



governmentattic.org

"Rummaging in the government's attic"

Description of document: Treasury Office of Inspector General (OIG) Management Implication Reports (MIR) 2016-2020 and List of MIRs 2017-2019

Requested date: 24-February-2020

Release date: 16-March-2020

Posted date: 25-May-2020

Source of document: FOIA Request
FOIA and Transparency
Department of the Treasury
Office of the Inspector General
Washington, DC 20220
Fax: 202-622-3895
[Online FOIA Request Form](#)

The governmentattic.org web site ("the site") is a First Amendment free speech web site, and is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.

From: Delmar, Richard K. <DelmarR@oig.treas.gov>
Sent: Fri, Mar 27, 2020 10:09 am
Subject: RE: FOIA - Treasury OIG - "management advisories"
Here they are with Exemption 7C redactions.

This production with redactions constitutes an adverse action under the FOIA. Accordingly, you have the right to appeal this determination within 90 days from the date of this letter. By filing an appeal, you preserve your rights under FOIA and give the agency a chance to review and reconsider your request and the agency's decision. Your appeal must be in writing, be signed by you or your representative, and contain the rationale for your appeal. Please address your appeal to:

FOIA Appeal
FOIA and Transparency
Privacy, Transparency, and Records
Department of the Treasury
1500 Pennsylvania Ave., N.W.
Washington, D.C. 20220

If you would like to discuss this response before filing an appeal to attempt to resolve your dispute without going through the appeals process, you may contact the Treasury DO FOIA Public Liaison at (202) 622-8098 or email FOIAPL@treasury.gov.

If you are unable to resolve your FOIA dispute through our FOIA Public Liaison, the Office of Government Information Services (OGIS) also mediates disputes between FOIA requesters and federal agencies as a non-exclusive alternative to litigation. If you wish to contact OGIS, you may write directly to:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Road – OGIS
College Park, MD 20740-6001
ogis@nara.gov
ogis.archives.gov
(202) 741-5770
(877) 684-6448

Please call me if you have questions.

Rich Delmar
Deputy Inspector General
Department of the Treasury
202-927-3973



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



Management Implication Report

Date of Report: OCT 25 2016

Prepared by:

Associated Case #: BEP-16-0101-I

Investigator

Approved by:

Anthony J. Scott
Special Agent in Charge

Background

The Bureau of Engraving and Printing (BEP) is a government agency within the United States Department of the Treasury that designs and produces a variety of security products for the United States government, most notable of which is Federal Reserve Notes (paper money) for the Federal Reserve Bank (FRB), the nation's central bank. In addition to paper currency, the BEP produces Treasury securities; military commissions and award certificates; invitations and admission cards; and many different types of identification cards, forms, and other special security documents for a variety of government agencies. With production facilities in Washington, DC, and Fort Worth, Texas, the BEP is the largest producer of government security documents in the United States.

In 2014, BEP created a validation plan to evaluate the performance of the Series 2009 \$100 Recovery Process under actual conditions prior to beginning full production. The validation was prepared to confirm the proper function of the Series 2009 \$100 Recovery Process ("Recovery Process") under normal operating conditions. As compared to Series 2009a \$100 Single Note Inspection (SNI) process, the Recovery Process required that:

- 1) Serial numbers of every note in a bundle and in a Cash-Pack was recorded and searchable.
- 2) Additional scrutiny, beyond the scope of the existing Office of Quality (OQ) NXG\$100 SNI Audit Program, was provided to monitor the level of creasing that was present in the "Fit" work coming off of SNI.
- 3) Packaging of Fit product is more consistent with packaging of BEP "New" product.

Verifications were performed to ensure the new equipment, materials, and data structures could perform as designed. The intent of this Validation was to confirm proper function of the overall

This Report is the property of the Office of Investigation, Treasury Office of the Inspector General. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordance with 5 U.S.C. § 552. This report is FOR OFFICIAL USE ONLY and its disclosure to unauthorized persons is prohibited.

system, including SNI and Note Packaging areas, under normal operating conditions and ensure there are no unintended consequences that negatively impact the requirements.

The adaptation that was used at the start of validation was "Adaptation Y", which was approved by BEP, FRB, and United States Secret Service on April 16, 2015 based on a live demonstration of its ability to detect various levels of creasing.

The primary goal of the SNI portion of the Validation was to validate the operation of the Optical Banknote Inspection System (OBIS) and the various procedures associated with the Recovery Process, especially barcode labeling of bundles and use of the Single Note Crease Detection System (SN-CDS). The team would accomplish these goals by running one full Process.

On October 15, 2015, The U.S. Department of Treasury, Office of Inspector General, Office of Investigations (TOIG), received a complaint from a Confidential Source (CS) of information alleging that BEP employees in the Ft. Worth, TX Western Currency Facility (WCF) conducted illegal strip searches of BEP employees in the SNI area after \$100 super notes were discovered missing.

The investigation revealed that there were two occurrences of missing notes in the SNI area. The first incident was in May 2015 when eleven \$100 super notes were discovered missing after the daily count. Per BEP protocol the Office of Security and the Security Manager along with BEP Police responded. The second incident occurred in July 2015, when it was discovered another eight \$100 super note bills were discovered missing at the day end count. Again the Office of Security and the Security Manager along with BEP Police responded.

The investigation determined that no BEP employees were stripped searched and BEP employees followed the procedures that are currently in place, however, the policies currently in place were implemented prior to the creation of the SNI process and need revision to include the SNI process and training of BEP Security Personnel. BEP, WCF has signs clearly posted outside of the WCF front entry point and prior to entering the magnetometers in the entry way of the building that all personnel are subject to search upon entering the WCF.

In addition, the investigation revealed training and procedural weaknesses that, if addressed, would likely improve the search procedures within the SNI area. With that goal in mind, this Management Implication Report (MIR) is submitted to BEP in an effort to identify and address these potential weaknesses.

Findings

TOIG interviewed several employees within the SNI area, to include BEP Police Officers. All interviewed stated that none of the employees had been briefed on what their rights are regarding being searched, however, all SNI employees signed consent to search forms, but some SNI employees felt pressure to comply with the request. BEP Police Officers who were interviewed all admitted that they have received no training regarding how to conduct administrative searches of employees when currency is discovered missing.

This Report is the property of the Office of Investigation, Treasury Office of the Inspector General. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordance with 5 U.S.C. § 552. This report is FOR OFFICIAL USE ONLY and its disclosure to unauthorized persons is prohibited.

BEP should consider implementing the following recommendations:

Finding #1- All BEP employees should receive training regarding their rights to be searched upon entering the facility as well as when a Missing Product Incident occurs. BEP Police should also be trained how to conduct these type of non-custodial searches.

Basis of Finding –

TOIG interviewed all SNI employees involved in the two separate Missing product Incidents and all were unaware of what their rights are regarding being searched within the facility. The BEP Police who responded to both of these incidents have not received any training regarding how to conduct Administrative searches relating to Missing Product Investigations.

Recommendation –

BEP should conduct training for all personnel as to their rights regarding a search of their person, lockers and vehicles on BEP property, as well as BEP Police Officers receiving training on how to conduct searches of personnel that are not in custody.

Finding #2 – BEP SNI Supervisors should conduct searches of the SNI machines prior to implementing a search of SNI employees and contacting the Office of Security et al.

Basis of Finding –

The investigation found that on the two separate Missing Product Incidents which occurred in May 2015 and July 2015, all of the Missing Product \$100 notes were recovered inside of the SNI machinery during the July 2015 incident.

Recommendation –

BEP SNI Supervisors should dismantle parts of the SNI machines in order to visually inspect inside the machines for live currency, prior to notifying the Office of Security, Security Manager and BEP Police personnel.

Finding #3 – BEP Police should conduct searches inside of the SNI area, thus preventing any SNI employee from being paraded out into the hallway in front of other BEP employees to be searched.

Basis of Finding –

BEP Police officers escorted employees out of the SNI area into the restroom in front of other BEP employees in the WCF and then numerous employees were ordered to remove their clothing in front of each other inside of the men's restroom which caused them embarrassment.

Recommendation –

BEP Police should purchase a portable changing area that can be erected inside of the SNI area, thus preventing an SNI employee from being paraded out of the area by BEP Police to the restroom/locker-room area to be searched. Each employee should be searched individually and not be made to disrobe in front of other co-workers.

Signatures

Case Agent: [REDACTED], Investigator

[REDACTED]
Signature

10/13/16
Date

Supervisor: Anthony J. Scott, Special Agent in Charge

[REDACTED]
Signature

10/24/16
Date



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



Management Implication Report

Date of Report: NOV 20 2017

Prepared by:

Special Agent

Associated Case #: BEP-16-1449-I

Approved by:

Jerry S. Marshall
Deputy Assistant Inspector
General for Investigations

Background

The Bureau of Engraving and Printing (BEP) is a government agency within the United States Department of the Treasury that designs and produces a variety of security products for the United States government, most notable of which is Federal Reserve Notes (paper money) for the Federal Reserve Bank (FRB), the nation's central bank. In addition to paper currency, the BEP produces Treasury securities; military commissions and award certificates; invitations and admission cards; and many different types of identification cards, forms, and other special security documents for a variety of government agencies. With production facilities in Washington, DC, and Fort Worth, Texas, the BEP is the largest producer of government security documents in the United States. The Office of Compliance (OC) evaluates and monitors internal control systems and maintains a comprehensive product accountability system.

In March 2015, the Board of Governors of the Federal Reserve System, Cash Advisory Group, endorsed the implementation of a revised Counterfeit Certification Program. As a result, there was no longer a need for the Counterfeit Program Administrators to retain the Treasury issued counterfeit test decks. These test decks were once used to certify FRB staff in detecting counterfeit money.

In March 2016, instructions for how to return the Treasury issued counterfeit test decks were distributed to the Counterfeit Program Administrators. The instructions requested that the counterfeit test decks be returned to the OC in accordance with the Treasury Currency Operations Manual (TCOM) Chapter 4030.40#6. This section of the manual states:

"To return test decks to the OC management must advise by email when they will be returning the test decks so they can be tracked, then enclose a copy of the inventory of each returned test deck and send them....FedEx next day with tracking to: BEP/Office of Compliance 301 14th St SW, Room 321-14A, Washington DC 20228."

This Report is the property of the Office of Investigation, Treasury Office of the Inspector General. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordance with 5 U.S.C. § 552. This report is FOR OFFICIAL USE ONLY and its disclosure to unauthorized persons is prohibited.

On October 31, 2016, The U.S. Department of Treasury, Office of Inspector General, Office of Investigations (TOIG), initiated an investigation regarding the allegation that a package containing counterfeit test decks arrived empty at the BEP.

The investigation revealed that FedEx package (tracking number 775954466187) was delivered to the BEP loading dock empty of its contents.

The investigation determined that no BEP OC employees disclosed to TOIG that they were aware of the March 21, 2016 instructions put forth by the Board of Governors of the Federal Reserve System, Cash Advisory Group. No BEP OC employee revealed that they were aware of TCOM Chapter 4030.40 as a possible reason for the package delivery and respective contents.

Findings

TOIG interviewed several employees within the BEP OC area, to include a senior supervisor. One interviewee stated that although a notification is sent containing an inventory of what the package should contain, the package could contain more or less than what the manifest reflects. Therefore, there is no confirmed way to determine the actual contents of the package. No employee was able to provide TOIG with the confirmed inventory of what was missing from FedEx package (tracking number 775954466187).

BEP should consider implementing the following recommendations:

Finding #1- All BEP OC employees should receive training regarding the delivery and tracking procedures for counterfeit, test decks, and old style notes as referenced in the TCOM.

Basis of Finding –

TOIG interviewed BEP OC employees involved in the delivery of FedEx package (tracking number 775954466187). These employees did not reveal to TOIG that they were aware of the specific counterfeit test decks that were being delivered in accordance with the March 21, 2016 instructions put forth by the Board of Governors of the Federal Reserve System, Cash Advisory Group.

TOIG reviewed TCOM Chapter 4030.40#6. This section of the manual states:

“To return test decks to the OC or CTO (as applicable), management must advise by email when they will be returning the test decks so they can be tracked, then enclose a copy of the inventory of each returned test deck and send them via U.S. Postal Service registered mail - return receipt requested, USPS Next Day with return receipt, UPS next day with tracking, or FedEx next day with tracking to:

BEP/Office of Compliance 301 14th St SW, Room 321-14A, Washington DC 20228.”

BEP OC employees did not provide an inventory of each returned test deck per the aforementioned instructions.

Recommendation –

Due to the lack of adherence to the Treasury Currency Operations Manual (TCOM) Chapter 4030.40#6 manual, the actual contents of the FedEx package (tracking number 775954466187) cannot be confirmed. BEP OC employees should receive training regarding the delivery procedures for counterfeit test decks and old style notes as referenced in the TCOM. Subsequent to that training, BEP OC employees should adhere to the TCOM instructions.

If the interpretation of TCOM Manual Chapter 4030.40#6 dictates that the inventory of the package is ONLY sent with the package and is not required as a separate mailing/email, the TCOM Manual Chapter 4030.40#6 should be updated to state that a copy of the inventory of each returned test deck mailing should be enclosed in the package AND sent via separate mail/email to the BEP OC.

Signatures

Case Agent: [REDACTED], Special Agent

[REDACTED]
Signature

10/26/2017
Date

Supervisor: Jerry S. Marshall, Deputy Assistant Inspector General for Investigations

[REDACTED]
Signature

17 NOV 2017
Date



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



Management Implication Report

Date of Report: March 24, 2020

Prepared by: [REDACTED]
Special Agent

Associated Case: BEP-17-0824-I

Approved by: Anthony J. Scott
Special Agent in Charge

Background

The Department of the Treasury, Office of Inspector General, Office of Investigations (TIG), received a referral from the Bureau of Engraving and Printing (BEP) alleging that BEP Police Officer [REDACTED] is committing fraud related to the Federal Employee Health Benefits (FEHB) program.

Findings

Finding #1 – TIG investigations determined that neither the BEP, nor the Department of the Treasury (Treasury), require verification documentation to substantiate a common law marriage when an employee elects a common law spouse and/or dependents to Federal Employee Health Benefits. The BEP and Treasury should consider implementing the following recommendations.

Basis of Finding – TIG investigations found that the BEP does not require documentary evidence of a common law marriage before processing employee benefit forms, allowing unauthorized personnel to be included on an employee's health plan.

Potential Impact – Requiring verification documentation of a common law marriage would prevent Treasury employees from adding unauthorized individuals to the FEHB program.

Recommendation

The BEP and Treasury should consider requiring employees to provide documentation substantiating the existence of a common law marriage when electing a common law spouse and/or dependents to receive employee health benefits. This documentation should be included with the FEHB election form (SF 2809).

The employee may substantiate a common law marriage and associated dependents by including any two (2) of the following documents when submitting a SF 2809:

- A personal affidavit stating when and where the employee and common law spouse mutually agreed to become husband and wife; whether they were ever married, ceremonially or otherwise,

This Report is the property of the Office of Investigations, Treasury Office of Inspector General. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordance with 5 U.S.C. § 552. This report is FOR OFFICIAL USE ONLY and its disclosure to unauthorized persons is prohibited.

to anyone else, and the details surrounding the end of any previous marriages (how they were ended, where, and when); and any other details that will help to establish the existence of a husband and wife relationship.

- Affidavits from other persons who know the employee and are familiar with their relationship, setting forth particulars such as the length of time they lived together; their address(es); whether there was any public announcement of their marriage; and whether their friends, neighbors, and relatives regard you as married.
- Deeds showing title to property held jointly by both parties to the common law marriage.
- Bank statements and checks showing joint ownership of the accounts.
- Insurance policies naming the other party as beneficiary.
- Birth certificates naming the employee and their common law spouse as parents of their child(ren).
- Employment records listing the common law spouse as an immediate family member.
- School records listing the names of both common law spouses as parents.
- Credit card accounts in the names of both common law spouses.
- Loan documents, mortgages, and promissory notes evidencing joint financial obligations of the parties.
- Any documents showing that the wife has assumed the surname of her common law husband.
- Church records indicating familial status, including membership information, baptismal certificates of the parties' child(ren), Sunday School registration forms, etc.

Signatures

Case Agent:

████████████████████

Date: 03/24/20

Supervisor:

Anthony J. Scott /s/

Date: 03/24/20



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



Management Implication Report

Date of Report: 7 OCT 2016

Prepared by: [REDACTED]
Special Agent

Associated Case #: BFS-16-1433-I

Approved by: Jerry Marshall
Deputy Assistant Inspector
General

Background

An investigation was initiated by the Department of the Treasury, Office of Inspector General, Office of Investigations (TOIG), after the Bureau of the Fiscal Service (BFS) reported that a BFS computer had made an unusually large number of outbound communication attempts to Internet Protocol (IP) addresses associated with Amazon Web Services (AWS).

TOIG's investigation substantiated the report and confirmed that the root cause of the unusually large number of outbound communication attempts was caused by a program installed by [REDACTED], an Application Development contractor with [REDACTED] who supports the BFS Integrated Document Management System (IDMS). The program installed by [REDACTED] (ruxit) was not approved by BFS for installation.

Findings

Finding #1 **Developers had local administrator rights on their BFS-issued computers**

Basis of Finding: This finding was confirmed via interviews with BFS Technical Lead [REDACTED], BFS IT Security Analyst [REDACTED], BFS contract software developer [REDACTED], and the digital forensic investigation of [REDACTED]'s BFS-issued computer.

Potential Impact: The wide scale issuance of local administrator rights contradicts the SANS 20 Critical Security Controls guidance on the "Controlled Use of Administrative Privileges." Local administrative rights allows users to install any software, circumvent monitoring and logging, access network traffic and use their computers for nearly any purpose without management's awareness or approval. This represents a threat to the confidentiality, integrity and availability of BFS information.

Recommendation: BFS should carefully weigh the risks of allowing local administrator access with the benefits of improved productivity and reduce software developer computer rights as appropriate.

Finding #2 Unauthorized software was installed on BFS-issued computers

Basis of Finding: The "ruxit" computer and network monitoring program was located on [REDACTED]'s BFS-issued computer during TOIG's digital forensic exam. A review of the BFS Approved Software list showed that the "ruxit" program was not on the list.

Potential Impact: The installation of unapproved software creates a significant vulnerability to an organization and contradicts the SANS 20 Critical Security Controls guidance on "Inventory of Authorized and Unauthorized Software." Unauthorized software can contain malware or cause unforeseen interoperability problems in computers and networks.

Recommendations: TOIG's investigation suggests that there may be a lack of employee awareness regarding how to locate the Approved Software List, therefore it is recommended that BFS initiate a process to improve employee awareness of the lists location and the approval process for software not on the list. The list could also benefit from a review to purge obsolete and unused software and to update it for new software.

Finding #3 Developer computers are not isolated from the BFS production network

Basis of Finding: Interviews with BFS Technical Lead [REDACTED] (b) (7)(C) and BFS IT Security Analyst.

Potential Impact: The software development process may call for the installation of software not on the Approved Software List, in order to test the software's applicability and functionality. In addition, by the nature of their jobs, software developers will be creating and testing applications that are unstable and/or unreliable. These in-development applications can and will cause problems with computers, networks and servers. That is the nature of software development. If the development process occurs on a production network those problems will affect mission accomplishment.

Recommendation: Create a subnet of the BFS network for software developers to utilize that is segmented from the BFS production network via a firewall. This will allow software developers the necessary freedom to efficiently create applications while protecting operational BFS network infrastructure and information.

Signatures

Case Agent: Agent [REDACTED] (b)
Special Agent (7)

[REDACTED]

Signature

7/18/16
Date

Supervisor: Jerry Marshall
Deputy Assistant Inspector General

[REDACTED]

Signature

26 AUG 2016
Date



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



Management Implication Report

Date of Report: FEB 06 2017

Prepared by: [REDACTED]
Special Agent

Associated Case #: BFS-16-2033-I

Approved by: Anthony J. Scott
Special Agent in Charge

Background

An investigation was initiated by the Department of the Treasury, Office of Inspector General, Office of Investigations (TOIG), after the Bureau of the Fiscal Service (BFS) reported personnel security incidents at the Federal Reserve Bank (FRB) of New York (FRB-NY) and the Federal Reserve Bank of Dallas (FRB-Dallas). Each incident involved a non-U.S. citizen FRB employee working on a Treasury project whose personnel security requirements mandated that only U.S. citizens work on them. TOIG's investigation confirmed that the incidents were the result of errors by the FRB and that no Treasury information or programs were compromised.

Finding

FRB fails to diligently adhere to Treasury security policies

Basis of Finding: As the fiscal agent for the Department of the Treasury, the FRB is obligated to adhere to and follow Treasury security policies when performing work on Treasury projects. Two separate personnel security incidents at two FRBs, each involving a failure to adhere or enforce relevant Treasury security policies is indicative of a *laissez-faire* attitude toward compliance with Treasury policies.

Potential Impact: The compromise of Treasury information and operations, especially the programs that involve the FRB, such as the debt auctions, cash management, and payments is nearly incalculable. Treasury risk and threat models are designed with that impact in mind, therefore, by failing to diligently apply the policies that implement those models, the FRB is potentially increasing the level of risk to dangerous levels.


Recommendation: BFS should implement an aggressive program to inspect and audit the compliance with all Treasury policies of all FRBs that perform work for the Treasury under the


This Report is the property of the Office of Investigation, Treasury Office of the Inspector General. Its contents may not be reproduced without written permission in accordance with 5 U.S.C. § 552. This report is FOR OFFICIAL USE ONLY and its disclosure to unauthorized persons is prohibited.

fiscal agent relationship. If the FRBs perform this inspection and audit themselves, BFS, or an organization they select should spot check and verify the findings.

Signatures


Case Agent:




Special Agent

1/11/17
Date

Supervisor:



Anthony J. Scott
Special Agent in Charge

1/30/17
Date



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



Management Implication Report

Date of Report: 06/29/17

Prepared by: [REDACTED]
Special Agent

Associated Case #: BFS-17-0817-I

Approved by: Anthony J. Scott
Special Agent in Charge

Background

An investigation was initiated by the Department of the Treasury, Office of Inspector General, Office of Investigations (TOIG), after the Bureau of the Fiscal Service (BFS) reported that an employee had been conducting Internet queries using search terms suggestive of attempts to view images of young males or child pornography using his BFS-issued mobile phone. The BFS recently issued Samsung Galaxy S7 smart phones running the Android 6.01 operating system to its employees. BFS is utilizing Samsung Knox, an extremely secure (FIPS 140-2, etc.) container-based solution that provides communication and collaboration tools to protect government information. The Knox container is encrypted and the Knox software performs numerous security checks to ensure that the Samsung phone it is installed on has not been compromised. If the Knox software detects an attempt to compromise the phone's operating system it deletes the Knox container. In addition, the Knox software suite enforces security settings on the phone that prevent access to the phone via its USB port. The BFS is using the Blackberry Enterprise Server (BES) as their Mobile Device Management (MDM) solution.

Finding

The current BFS Samsung Knox implementation inhibits investigations

Basis of Finding: In the course of the investigation referenced above, TOIG encountered a BFS-issued Samsung Galaxy S7. The use of a non-native MDM limited the amount of logging data for BFS IT Security to analyze, which delayed the identification of the employee performing the searches and reduced the certainty of that identification. Once the user was identified and through coordination with BFS, TOIG was able to secure the phone and have the account unlocked without triggering any Knox security countermeasures. TOIG then attempted to obtain a forensic image of the phone using Cellebrite UFED4PC, an industry leader in mobile device forensics. However, even with the phone unlocked and the assistance of the BFS Knox administrator, Cellebrite failed to acquire an image of the phone. The BFS Knox administrator

This Report is the property of the Office of Investigation, Treasury Office of the Inspector General. Its contents may not be reproduced without written permission in accordance with 5 U.S.C. § 552. This report is FOR OFFICIAL USE ONLY and its disclosure to unauthorized persons is prohibited.

was concerned that the BES MDM did not offer the full suite of management and configuration options. BFS contacted Samsung tech support but was unable to obtain a solution. TOIG contacted the Federal Bureau of Investigation (FBI) which deploys Knox on their issued mobile phones to inquire how they obtained data from their phones during internal investigations. The FBI informed TOIG that they did not possess a technique to circumvent Knox, rather FBI policy was that users Knox containers were backed up to FBI servers and that if data was needed it was obtained from the most recent backup.

Potential Impact: The utilization of a third party MDM creates a significant inefficiency in the management of BFS-issued mobile phones secured by Knox. Not capturing all potential logging information requires manual workarounds and is personnel dependent, i.e. if the BFS IT Security engineer who understands the work flow is not available then the identification of mobile device users can be delayed which will impact time sensitive investigations. In addition, if the BFS Knox administrator does not have access to the entire suite of management tools then the ability to respond to investigative requests or incidents may be negatively impacted.

The prevention of forensic image acquisition is an unavoidable feature of a strong security system. That feature however, can negatively impact the collection of evidence in criminal and administrative investigations.

Recommendations:

1. BFS should identify and migrate to more effective MDM for Samsung Knox.
2. BFS should implement a remote backup solution that captures the communications (text messages, email, etc.), Internet usage, images, and files created or stored on BFS-issued mobile phones. This solution should backup this data as frequently as technically and economically feasible, daily if possible, but not less frequently than weekly.

Signatures

Case Agent:

[REDACTED]
Special Agent

[REDACTED]
Signature

6/29/17
Date

Supervisor:

Anthony J. Scott
Special Agent in Charge

[REDACTED]
Signature

6/29/17
Date



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



Management Implication Report

Date of Report: June 14, 2018

Approved by: Anthony Scott
Special Agent in Charge (SAC)

Associated Case #: DO-18-0034-P

Prepared by: [REDACTED]
Assistant to the Special Agent in Charge

Background

The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 established the Office of Financial Research (OFR) to support the Financial Stability Oversight Council, the Council's member organizations, and the public by delivering high-quality financial data, standards and analysis. The OFR accomplishes this mission by looking holistically across the financial system to measure and analyze risks, perform essential research, and collect and standardize financial data.

In February 2018, OFR notified the Treasury Office of Inspector General (TIG) that two videos on the video uploading website YouTube, contained threats directed at OFR personnel and property in Washington, DC. OFR also filed a police report with the Federal Protective Service (FPS) with the same allegations. OFR did not provide copies of the videos in the course of their reporting to TIG or FPS.

The videos in question had been removed from YouTube prior to TIG's opening of an investigation to determine the identity of the subscriber who posted them. YouTube objected to the administrative subpoena used to compel the production of the identity of the YouTube subscriber. Upon commencement of litigation to determine if the subpoena would be enforced by the Department of Justice (DOJ), OFR notified TIG that their organization did, in fact, have copies of the aforementioned videos. The videos were supplied to TIG's Office of Investigations and TIG's Office of Counsel (OC), which reviewed them and determined that they did not threaten physical violence.

The aforementioned investigation revealed a weakness that, if addressed, would likely improve the integrity of complaints coming from the OFR. With that goal in mind, this Management Implication Report (MIR) is submitted to remediate this shortcoming.

The TIG has been in contact with OFR management throughout the aforementioned investigation. It should be noted that OFR management has been receptive to the TIG, candid about their deficiencies, and open to implementing remedial measures.

This Report is the property of the Office of Investigation, Treasury Office of the Inspector General. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordance with 5 U.S.C. § 552. This report is FOR OFFICIAL USE ONLY and its disclosure to unauthorized persons is prohibited.

Finding - Submitting an incomplete complaint.***Basis of Finding –***

TIG determined that the submission of an incomplete complaint wasted government resources and prevented TIG and FPS from fully evaluating OFR's assertion that the videos were threatening and worthy of the allocation of investigative resources. This lack of information required TIG to serve an administrative subpoena on YouTube to identify the subscriber and view the videos. YouTube's objection to the subpoena then caused the DOJ to have to assign an Assistant United States Attorney to the matter, taking them away from the litigation they were pursuing.

Most critically, at the onset of litigation regarding the subpoena, OFR notified TIG that they did, in fact possess copies of the videos. OFR's withholding of the videos raises the question that they attempted to use federal law enforcement (TIG and FPS) in an attempt to identify and intimidate individuals exercising their First Amendment rights and/or identifying a Whistleblower.

Recommendation-

The OFR should submit all information and any and all supporting documentation and/or media to the TIG in a timely manner.

Potential Impact –

The lack of timely provision of the videos created an atmosphere of concern which led to the unnecessary utilization of federal law enforcement resources, DOJ litigators and raised the question of whether OFR attempted to use federal law enforcement in an attempt to identify and intimidate individuals exercising their First Amendment rights and/or a Whistleblower.

Signatures

Case Agent: [REDACTED] Assistant Special Agent in Charge

[REDACTED]
Signature

6/14/2018
Date

Supervisor: Anthony Scott, Special Agent in Charge

[REDACTED]
Signature

6/14/18
Date



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



Management Implication Report

Date of Report:

OCT 25 2019

Prepared by:

Special Agent

Associated Case #: DO-19-0057

Approved by:

Anthony Scott
Special Agent in Charge

Background

The U.S. Department of the Treasury (Treasury), Office of Inspector General, Office of Investigations (TIG), initiated an investigation in March 2019, to determine how and why digital evidence (Treasury issued computers) requested by TIG in a criminal investigation (DO-19-0025-1) came to be destroyed. The investigation determined that Office of the Chief Information Officer (OCIO) Supervisory IT Specialist [REDACTED] was responsible for providing the digital evidence to TIG and that [REDACTED] had been informed of the TIG records request approximately two weeks prior to the subject of the investigation being placed on administrative leave and escorted from Main Treasury. [REDACTED] took no action to secure the digital evidence for approximately three weeks, then called the Treasury Desk Side Support team and learned that the digital evidence had been transferred to the IT Asset Management team and wiped (erased by overwriting the internal storage).

The investigation was referred to the United States Attorney's Office for the District of Columbia (USAO-DC) which did not identify a criminal violation of 18 U.S.C. §1505 "Obstruction of proceedings before departments, agencies and committees."

Findings

The investigation did not identify a deliberate attempt by [REDACTED] to obstruct a TIG records request. However, [REDACTED]'s lack of responsiveness allowed the digital evidence to be destroyed which was effectively a violation of 31 Code of Federal Regulations (CFR) § 207, Treasury Order (TO) 114-01 and Treasury Directive (TD) 40-01. In addition, the behavior of contractors working for the OCIO in response to a TIG investigation suggests that a culture of compliance does not exist within OCIO with respect to cooperation with TIG investigations.

DO should consider implementing the following recommendations:

This Report is the property of the Office of Investigation, Treasury Office of the Inspector General. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordance with 5 U.S.C. § 552. This report is FOR OFFICIAL USE ONLY and its disclosure to unauthorized persons is prohibited.

Finding #1- DO lacks policies and implement procedures on how to systematically, discreetly and efficiently respond to and document TIG record requests.

Basis of Finding –

TIG interviewed government employees and contractors involved in fulfilling TIG record requests. No one could cite or was aware of an official policy on how to handle TIG record requests pertaining to Treasury Electronically Stored Information (ESI), computers and/or mobile devices. The interviews portrayed an environment where TIG record requests, even those pertaining to criminal investigations, were not addressed in a timely, systematic, professional fashion. In addition, no formalized, limited access, record request tracking system exists.

Recommendation –

DO should create a policy and procedures on how to how to systematically, discreetly and efficiently respond to and document TIG record requests. The policy and procedures should include but not be limited to:

1. Creating a formal chain of command responsible for fulfilling TIG record requests.
2. Creating a formalized work flow for fulfilling TIG record requests.
3. Ensuring that TIG record requests remain confidential.
4. Creating a tracking system to document the process of fulfilling TIG record requests
5. Defining the specific roles and responsibilities of the personnel responsible for fulfilling TIG record requests and including that as a performance metric for them.
6. Allowing only vetted and trained government employees to fulfill TIG record requests.
7. Providing TIG with the names and contact information of all DO personnel responsible for fulfilling TIG record requests.

Finding #2 – Office of the Chief Information Officer (OCIO) contractors are unaware of their duty to cooperate with TIG investigations.

Basis of Finding –


During TIG's investigation to determine how and why digital evidence requested in a criminal investigation came to be destroyed. The initial attempt to interview OCIO Desk Side Support team personnel was denied by lead contractor [REDACTED] who stated he had called [REDACTED] and that TIG would have to call [REDACTED] before [REDACTED] would speak to him. When informed that TIG did not have to ask permission to conduct interviews, [REDACTED] told the TIG Special Agent to leave his office and refused to identify his employer.


Recommendation –

OCIO should ensure that all contractors are aware of their responsibilities to cooperate with TIG, or any other investigation as a requirement of their contract. OCIO should implement a formal policy and procedures to remove contractors who fail to cooperate with TIG investigations.

Signatures

Case Agent:

 Special Agent

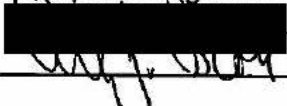


Signature

10/21/19
Date

Supervisor:

Anthony Scott, Special Agent in Charge



Signature

10/25/19
Date



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



Management Implication Report

Date of Report: OCT 24 2019

Prepared by: [REDACTED]
Special Agent

Associated Case #: DO-19-0058-I
DO-17-0376-I

Approved by: Anthony J. Scott
Special Agent in Charge

Background

The U.S. Department of the Treasury, Office of Financial Research (OFR) helps to promote financial stability by looking across the financial system to measure and analyze risks, perform essential research, and collect and standardize financial data. Recently, the U.S. Department of the Treasury, Office of Inspector General (TIG) investigated multiple incidents where OFR's Washington, D.C. office spaces were vandalized by an individual or group of individuals who placed obscene writing and obscene pictures throughout the office.

In December 2016, OFR reported to TIG that sometime between 7 pm on December 16, 2016, and approximately 8 am on December 19, 2016, numerous offices within OFR's office space were defaced. Phallic drawings were found on several windows on the 6th and 12th floors of the OFR office building.

The investigation determined that the allegation was substantiated. TIG reviewed access logs and identified a subject of interest who was responsible for the vandalism. TIG interviewed the subject and obtained a confession.

A separate vandalism incident occurred between November 2016 and December 2016. The words "Get Fired Already!!" were written on an OFR Employee's office door. TIG reviewed badge records for that time period, but was unable to identify a suspect.

In a separate investigation opened in July 2019, OFR reported to TIG the presence of obscene images located in office room 1007 on the 10th floor. The obscene images were discovered on June 5, 2019 and consisted of the phallic symbol made of push-pins attached to a cork board and the drawing on a whiteboard of a stick figure holding a firearm with a caption saying "I am Bob."

The investigation was unable to determine the responsible party. TIG reviewed access logs, interviewed potential witnesses, and submitted evidence for fingerprint analysis. TIG identified a subject of interest, however, the subject is no longer employed by the Department of the Treasury and refused an interview request from TIG.

This Report is the property of the Office of Investigation, Treasury Office of the Inspector General. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordance with 5 U.S.C. § 552. This report is FOR OFFICIAL USE ONLY and its disclosure to unauthorized persons is prohibited.

The aforementioned investigations revealed weaknesses that, if addressed, would likely improve the integrity and security of the office spaces OFR occupies. With that goal in mind, this Management Implication Report (MIR) is submitted to OFR management in an effort to identify and address these potential vulnerabilities and weaknesses.

Findings

During TIG's investigations, TIG was made aware and observed unassigned offices utilized as impromptu conference rooms and private areas where an employee who does not have an office may conduct personal or work related business in private. TIG also observed the office spaces within OFR do not have any type of video surveillance.

The OFR should consider implementing the following recommendations.

Finding #1- Individual unassigned offices within OFR are left unsecured with access not controlled.

Basis of Finding –

TIG found the individual unassigned offices within OFR's office space are left unlocked, allowing anyone to access the spaces for private use. These spaces are being utilized as impromptu conference rooms as well as a place a person could take a personal phone calls.

Potential Impact –

Allowing vacant offices to remain unlocked and permitting employees to utilize these spaces for their private use could reduce the accountability for that space. As mentioned in the investigations, this could lead to vandalism, theft, or unauthorized activity within OFR's office space.

Recommendation –

The OFR should assure that all vacant offices remain locked with controlling access to these spaces kept to the necessary personnel. These personnel should ensure unauthorized personnel are not accessing these spaces unless they have a legitimate purpose related to OFR business.

Finding #2 – OFR office spaces are not equipped with video surveillance.

Basis of Finding –

Including the investigations mentioned in this report, OFR has a history of reporting employee misconduct issues to TIG in which the evidence must rely on witness statements or circumstantial evidence. In many cases, there is no video evidence. In cases of vandalism, theft or threats against employees, OFR and TIG must rely on admission statements made by subjects.

Recommendation –

The OFR would benefit from an office video surveillance system. Video surveillance will assist with keeping employees and property safe. It can also provide proof of blatant disregards for safety measures among employees. In the event of an act of vandalism, theft or threat, a video surveillance system can provide evidence as to who was responsible.

Signatures

Case Agent: [REDACTED]

Signature [REDACTED]

Date

10/24/2019

Supervisor: Anth [REDACTED]

Signature [REDACTED]

Date

10/24/19



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



Management Implication Report

Date of Report:

NOV 21 2019

Prepared by:

Special Agent

Associated Case #: FinCEN-19-0052-I

Approved by:

Anthony J. Scott
Special Agent in Charge

Background

The Department of the Treasury, Office of Inspector General, Office of Investigations (TIG) opened an investigation into malfeasance by several Financial Crimes Enforcement Network (FinCEN) employees in May 2018 under suspicion of leaking classified material to media outlets. As a result of the investigation, four FinCEN employees [REDACTED], [REDACTED], [REDACTED], and [REDACTED] were placed on administrative leave, and escorted from FinCEN office space. When this occurred, their offices were secured by FinCEN security with their assigned government furnished computers locked within those spaces. In March 2019, TIG requested the hard drives from several of those computers. When this request was made it was discovered that the computers were removed from the secured offices, and transferred to the Technology Division (TD) where several of the hard drives were reprogrammed with the standard FinCEN computer configuration. This oversight resulted in overwriting the data that was preserved on those hard drives.

On April 2, 2019, TIG opened an investigation into allegations of evidence tampering by FinCEN Employees [REDACTED], [REDACTED], [REDACTED], [REDACTED]ng, [REDACTED], and [REDACTED]. Those employees were interviewed, and their emails reviewed in order to determine why the computers were removed from their secured offices, why two of the hard drives were reimaged by the TD, and why the equipment was placed in TD storage.

Findings

The investigation determined that there was no wrongdoing or malfeasance conducted by FinCEN employees when the computers were removed from secured offices, and two of the hard drives were reimaged. A TD employee approached [REDACTED] (b) (7)(C) and asked if he could take possession of the computer monitors from offices 2004, 2007, 2020, and 2032 which were assigned to the employees on administrative leave. [REDACTED] did not give clearance to

This Report is the property of the Office of Investigation, Treasury Office of the Inspector General. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordance with 5 U.S.C. § 552. This report is FOR OFFICIAL USE ONLY and its disclosure to unauthorized persons is prohibited.

remove those items, and opened a dialogue with FinCEN stakeholders in order to gain approval. During the course of the email chains, terminology morphed from the initial email which called the items "monitors", and then "equipment" which was not noticed by those on the email clearance chain. Once approval was received from FinCEN stakeholders to remove the monitors, the final email chain word "equipment" morphed into "Desk Tops and Monitors" which added confusion to the initial intent of the first email. As a result, this led to the computers and monitors being removed by TD and placed into their general storage area for future reassignment. Two of the computers had their hard drives removed and the latest FinCEN Windows image was installed. This was not discovered until TIG requested the hard drive from Mark Hanson's computer.

During the interviews, multiple employees referenced that there was no official FinCEN policy or procedure on how to handle, segregate, or secure government furnished computers, smart phones, tablets, or other equipment when an employee is placed on administrative leave. FinCEN made a good faith effort by locking the offices of the four employees, but through a sequence of events, the equipment was prematurely removed, and the integrity of any evidence on those hard drives was destroyed.

FinCEN should consider implementing the following recommendations:

Finding #1- FinCEN should create a policy and procedures on how to properly secure the assigned office spaces, computers, mobile devices, and other government furnished equipment when their employees are placed on administrative leave.

Basis of Finding –

TIG interviewed all of the employees involved with the access or removal of the computers from the secured office spaces. TIG did not find, and no employee could cite or was aware of an official policy on how to proceed with the office spaces, computers, mobile devices, or other government furnished equipment when an employee is placed on administrative leave. These employees made a good faith effort to secure the offices thereby denying access to the spaces and equipment. However, due to a series of events, this system failed and the computers were removed from the secured office space.

Recommendation –

FinCEN should create a policy and procedures on how to properly secure the assigned office spaces, computers, mobile devices, and other government furnished equipment when their employees are placed on administrative leave. This policy should ensure measures are taken so that only a small core group of employees have access to the spaces and equipment thereby mitigating the risk of a similar incident occurring again. The policies should explicitly state what actions to take with the employee's computers, phones, mobile devices, and office space and how to secure it to prevent tampering and avoid any confusion on the proper actions to take.

Finding #2 – FinCEN should identify a secure storage space, so that any electronic devices can be safely secured, cannot be tampered with, or reissued as if they were in the available TD inventory.

Basis of Finding –

The investigation found that the computers were secured in the locked offices assigned to the employees on administrative leave. Those offices were entered, the items taken by TD personnel, and were made ready for reissuance. Additionally, other devices such as government issued laptops, tablets, and phones were stored in boxes in the security office. It was apparent that no one location was identified or utilized for the storage of this equipment which allowed it to be tampered with and/or reissued.

Recommendation –

FinCEN should identify a location to secure all government furnished computers, phones, mobile devices, and other related equipment so that they cannot mistakenly be removed, reimaged or wiped, and placed back into the regular inventory for reassignment. This area should only be accessed by a small number of individuals identified by management to secure this equipment, and a log should be maintained that annotates when the room is accessed, by whom, and the reason why. Furthermore, FinCEN should require that all equipment is secured in a uniform manner, and that it be placed in evidence bags with anti-tamper seals. If the use of evidence is not possible due to physical limitations, FinCEN should place anti-tamper seals directly over any ports or other areas which would allow physical or electronic access into the device. If the seals are disturbed, it would show that the evidence was tampered with and any instances of this occurring must immediately be reported to the OIG.

Finding #3 – FinCEN should create a policy that clearly defines how and when equipment and office spaces assigned to employees on administrative leave can be properly cleared for issuance back to the employee, or refreshed for reassignment to the pool of available resources.

Basis of Finding –

FinCEN employees explained that because verbiage was slightly changed in several email chains, equipment that should have remained secured, was taken into possession by TD and placed in their storage for reassignment when needed. This equipment was removed prematurely, prior to the TIG investigation concluding and a hard drive containing evidence was reimaged. This occurred due to some oversight, and without the full knowledge of FinCEN management or security.

Recommendation –

When a FinCEN employee who was previously on administrative leave is terminated or returns to work, their devices should not be released from secure storage until the release is approved by the FinCEN Security Director, the Chief Information Officer, the Human Resources Director, and the General Counsel. This approval should also explicitly state the next steps to be taken and the final disposition of the equipment (whether it will be re-used, destroyed, or disposed).

Signatures

Case Agent: [REDACTED] Special Agent

Signature

Date

Supervisor: Anthony J. Scott, Special Agent in Charge

Signature

Date

This document is the property of the U.S. Department of the Treasury, Office of Inspector General, Office of Investigations. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordance with the law.

Number	Category	Upload Date
FinCEN-19-0052-I	Management Implication Report (MIR)	21Nov2019
DO-19-0057-I	Management Implication Report (MIR)	28Oct2019
DO-19-0058-I	Management Implication Report (MIR)	24Oct2019
BFS-16-1433-I	Management Implication Report (MIR)	23Oct2018
DO-18-0034-P	Management Implication Report (MIR)	18Jun2018
BEP-17-0824-I	Management Implication Report (MIR)	06Feb2018
BEP-16-1449-I	Management Implication Report (MIR)	20Nov2017
BFS-17-0817-I	Management Implication Report (MIR)	07Aug2017
OCC-16-2767-I	Management Implication Report (MIR)	15Mar2017
BFS-16-2033-I	Management Implication Report (MIR)	09Feb2017
BEP-16-0101-I	Management Implication Report (MIR)	27Jan2017

This document is the property of the U.S. Department of the Treasury, Office of Inspector General, Office of Investigations. It contains sensitive law enforcement information and its contents may not be reproduced without written permission in accordance with the law.