No. 218, Notice of new system of records, *Export Import Bank Privacy Act of 1974; Narrative Statement & System of Records Notice* (November 2022).

² 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."

a party on the Watch List, verifying negative information about the parties, and how the list is used to apply mitigating measures raises concerns regarding fairness and consistency.

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*.³ OIG believes that the evidence obtained provides a reasonable basis for the findings and recommendations outlined below. OIG issued eight recommendations to improve EXIM's Watch List program. In its comments on the draft report, EXIM concurred with the recommendations. OIG considers the recommendations resolved. EXIM's formal response to this management advisory is reprinted in its entirety in Appendix A.

Background

EXIM's procedures describe the Watch List as a due diligence and risk mitigation tool maintained by the Office of General Counsel (OGC). It is a central repository of names of parties (individuals and businesses) that have been referred by EXIM personnel or OIG based on suspicious activity by the applicant. EXIM employees told OIG they did not know when the agency first established the Watch List. However, OGC employees stated that the centralized list was started to eliminate individual lists maintained by EXIM loan officers. EXIM subsequently expanded the Watch List to track activity dates. Beginning in 2020, the agency embedded the Watch List into agency's application system to automatically notify OGC in the event of a match. In such cases, OGC works with loan officers to mitigate any risk of doing business with the identified party.

EXIM's Watch List procedures state the agency will still conduct business with the party unless they are otherwise excluded from doing business with the federal government or do not qualify for a specific transaction. The procedures also state that the Watch List cannot be used to de facto debar parties. As of August 14, 2024, there were 764 parties on the Watch List. Between October 1, 2022, and August 14, 2024, 83 parties were added to the list and three parties were deactivated.⁴

EXIM's Watch List procedures require agency personnel to report any reasonable suspicion of fraud, corruption, or other illegal or untrustworthy activities connected to an EXIM program to OIG, as well as OGC. The procedures state that a party may be added to the Watch List if:

1. The party's misconduct is connected to an EXIM program; and the referral provides sufficient information to determine that:

³ Council of the Inspectors General on Integrity and Efficiency, [Quality Standards for Federal Offices of Inspector General](#) (August 2012).

⁴ As described below, EXIM deactivates parties instead of removing them from the Watch List. EXIM's Watch List policy describes circumstances under which a party is to be removed; the policy makes no reference to deactivation.

- i. there is a reasonable basis to believe that the referred party is involved in a suspicious activity, fraud, corruption, and/or money laundering;
 - ii. the referred party has a reputation for untrustworthy behavior; or
 - iii. the referred party is suspected to be untrustworthy.
2. The referral provides sufficient concrete information that is not publicly available that it would allow EXIM to implement effective mitigating measures to an EXIM transaction.

Similarly, the procedures state that a party may be removed from the Watch List if:

1. The party has been on the Watch List for ten years without a match to a transaction.
2. OGC does not have a record explaining why the party was added to the Watch List.⁵
3. The party has been cleared of any suspicion.

EXIM procedures do not define the terms removal or deactivation, nor do they specify how a removed or deactivated party may be again placed on the Watch List.

OIG announced on July 12, 2024, that it was conducting research on EXIM's Watch List to determine how the Watch List is used and updated and whether further OIG work was necessary. OIG's research included gathering data, reviewing pertinent documents, and conducting meetings with agency officials. OIG reviewed data from October 1, 2022, through August 15, 2024. The research was conducted at EXIM headquarters from July 2024 to November 2024.

OIG Conclusions

OIG found that EXIM's implementation of the Watch List program presents potential legal risks to the agency and limits the effectiveness of the program. As described below, OIG found that EXIM's Watch List procedures lack clear requirements for how to manage concerns with applicants that could adversely affect EXIM and how the agency should coordinate with OIG on fraud matters. OIG also found that the agency did not provide links to the Watch List SORN on its website and identify potential concerns with the legal sufficiency of the Watch List program.

Watch List Program Raises Legal Sufficiency Concerns

OIG identified potential concerns with the legal sufficiency of EXIM's Watch List program. In addition, OIG found that EXIM had not conducted a written assessment nor documented the legal sufficiency of maintaining the Watch List. The vagueness of the standard for placing a party on the Watch List, verifying negative information about the parties, and how the list is used to apply mitigating measures raises concerns regarding fairness and consistency. For example, the lack of standards for concluding suspicious activity exists creates a risk of inconsistency in placing parties on the Watch List. Similarly, the lack of clarity regarding how a

⁵ This would generally pertain to names that were added to the Watch List prior to 2020.

concern is confirmed or updated at the time of a match creates a risk of inconsistency and insufficient due diligence in assessing the need for mitigation. Finally, the lack of clarity regarding when mitigation is required, the scope of mitigation available to EXIM, and whether the party is notified of the reason for the requirement and given an opportunity to provide feedback creates concerns about consistency and reasonableness.

During this engagement, EXIM employees told OIG the agency recently updated its procedures to clarify the standards they use and worked with the Office of the Chief Information Officer to make enhancements to the program. The *Standards for Internal Control in the Federal Government*⁶ require that management identify, analyze, and respond to risks related to achieving the defined objectives. Uncertainty regarding the legal sufficiency of this process and how the list is used to apply mitigating measures raises concerns regarding fairness and consistency and could place the agency at greater legal risk.

Watch List Procedures Lacked Clarity

OIG found that EXIM's Watch List procedures lack clear requirements for managing concerns with applicants that could adversely affect EXIM. Specifically, OIG identified the following issues:

- The procedures do not explain when mitigating measures should be applied to an applicant on the Watch List, or what, if any, measures can be added to mitigate the risk of doing business with a party. Mitigating measures should be applied to applicants consistently based on the concern(s) identified. EXIM also did not clearly document mitigating measures applied to an applicant and the results of the application process for participants on the Watch List.
- EXIM procedures do not clearly state how the agency is to add parties to the Watch List. For example, the procedures do not specify what constitutes a reputation for suspicion or untrustworthy behavior or a referral from another agency.
- The procedures do not specify the actions that EXIM takes to verify the information that results in a party being added to the Watch List to update the information if a match occurs regarding a subsequent transaction or clear the party of suspicion when there is a match.
- The procedures and EXIM's practices regarding parties EXIM determines should no longer be on the Watch List are unclear. The procedures mention removal from the Watch List, but EXIM employees told OIG that parties are not removed and instead remain on the Watch List but are "deactivated" and not scanned against applicants for matches. EXIM does not proactively determine if parties should be removed or deactivated from the list based on applicable criteria; parties are only deactivated if there is a match to an application and the removal criteria is met. In addition, as stated

⁶ Government Accountability Office, [Standards for Internal Control in the Federal Government](#) (GAO-14-704G, September 2014).

above, EXIM procedures do not define the terms removal or deactivation nor do they specify how a removed or deactivated party may be again placed on the Watch List. An EXIM employee told OIG that the agency deactivates parties, instead of removing parties, to maintain a record of who was on the Watch List and why. The EXIM employee also said the agency would follow the Watch List procedures for adding parties if a deactivated party should be added back to the Watch List.

The *Standards for Internal Control in the Federal Government*⁷ require management to implement control activities through policies and design the entity's information system and related control activities to achieve objectives and respond to risks. A lack of clarity within EXIM's Watch List procedures, including the lack of defining the terms "removal" and "deactivation," could lead to parties being inconsistently and inappropriately included on the Watch List for suspicious activity. Additionally, without clearly defined tools for mitigating risks, there is a risk that mitigating measures may be applied inconsistently to parties on the Watch List, creating concerns for fairness and consistency.

EXIM Coordination Mechanism with OIG Unclear

OIG found that EXIM had not established a clear mechanism for coordinating with OIG on fraud matters related to the Watch List. Specifically, OIG found that OGC did not have a clear process for coordinating with OIG on information regarding suspicious activity and ongoing OIG investigations. EXIM's Watch List procedures do not state a requirement or a documented process for outreach to or coordination with OIG on potential fraud, corruption, or money laundering, either when the party is placed on the Watch List, or when a match is confirmed.

The Government Accountability Office's *Framework for Managing Fraud Risks in Federal Programs*⁸ states that agency should collaborate and communicate with OIG to improve the agency's understanding of fraud risks and align efforts to address fraud. In the absence of clearly defined processes for communications between the agency and OIG, the agency is potentially exposed to increased fraud risk.

System of Record Notice Not Posted in Accordance with Federal Guidance

Finally, OIG identified that EXIM's SORN for the Watch List was not posted on its public website, as required. The Office of Management and Budget Circular A-108⁹ states that agencies shall list and provide links to complete, up-to-date versions of all agency SORNs on their website. During this engagement, EXIM employees told OIG that there is no specific reason that the

⁷ Government Accountability Office, [Standards for Internal Control in the Federal Government](#) (GAO-14-704G, September 2014).

⁸ Government Accountability Office, [A Framework for Managing Fraud Risks in Federal Programs](#) (GAO-15-593SP, July 2015).

⁹ Office of Management and Budget, [Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act](#) (Circular A-108, December 2016).

SORN was not on the website and indicated they would remind the website administrators to post it. By not publicizing the SORN on EXIM's website, applicants may not be aware of the existence of the Watch List.

As previously noted, EXIM considers the Watch List a due diligence and risk management tool. OIG plans to initiate a review of EXIM's due diligence processes during FY 2025 to assess the effectiveness of EXIM's due diligence processes related to potential EXIM transaction participants. Accordingly, OIG is not opining on the overall efficacy of EXIM's due diligence process.

Recommendations

OIG issued eight recommendations to improve EXIM's Watch List program. In its comments on the draft report, EXIM concurred with the recommendations. OIG considers the recommendations resolved.

Recommendation 1: The Office of General Counsel should conduct and document an assessment on the legal sufficiency of the Watch List program and its impact on addressing potential applicant misconduct or untrustworthiness through mitigation measures and document their conclusions.

Recommendation 2: The Office of General Counsel should update the Watch List procedures to include examples of risks warranting mitigating measures and what mitigating measures can be applied to parties when there is a match.

Recommendation 3: The Office of General Counsel should implement documentation requirements for actions taken as a result of Watch List matches, to include support for taking mitigating measures.

Recommendation 4: The Office of General Counsel should update the Watch List procedures to include examples of a suspicion and reputation of untrustworthy behavior and to add parties based on referrals from other agencies.

Recommendation 5: The Office of General Counsel should update the Watch List procedures to align with actual practices regarding parties EXIM determines should no longer be on the Watch List; the standards for deactivation or removal, including when there is a match to a party that should be deactivated or removed; and in the case of deactivation what the implications are for future searches and reactivation.

Recommendation 6: The Office of General Counsel, in coordination with the Office of the Chief Information Officer, should implement a process for automatically deactivating or removing parties that have been on the Watch List over 10 years without a match.

Recommendation 7: The Office of General Counsel should state and implement a requirement in the procedures and develop a process to concurrently notify OIG whenever there are

new parties added to the Watch List, there are true matches on the Watch List, and there are parties removed or deactivated from the Watch List.

Recommendation 8: The Office General Counsel, in coordination with the Office of Communications, should upload the Watch List system of record notice to EXIM's public website.

APPENDIX A: MANAGEMENT RESPONSE



Helping American Businesses Win the Future

DATE: January 23, 2025

TO: Eric Rivera, Assistant Inspector General for Audit, Office of Inspector General

THROUGH: Ravi Singh, Acting Chief Financial Officer

FROM: Victoria Coleman, Deputy General Counsel and Acting General Counsel

SUBJECT: EXIM Management Response to the Report
Management Advisory: Implementation of Watch List Program Presents Potential Legal Risks and Limits Effectiveness (OIG-O-25-04)

RAVI SINGH

Digitally signed by RAVI SINGH
Date: 2025.01.24
15:42:49 -05'00'

VICTORIA COLEMAN

Digitally signed by VICTORIA COLEMAN
Date: 2025.01.24
16:23:11 -05'00'

Dear Mr. Rivera,

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 Advisory: Implementation of Watch List Program Presents Potential Legal Risks and Limits Effectiveness (OIG-O-25-04)*, dated January 22, 2025 (the “Report”). Management continues to support the OIG’s work which complements EXIM’s efforts to continually improve its processes.

EXIM Bank values the OIG’s comprehensive review and concurs with all of the recommendations in the Report. Although the Report concludes that the Watch List program presents potential legal risks to EXIM Bank, the OIG has not identified any legal violations. Further, and contrary to the Report, the Watch List Procedures do have standards for placing a party on and removing a party from the Watch List. Nevertheless, EXIM remains committed to taking prompt and decisive action to enhance its processes and improve its procedures, where it is pertinent to do so.

EXIM thanks the OIG for its efforts to ensure EXIM’s policies and procedures continue to improve, as well as the work it does to protect EXIM from fraud, waste, and abuse. EXIM looks forward to continuing to strengthen the working relationship with the OIG.

Please find the eight recommendations from the Report and the corresponding management responses below.

Recommendation 1: The Office of General Counsel should conduct and document an assessment on the legal sufficiency of the Watch List program and its impact on addressing potential applicant misconduct or untrustworthiness through mitigation measures and document their conclusions.

Management response: EXIM concurs with this recommendation. The Office of General Counsel will conduct and document an assessment on the legal sufficiency of the Watch List program and its impact on addressing potential applicant misconduct or untrustworthiness through mitigation measures and document their conclusions.

Recommendation 2: The Office of General Counsel should update the Watch List procedures to include examples of risks warranting mitigating measures and what mitigating measures can be applied to parties when there is a match.

Management response: EXIM concurs with this recommendation. The Office of General Counsel will update the Watch List procedures to include examples of risks warranting mitigating measures and what mitigating measures can be applied to parties when there is a match.

Recommendation 3: The Office of General Counsel should implement documentation requirements for actions taken as a result of Watch List matches, to include support for taking mitigating measures.

Management response: EXIM concurs with this recommendation. The Office of General Counsel will implement documentation requirements for actions taken as a result of Watch List matches, to include support for taking mitigating measures.

Recommendation 4: The Office of General Counsel should update the Watch List procedures to include examples of a suspicion and reputation of untrustworthy behavior and to add parties based on referrals from other agencies.

Management response: EXIM concurs with this recommendation. The Office of General Counsel will update the Watch List procedures to include examples of a suspicion and reputation of untrustworthy behavior and to add parties based on referrals from other agencies.

Recommendation 5: The Office of General Counsel should update the Watch List procedures to align with actual practices regarding parties EXIM determines should no longer be on the Watch List; the standards for deactivation or removal, including when there is a match to a party that should be deactivated or removed; and in the case of deactivation what the implications are for future searches and reactivation.

Management response: EXIM concurs with this recommendation. The Office of General Counsel will update the Watch List procedures to align with actual practices regarding parties EXIM determines should no longer be on the Watch List; the standards for deactivation or removal, including when there is a match to a party that should be deactivated or removed; and in the case of deactivation what the implications are for future searches and reactivation.

Recommendation 6: The Office of General Counsel, in coordination with the Office of the Chief Information Officer, should implement a process for automatically deactivating or removing parties that have been on the Watch List over 10 years without a match.

Management response: EXIM concurs with this recommendation. The Office of General Counsel, in coordination with the Office of the Chief Information Officer, will implement a process for automatically deactivating or removing parties that have been on the Watch List over 10 years without a match.

Recommendation 7: The Office of General Counsel should state a requirement in the procedures and develop a process to concurrently notify OIG whenever there are new parties added to the Watch List, there are true matches on the Watch List, and there are parties removed or deactivated from the Watch List.

Management response: EXIM concurs with this recommendation. The Office of General Counsel will state a requirement in the procedures and develop a process to concurrently notify OIG whenever there are new parties added to the Watch List, there are true matches on the Watch List, and there are parties removed or deactivated from the Watch List.

Recommendation 8: The Office of General Counsel, in coordination with the Office of Communications, should upload the Watch List system of record notice to EXIM's public website.

Management response: EXIM concurs with this recommendation. The Office of General Counsel, in coordination with the Office of Communications, will upload the Watch List system of record notice to EXIM's public website.

CC:

Mark Chu, Assistant General Counsel, Litigation, Fraud and Compliance

Marina Braginskaya, Senior Counsel, Litigation, Fraud and Compliance

Jennifer Cowan, Counsel, Litigation, Fraud and Compliance

Michaela Smith, Director of Audit and Internal Controls Program | Internal Controls and Compliance

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](https://www.oversight.gov).