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

Washington, D.C.
FBI National Press Office
(202) 324-3691

November 10, 2021

Rachel Rojas Named Assistant Director of the Insider Threat Office

Director Christopher Wray has named Rachel Rojas as the assistant director of the Insider Threat Office at FBI Headquarters in Washington, D.C. Ms. Rojas most recently served as the special agent in charge of the Jacksonville Field Office in Florida.

The Insider Threat Office is the FBI's central strategic coordinating component for all insider threat issues.

Ms. Rojas joined the FBI in 1996 as an investigative specialist for the New York Field Office. She successfully applied to become a special agent and completed her academy training in 2000. As an agent, Ms. Rojas returned to New York to investigate administrative and drug matters. After 9/11, she investigated financing data and communications tied to the attack.

In 2005, Ms. Rojas was promoted to a supervisory special agent and transferred to the Terrorism Financing Operations Section of the Counterterrorism Division at FBI Headquarters. She returned to New York in 2007 to oversee the applicant program, then moved to focus on mortgage and bank fraud.

In 2012, she was promoted to assistant special agent in charge of New York's Criminal Division. She was responsible for overseeing complex financial crime threats, public corruption, civil rights, health care fraud, and other issues. The next year, Ms. Rojas was named assistant special agent in charge over New York's Violent Criminal Threat Branch, managing the Safe Streets gang and violent crime task forces, bank robberies, fugitives, human trafficking, and other programs.

Ms. Rojas returned to FBI Headquarters in 2015 as a section chief in the Security Division, responsible for the physical and technical protection of FBI personnel, facilities, information, and operations worldwide. In 2019, Ms. Rojas became the FBI's first Latina special agent in charge when she was appointed to lead the Jacksonville Field Office in Florida.

Ms. Rojas earned a bachelor's degree in communications/journalism from Boston University and a master's in international management/leadership from Manhattanville College.

RECENT INSIDER THEFT CASES

Michael Mitchell, a sales clerk and engineer, became disgruntled and was fired from his job based on poor performance. Mitchell signed statements affirming he had returned all proprietary information to his employer and was reminded of nondisclosure policies. However, Mitchell kept numerous computer files, entered into a consulting agreement with a rival Korean company, and provided trade secrets from his former employer to that company. In March 2010, he was sentenced to 18 months in prison and ordered to pay his previous employer over $187,000.

Shalin Jhaveri, a technical operations associate, gave trade secrets to a person he believed was an investor willing to finance a business venture in India, and confirmed to the investor that the information he had taken from his employer was everything he needed to start the business. He confessed that he disguised his actions to evade detection. In January 2011, he was sentenced to time served (one year and fifteen days), three years probation, a $5,000 fine, and a $100 Special Assessment.

David Yen Lee accepted a job on 27 February 2009 from a business competitor in China, but did not resign from his current employer until 16 March 2009. Lee admitted to downloading trade secrets from his employer's secured computer system for several months prior to his resignation. The stolen trade secrets were worth between $7 million and $20 million. In December 2010, Lee was sentenced to 15 months in prison and three years supervised release.

Sergey Aleynikov, a computer programmer, worked for a company on Wall Street from May 2007 until June 2009. During his last few days at that company, he downloaded, and transferred 32 megabytes of proprietary computer codes– a theft that could have cost his employer millions of dollars. He hoped to use the computer codes at his new Chicago-based employer. He attempted to hide his activities, but the company discovered irregularities through its routine network monitoring systems. In December 2010, Aleynikov was found guilty of theft of trade secrets and transportation of stolen property in foreign commerce.

Greg Chung spied for China from 1979-2006. Federal charges against Chung consisted of stealing trade secrets about the space shuttle, the Delta IV rocket and the C-17 military cargo jet for the benefit of the Chinese government. Chung's motive was to "contribute to the Motherland." He was an engineer that stole hundreds of thousands of documents. He traveled to China under the guise of giving lectures while secretly meeting with Chinese government officials and agents. He was also encouraged to use Chi Mak (see below) to transfer information back to China. Chung was arrested in February 2008 and in February 2010 he was sentenced to over 15 years in prison.

Chi Mak admitted that he was sent to the United States in 1978 in order to obtain employment in the defense industry with the goal of stealing US defense secrets, which he did for 20 plus years. He most recently passed information on quiet electric propulsion systems for the next generation of US submarines, details on the Aegis radar system, and information on stealth ships being developed by the US Navy. The Chinese government tasked Mak to acquire information on other specific technologies. Mak recruited family members to encrypt and covertly courier information back to China. In May 2007, Chi Mak was convicted of conspiracy, attempting to violate export control laws, failing to register as an agent of a foreign government, and making false statements to investigators. He was sentenced to over 24 years in prison, and four members of his family received varying sentences of up to 10 years in prison.

For additional information, training, or assistance, contact the FBI.
www.fbi.gov

U.S. Department of Justice
Federal Bureau of Investigation

A company can often detect or control when an outsider (non-employee) tries to access company data either physically or electronically, and can mitigate the threat of an outsider stealing company property. However, the thief who is harder to detect and who could cause the most damage is the insider–the employee with legitimate access. That insider may steal solely for personal gain, or that insider may be a "spy"–someone who is stealing company information or products in order to *benefit another organization or country.*

THE INSIDER THREAT

An introduction to detecting and deterring an insider spy

- Disgruntled
- Working odd hours
- Unexplained affluence
- Unreported foreign travel

This brochure serves as an introduction for managers and security personnel on how to detect an insider threat and provides tips on how to safeguard your company's trade secrets.

PROTECT YOUR INTELLECTUAL PROPERTY

Theft of intellectual property is an increasing threat to organizations, and can go unnoticed for months or even years.

There are increased incidents of employees taking proprietary information when they believe they will be, or are, searching for a new job.

Congress has continually expanded and strengthened criminal laws for violations of intellectual property rights to protect innovation and ensure that egregious or persistent intellectual property violations do not merely become a standard cost of doing business.

A domestic or foreign business competitor or foreign government intent on illegally acquiring a company's proprietary information and trade secrets may wish to place a spy into a company in order to gain access to non-public information. Alternatively, they may try to recruit an existing employee to do the same thing.

PERSONAL FACTORS

There are a variety of motives or personal situations that may increase the likelihood someone will spy against their employer:

Greed or Financial Need: A belief that money can fix anything. Excessive debt or overwhelming expenses.

Anger/Revenge: Disgruntlement to the point of wanting to retaliate against the organization.

Problems at work: A lack of recognition, disagreements with co-workers or managers, dissatisfaction with the job, a pending layoff.

Ideology/Identification: A desire to help the "underdog" or a particular cause.

Divided Loyalty: Allegiance to another person or company, or to a country besides the United States.

Adventure/Thrill: Want to add excitement to their life, intrigued by the clandestine activity, "James Bond Wannabe."

Vulnerability to blackmail: Extra-marital affairs, gambling, fraud.

Ego/Self-image: An "above the rules" attitude, or desire to repair wounds to their self-esteem. Vulnerability to flattery or the promise of a better job. Often coupled with Anger/Revenge or Adventure/ Thrill.

Ingratiation: A desire to please or win the approval of someone who could benefit from insider information with the expectation of returned favors.

Compulsive and destructive behavior: Drug or alcohol abuse, or other addictive behaviors.

Family problems: Marital conflicts or separation from loved ones.

ORGANIZATIONAL FACTORS

Organizational situations may increase the ease for thievery:

The availability and ease of acquiring proprietary, classified, or other protected materials. Providing access privileges to those who do not need it.

Proprietary or classified information is not labeled as such, or is incorrectly labeled.

The ease that someone may exit the facility (or network system) with proprietary, classified or other protected materials.

Undefined policies regarding working from home on projects of a sensitive or proprietary nature.

The perception that security is lax and the consequences for theft are minimal or non-existent.

Time pressure: Employees who are rushed may inadequately secure proprietary or protected materials, or not fully consider the consequences of their actions.

Employees are not trained on how to properly protect proprietary information.

BEHAVIORAL INDICATORS

Some behaviors may be a clue that an employee is spying and/ or methodically stealing from the organization:

Without need or authorization, takes proprietary or other material home via documents, thumb drives, computer disks, or e-mail.

Inappropriately seeks or obtains proprietary or classified information on subjects not related to their work duties.

Interest in matters outside the scope of their duties, particularly those of interest to foreign entities or business competitors.

Unnecessarily copies material, especially if it is proprietary or classified.

Remotely accesses the computer network while on vacation, sick leave, or at other odd times.

Disregards company computer policies on installing personal software or hardware, accessing restricted websites, conducting unauthorized searches, or downloading confidential information.

Works odd hours without authorization; notable enthusiasm for overtime work, weekend work, or unusual schedules when clandestine activities could be more easily conducted.

Unreported foreign contacts (particularly with foreign government officials or intelligence officials) or unreported overseas travel.

Short trips to foreign countries for unexplained or strange reasons.

Unexplained affluence; buys things that they cannot afford on their household income.

Engages in suspicious personal contacts, such as with competitors, business partners or other unauthorized individuals.

Overwhelmed by life crises or career disappointments.

Shows unusual interest in the personal lives of co-workers; asks inappropriate questions regarding finances or relationships.

Concern that they are being investigated; leaves traps to detect searches of their work area or home; searches for listening devices or cameras.

Many people experience or exhibit some or all of the above to varying degrees; however, most people will not cross the line and commit a crime.

YOU CAN MAKE A DIFFERENCE

Organizations need to do their part to deter intellectual property theft:

- Educate and regularly train employees on security or other protocols.
- Ensure that proprietary information is adequately, if not robustly, protected.
- Use appropriate screening processes to select new employees.
- Provide non-threatening, convenient ways for employees to report suspicions.
- Routinely monitor computer networks for suspicious activity.
- Ensure security (to include computer network security) personnel have the tools they need.

Remind employees that reporting security concerns is vital to protecting your company's intellectual property, its reputation, its financial well-being, and its future. They are protecting their own jobs. Remind them that if they see something, to say something.

GET ASSISTANCE

Being aware of potential issues, exercising good judgment, and conducting discrete inquiries will help you ascertain if there is a spy in your midst. However, if you believe one of your employees is a spy or is stealing company trade secrets, do not alert the person to the fact that he/she is under suspicion, but seek assistance from trained counterintelligence experts–such as the FBI. The FBI has the tools and experience to identify and mitigate such threats. If asked to investigate, the FBI will minimize the disruption to your business, and safeguard your privacy and your data. Where necessary, the FBI will seek protective orders to preserve trade secrets and business confidentiality. The FBI is committed to maintaining the confidentiality and competitive position of US companies. The FBI will also provide security and counterintelligence training or awareness seminars for you and your employees upon request.

INSIDER THREATS

FBI Employee Was 'Insider Threat' for 12 Years

By SecureWorld News Team

Read more about the author

MON | MAY 24, 2021 | 12:11 PM PDT

She had been a long-term and trusted employee of the FBI, working out of the Bureau's Kansas City office.

However, prosecutors now say she was much more than that. She was also an insider threat, according to a newly unsealed federal indictment.

Kendra Kingsbury, a 48-year-old FBI analyst, is accused of removing "Secret" and "Classified" documents relating to a number of FBI operations. This includes details on how the agency is trying to defend the United States against cyber threats.

FBI analyst accused of being insider threat

If you are in an analyst role long-term, you likely support all kinds of efforts and teams based on where there is a need.

Over her 12-year career, Kingsbury worked for several different FBI squads, including those focused on illegal drug trafficking, violent crime, violent gangs, and counterintelligence.

And she is accused of illegally taking home secret and classified documents for almost her entire career:

Most Recent

POLICY

DOJ Announces New Policy for Computer Fraud and Abuse Act

Most Popular

E. Kohler, Jr. Assistant Director of the FBI's Counterintelligence Division.

"The defendant, who's well trained in handling classified information, put her country's sensitive secrets at risk. The FBI will go to great lengths to investigate individuals who put their own interests above U.S. national security, including when the individual is an FBI employee."

Specific accusations against the FBI insider threat

The court documents reveal two specific charges against Kingsbury. One charge relates to domestic documents she is accused of stealing:

"Count one of the federal indictment relates to numerous documents classified at the secret level that describe intelligence sources and methods related to U.S. government efforts to defend against counterterrorism, counterintelligence and cyber threats.

The documents include details on the FBI's nationwide objectives and priorities, including specific open investigations across multiple field offices. In addition, there are documents relating to sensitive human source operations in national security investigations, intelligence gaps regarding hostile foreign intelligence services and terrorist organizations, and the technical capabilities of the FBI against counterintelligence and counterterrorism targets."

The second charge relates to international operations and foreign intelligence:

"Count two of the federal indictment relates to numerous documents classified at the secret level that describe intelligence sources and methods related to U.S. government efforts to collect intelligence on terrorist groups. The documents include information about al Qaeda members on the African continent, including a suspected associate of Usama bin Laden.


CYBER LAW

Suing the CISO: SolarWinds Fires Back

More Like This


NETWORK SECURITY

Insider Threats at AT&T Wireless Activated by Cybercriminals

Africa."

Ponemon on why insider threats are so challenging to stop

We asked Dr. Larry Ponemon, founder of the Ponemon Institute, why insider threats tend to be so damaging to an organization or agency and why rogue employees sometimes get away with their violations for years.

He says part of the problem with malicious insiders is that no one wants to believe the worst.

> "We found that companies err on the side of goodness. They don't want to accuse somebody without full evidence of a crime, so they write it off as negligence," Ponemon tells SecureWorld.
>
> "And we discovered insider threats are not viewed as seriously as external threats, like a cyber attack. But when companies had an insider threat, in general, they were much more costly than external incidents. This was largely because the insider that is smart has the skills to hide the crime, for months, for years, sometimes forever."

In this most recent case of the FBI insider threat, it took 12 years for the Bureau to uncover what was happening and put a stop to it.

> "As an intelligence analyst for the FBI, the defendant was entrusted with access to sensitive government materials," said Assistant Attorney General John C. Demers for the Justice Department's National Security Division. "Kingsbury is alleged to have violated our nation's trust by stealing and retaining classified documents in her home for years. Insider threats are a significant danger to our national security, and we will continue to work relentlessly to identify, pursue and prosecute individuals who pose such a threat."

But saying you will stop an insider threat and actually doing it are two entirely different thing—especially if a rogue employee knows what they are doing is wrong.

classified materials and transportation and storage of those materials in unauthorized locations risked disclosure and transmission of those materials, and therefore could endanger the national security of the United States and the safety of its citizens. She also knew that violating the rules governing the handling of classified information could result in criminal prosecution."

Insider threat detection strategy for organizations

If you are working on an insider threat detection strategy or want to benchmark your current program, register now for the SecureWorld Remote Session, Mitigate Insider Risk in Financial Firms, which is available live and on-demand.

The webcast will feature SecureWorld, FINRA, and Proofpoint experts for a panel discussion about insider-led breaches at financial services organizations and will tackle these topics:

- The main insider threat profiles and how to address each
- Why insider threats are unique and require more context than other threats
- How to reduce response time and costs by speeding up investigation

Tags: Insider Threats, Encryption / DLP

Comments

First Name*

Last Name

Submit Comment

U.S. Department of Justice

Federal Bureau of Investigation
Washington, D.C. 20535

April 17, 2018

MR. WILLIAM FERNANDES
MUCKROCK
DEPT MR 38820
411A HIGHLAND AVENUE
SOMERVILLE, MA 02144-2516

FOIPA Request No.: 1378216-000
Subject: OPR Abstract of Disciplinary Action Against Massachusetts Employees
(2015-2016)

Dear Mr. Fernandes:

The enclosed documents were reviewed under the Freedom of Information Act (FOIA), Title 5, United States Code, Section 552. Below you will find check boxes under the appropriate statute headings which indicate the types of exemptions asserted to protect information which is exempt from disclosure. The appropriate exemptions are noted on the enclosed pages next to redacted information. In addition, a deleted page information sheet was inserted to indicate where pages were withheld entirely and identify which exemptions were applied. The checked exemptions boxes used to withhold information are further explained in the enclosed Explanation of Exemptions.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☑ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☑ (b)(6)		☐ (k)(7)

2 pages were reviewed and 2 pages are being released.

Below you will also find additional informational paragraphs about your request. Where applicable, check boxes are used to provide you with more information about the processing of your request. Please read each item carefully.

☐ Document(s) were located which originated with, or contained information concerning, other Government Agency (ies) [OGA].

☐ This information has been referred to the OGA(s) for review and direct response to you.
☐ We are consulting with another agency. The FBI will correspond with you regarding this information when the consultation is completed.

☐ In accordance with standard FBI practice and pursuant to FOIA exemption (b)(7)(E) and Privacy Act exemption (j)(2) [5 U.S.C. § 552/552a (b)(7)(E)/(j)(2)], this response neither confirms nor denies the existence of your subject's name on any watch lists.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the Freedom of Information Act (FOIA). See 5 U.S.C. § 552(c) (2006 & Supp. IV (2010). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist. Enclosed for your information is a copy of the Explanation of Exemptions.

For questions regarding our determinations, visit the www.fbi.gov/foia website under "Contact Us." The FOIPA Request Number listed above has been assigned to your request. Please use this number in all correspondence concerning your request.

You may file an appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, Suite 11050, 1425 New York Avenue, NW, Washington, D.C. 20530-0001, or you may submit an appeal through OIP's FOIAonline portal by creating an account on the following website: https://foiaonline.regulations.gov/foia/action/public/home. Your appeal must be postmarked or electronically transmitted within ninety (90) days from the date of this letter in order to be considered timely. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal." Please cite the FOIPA Request Number assigned to your request so it may be easily identified.

You may seek dispute resolution services by contacting the Office of Government Information Services (OGIS) at 877-684-6448, or by emailing ogis@nara.gov. Alternatively, you may contact the FBI's FOIA Public Liaison by emailing foipaquestions@fbi.gov. If you submit your dispute resolution correspondence by email, the subject heading should clearly state "Dispute Resolution Services." Please also cite the FOIPA Request Number assigned to your request so it may be easily identified.

☐ The enclosed material is from the main investigative file(s), meaning the subject(s) of your request was the focus of the investigation. Our search located additional references, in files relating to other individuals, or matters, which may or may not be about your subject(s). Our experience has shown such additional references, if identified to the same subject of the main investigative file, usually contain information similar to the information processed in the main file(s). As such, we have given priority to processing only the main investigative file(s) given our significant backlog. If you would like to receive any references to the subject(s) of your request, please submit a separate request for the reference material in writing. The references will be reviewed at a later date, as time and resources permit.

☑ See additional information which follows.

Sincerely,

David M. Hardy
Section Chief
Record/Information
Dissemination Section
Records Management Division

The enclosed documents represent the final release of information responsive to your Freedom of Information Act (FOIA) request. This material is being provided to you at no charge.

Enclosure(s)

EXPLANATION OF EXEMPTIONS

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

(b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;

(b)(2) related solely to the internal personnel rules and practices of an agency;

(b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

(b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(b)(9) geological and geophysical information and data, including maps, concerning wells.

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

(d)(5) information compiled in reasonable anticipation of a civil action proceeding;

(j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;

(k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;

(k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;

(k)(4) required by statute to be maintained and used solely as statistical records;

(k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service he release of which would compromise the testing or examination process;

(k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

FBI/DOJ

PRECEDENT REPORT

LIMITED TO:

To maintain the anonymity of the person(s) involved, the term "he" is being used to refer to both genders.

1 **OPR# 2014-0237, APU# 2015-0066** **Closed:** 7/31/2015 **References:** 2.6, 3.5, 3.6, 5.20, 5.22

b6
b7C

(5.22);
(5.20);
(3.6);
(3.5);
(2.6)

b6
b7C

5.22,
5.20,
3.5,
3.6,
5.22 –
5.20
3.5 – 5
3.6 –
2.6 –

MITIGATION:

AGGRAVATION:

FINAL ACTION(S): OPR PROPOSED DECISION Proposed DISMISSAL
OPR FINAL DECISION: DISMISSAL
DRB: AFFIRMED

2 **OPR# 2015-0016** **Closed:** 3/6/2015 **References:** 3.10, 3.9, 5.7

b6
b7C

(3.10);
(3.9);
(5.7).

MITIGATION:

AGGRAVATION:

FINAL ACTION(S): OPR PROPOSED DECISION Proposed 50 CALENDAR DAYS SUSPENSION WITHOUT PAY
OPR FINAL DECISION: 50 CALENDAR DAYS SUSPENSION WITHOUT PAY

LIMITED TO:

To maintain the anonymity of the person(s) involved, the term "he" is being used to refer to both genders.

3 **OPR# 2015-0185** **Closed:** 8/28/2015 **References:** 3.3

[redacted] (3.3). b6 b7C

MITIGATION: [redacted]

AGGRAVATION:

FINAL ACTION(S): OPR FINAL DECISION: 1 CALENDAR DAYS SUSPENSION WITHOUT PAY

4 **OPR# 2016-0124** **Closed:** 9/7/2016 **References:** 5.21

[redacted] in violation of (5.21 - Unprofessional Conduct - Off Duty).

AGGRAVATION: [redacted]

FINAL ACTION(S): OPR FINAL DECISION: 7 CALENDAR DAYS SUSPENSION WITHOUT PAY b6 b7C