Office of the Inspector General
U.S. Department of Justice

Public Summary

Audit of the Federal Bureau of Investigation's Insider Threat Program

Audit Division 17-35 September 2017

PUBLIC SUMMARY

AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S INSIDER THREAT PROGRAM

The Federal Bureau of Investigation (FBI) is charged with protecting some of America's most sensitive secrets from enemies both foreign and domestic. Threats to these secrets can come from outside the FBI, such as foreign intelligence agencies or international or domestic hackers, as well as from inside the FBI, such as employees and contractors with access to national security-related information. After the 2010 leak of classified material by a U.S. Army intelligence analyst, President Obama issued Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information." This executive order created the National Insider Threat Task Force (NITTF) and directed all agencies that operate or access classified computer networks to designate a senior official to oversee the safeguarding of classified information and establish an insider threat and detection program.

The NITTF defines an "insider threat" as "someone who misuses or betrays, wittingly or unwittingly, his or her authorized access to any U.S. Government resource." Because of the severity of the damage insider threats can inflict, one of the FBI's Counterintelligence Division's top goals is to, "Protect the secrets of the U.S. intelligence community, using intelligence to focus our investigative efforts and collaborating with our government partners to reduce the risk of espionage and insider threats."

In November 2012, as required by Executive Order 13587, the NITTF developed the National Insider Threat Policy and Minimum Standards. In February 2014, to comply with the policy and standards, former FBI Director James Comey approved the establishment of the Insider Threat Center (InTC) and later designated the InTC's Section Chief as the FBI's designated senior official under the Executive Order.

The Department of Justice Office of the Inspector General (OIG) performed an audit to examine the Insider Threat Program's (InTP) adherence to the NITTF's National Insider Threat Policy and Minimum Standards, as well as other related policies. Our audit focused on the period of April 2014 through March 2017.

To accomplish our objective, we interviewed FBI officials, including individuals from the FBI's Insider Threat Center and entities that process leads from the Insider Threat Center, including the Security Division, Inspection Division, Counterintelligence Division, and the Critical Incident Response Group. We also spoke with individuals with responsibilities related to insider threat from the Information Technology Branch, Human Resources Division, Finance Division, the

Office of the Chief Information Officer, the Resource Planning Office, and the Office of General Counsel.

We also interviewed staff from other government agencies and entities to learn about their efforts to manage and oversee insider threat programs, including the National Insider Threat Task Force, the Government Accountability Office, the Central Intelligence Agency Office of Inspector General and Office of Medical Services, the Defense Intelligence Agency Office of Inspector General, and the National Security Agency Office of Psychological Assessment Services.

We reviewed insider threat policy, guidance, plans, and assessments, including Executive Order 13587, the National Insider Threat Policy and Minimum Standards, Committee on National Security Systems Directive 504, and FBI Insider Threat Program Policy Directive 0863D. To assess insider threat internal controls, we reviewed insider threat leads tracked in the FBI's Sentinel case management system, and compared results from past FBI information technology asset inventory efforts.

Based on the results of our audit, this report makes the following eight recommendations that we believe will improve the FBI's program for deterring, detecting and mitigating malicious insider threats. The FBI agreed with all eight recommendations, as described in Attachment 1. Our analysis of those responses and the summary of actions necessary to close the report are found in Attachment 2. The final OIG audit report contains classified national security information and the overall classification of the report is "Secret."

1. Track, summarize, and annually report InTP performance metrics as required.

2. Ensure that leads and referrals concerning insider threats are handled and monitored in a systematic way, including making sure that leads go to the appropriate point of contact at each internal FBI component.

3. Pursue technological solutions to mitigate the need for, or reduce the risk of, stand-alone systems.

4. Conduct a comprehensive inventory of classified networks, systems, applications, and other information technology assets and identify a component responsible for maintaining the inventory.

5. Ensure user activity monitoring (UAM) coverage over all classified systems and networks and identify a component to maintain an accurate inventory of all information technology assets that have user activity monitoring coverage.

6. Perform a comprehensive review of the Insider Threat Risk Board (ITRB) charter, update as needed, and ensure that the board meets as is determined to be appropriate.[1]

7. Conduct an assessment to determine whether pre-employment psychological evaluations or an expansion of psychological evaluations for current employees should be implemented to improve its insider threat prevention efforts.

8. Ensure that the OIG receives notification of all insider threat investigations, including threats classified as counterespionage, in a timely manner, consistent with the Inspector General Act and Department regulations.

[1] The FBI established the ITRB in 2014 and assigned it the mission of "determin[ing] mitigation plans for personnel who pose a potential insider threat, as well as prioritiz[ing] and resolv[ing] conflicts between divisions regarding proposed solutions to significant Insider Threat vulnerabilities." Pursuant to its existing charter, it is supposed to meet on a monthly basis.

ATTACHMENT 1

FEDERAL BUREAU OF INVESTIGATION'S RESPONSE TO THE DRAFT AUDIT REPORT

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

September 20, 2017

The Honorable Michael E. Horowitz
Inspector General
Office of the Inspector General
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530

Dear Mr. Horowitz:

The Federal Bureau of Investigation (FBI) appreciates the opportunity to review and respond to your office's report entitled, *Audit of the Federal Bureau of Investigation's Insider Threat Program.*

We are pleased that you found, "The FBI has made much progress regarding the NITTF's [National Insider Threat Task Force] minimum standards, improving internal communications, and developing analytical tools to aid in identifying and coordinating the investigation into potential insider threats."

We agree that it is important to continue the progress that has been made to date in regards to the FBI's Insider Threat Program to include a comprehensive inventory of FBI IT assets and monitoring of those assets. In that regard, we concur with the eight recommendations for the FBI.

Should you have any questions, feel free to contact me. We greatly appreciate the professionalism of your audit staff throughout this matter.

Sincerely,

James C. Langenberg
Section Chief
External Audit and Compliance Section
Inspection Division

Enclosure

The Federal Bureau of Investigation's (FBI) Response to the Office of the Inspector General's Audit of the FBI's Insider Threat Program

Report Recommendation #1: "The OIG recommends the FBI track, summarize, and annually report InTP performance metrics as required."

FBI Response to Recommendation #1: Concur. The FBI, as noted in the subject report, is actively developing the Javelin system which will assist in the collection of performance metrics for the program.

Report Recommendation #2: "The OIG recommends that the FBI ensure that leads and referrals concerning insider threats are handled and monitored in a systematic way, including making sure that leads go to appropriate point of contact at each internal FBI component."

FBI Response to Recommendation #2: Concur. The FBI, as noted in the subject report, is actively developing the Javelin system to automate the process and improve de-confliction.

Report Recommendation #3: "The OIG recommends that the FBI pursue technological solutions to mitigate the need for, or reduce the risk of, stand-alone systems."

FBI Response to Recommendation #3: Concur. The FBI will pursue technological solutions to mitigate the need for, or reduce the risk of, stand-alone systems.

Report Recommendation #4: "The FBI Conduct a comprehensive inventory of classified networks, systems, applications, and other IT assets and identify a component responsible for maintaining the inventory.

FBI Response to Recommendation #4: Concur. The FBI will conduct a comprehensive inventory of classified networks, systems, applications, and other IT assets and identify a component responsible for maintaining the inventory.

Report Recommendation #5: "The OIG recommends the FBI ensure UAM coverage over all classified systems and networks and identify a component to maintain an accurate inventory of all IT assets that have UAM coverage."

FBI Response to Recommendation #5: Concur. The FBI will identify and prioritize critical systems/networks which require UAM. This should be a risk based decision process undertaken in conjunction with the OCIO so there is alignment with all threat vectors across the organization.

Report Recommendation #6: "The OIG recommends the FBI perform a comprehensive review of the ITRP charter, update as needed, and ensure that the ITRP meets as is determined to be appropriate."

FBI Response to Recommendation #6: Concur. The FBI will perform a comprehensive review of the ITRP charter.

Report Recommendation #7: "The OIG recommends the FBI conduct an assessment to determine whether pre-employment psychological evaluations or an expansion of psychological evaluations for current employees should be implemented to improve its insider threat prevention efforts."

FBI Response to Recommendation #7: Concur. The FBI is actively assessing the feasibility of psychological evaluations.

Report Recommendation #8: "The OIG recommends the FBI ensure that the OIG receives notification of all insider threat investigations, including threats classified as counterespionage, in a timely manner, consistent with the Inspector General Act and Department regulations."

FBI Response to Recommendation #8: Concur. Pursuant to an agreement between the Assistant Director of the FBI's Counterintelligence Division and the Inspector General, beginning in September 2017, the FBI will periodically brief the OIG regarding insider threat investigations.

ATTACHMENT 2

OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT

The OIG provided a draft of the audit report to the Federal Bureau of Investigation (FBI). The FBI's response is incorporated in Attachment 1. The following provides the OIG analysis of the response and summary of actions necessary to close the report.

Recommendations:

1. **Track, summarize, and annually report InTP performance metrics as required.**

   Resolved. The FBI concurred with our recommendation. In its response, the FBI stated that it is actively developing a new system which will assist in the collection of performance metrics for the program.

   This recommendation can be closed when we receive evidence that the FBI had deployed the new system, is utilizing the system to track and summarize InTP performance metrics, and documents those metrics in an annual report as required.

2. **Ensure that leads and referrals concerning insider threats are handled and monitored in a systematic way, including making sure that leads go to the appropriate point of contact at each internal FBI component.**

   Resolved. The FBI concurred with our recommendation. In its response, the FBI stated that it is actively developing a system that will automate the process and improve deconfliction.

   This recommendation can be closed when we receive evidence that the FBI has deployed the system and standardized the handling of leads.

3. **Pursue technological solutions to mitigate the need for, or reduce the risk of, stand-alone systems.**

   Resolved. The FBI concurred with our recommendation. In its response, the FBI said that it will pursue technological solutions to mitigate the need for, or reduce the risk of, stand-alone systems.

This recommendation can be closed when we receive evidence that the FBI has developed a technological solution that mitigates or reduces the risks posed by the use of stand-alone systems.

4. **Conduct a comprehensive inventory of classified networks, systems, applications, and other information technology assets and identify a component responsible for maintaining the inventory.**

   Resolved. The FBI concurred with our recommendation. In its response, the FBI said it will conduct a comprehensive inventory of classified networks, systems, applications, and other IT assets and identify a component responsible for maintaining the inventory.

   This recommendation can be closed when we receive evidence that an inventory has been conducted and that a component has been tasked with maintaining that inventory.

5. **Ensure user activity monitoring (UAM) coverage over all classified systems and networks and identify a component to maintain an accurate inventory of all information technology assets that have user activity monitoring coverage.**

   Resolved. The FBI concurred with our recommendation. In its response, the FBI said it will identify and prioritize critical systems/networks which require UAM and that this should be a risk based decision undertaken in conjunction with the Office of the Chief Information Officer (OCIO) so there is alignment with all threat vectors across the organization. We consider the recommendation resolved because the FBI concurred; however, current policy requires that all classified systems have UAM coverage. We agree that prioritizing IT assets based on risk is a good idea for adding UAM coverage to those assets, but in order to meet the policy as it is currently written, all classified assets must have UAM coverage. Further, the FBI did not mention how it will maintain an inventory of all IT assets that have UAM coverage. We will work with the FBI to ensure that this portion of the recommendation is completed.

   This recommendation can be closed when we receive evidence that all classified networks and systems have UAM coverage and that a component has been tasked with maintaining an accurate inventory of all IT assets that have UAM coverage.

6. **Perform a comprehensive review of the Insider Threat Risk Board (ITRB) charter, update as needed, and ensure that the board meets as is determined to be appropriate.**

   Resolved. The FBI concurred with our recommendation. In its response, the FBI said it will perform a comprehensive review of the ITRB charter.

   This recommendation can be closed when we receive evidence that the charter has been reviewed and that the board is meeting as required by the charter.

7. **Conduct an assessment to determine whether pre-employment psychological evaluations or an expansion of psychological evaluations for current employees should be implemented to improve its insider threat prevention efforts.**

   Resolved. The FBI concurred with our recommendation. In its response, the FBI said it is actively assessing the feasibility of psychological evaluations.

   This recommendation can be closed when we receive evidence that the assessment has been completed.

8. **Ensure that the OIG receives notification of all insider threat investigations, including threats classified as counterespionage, in a timely manner, consistent with the Inspector General Act and Department regulations.**

   Resolved. The FBI concurred with our recommendation. In its response, the FBI said that, pursuant to an agreement between the Assistant Director of the Counterintelligence Division and the Inspector General, beginning in September 2017 the FBI will periodically brief the OIG regarding insider threat investigations.

   This recommendation can be closed when we receive evidence that those briefings are taking place and that the OIG is receiving notification of insider threat investigations, including threats classified as counterespionage, in a timely manner.

The Department of Justice Office of the Inspector General (DOJ OIG) is a statutorily created independent entity whose mission is to detect and deter waste, fraud, abuse, and misconduct in the Department of Justice, and to promote economy and efficiency in the Department's operations. Information may be reported to the DOJ OIG's hotline at www.justice.gov/oig/hotline or (800) 869-4499.

Office of the Inspector General
U.S. Department of Justice
www.justice.gov/oig