U.S. COMMODITY FUTURES TRADING COMMISSION
Office of Inspector General
Three Lafayette Centre
1155 21st Street, NW, Washington, DC 20581
Telephone: (202) 418-5110
Facsimile: (202) 418-5522

June 27, 2016

TO: Timothy G. Massad, Chairman
Commissioner Sharon Y. Bowen
Commissioner J. Christopher Giancarlo

FROM: A. Roy Lavik
Inspector General

SUBJECT: Investigation into a Potential Information Technology Security Incident

Attached is an investigation by my Office into a potential information technology security incident. The matter was referred by Management following the recommendation of the agency's Incident Response Team.

Please keep in mind this version of the report is confidential and unredacted, and let us know if you would like to discuss anything in the report.

Attachment: Investigation into a Potential Information Technology Security Incident

Cc (with attachment): Jonathan L. Marcus, General Counsel
John L. Rogers, Chief Information Officer
Anthony C. Thompson, Executive Director

Investigation into a Potential Information Technology Security Incident

Prepared by the
Office of the Inspector General
Commodity Futures Trading Commission

June 27, 2016

Table of Contents

BACKGROUND, SCOPE & METHODOLOGY

On June 4, 2015, the Commodity Futures Trading Commission's ("CFTC") Office of the Inspector General ("OIG") received a letter from the CFTC's General Counsel, Chief Information Officer, and Executive Director,[1] requesting investigation into a computer security incident. Attached was a report ("IRT report")[2] from the CFTC's Incident Response Team ("IRT").[3]

The IRT's investigation of the incident had uncovered potentially problematic activity involving personnel in the Office of Data and Technology ("ODT"). Because any internal CFTC investigation would require ODT's assistance, the IRT determined that an independent investigation was needed into the following issues: (1) whether CFTC systems or information had been compromised in the transmission of data between CFTC servers and the home servers of ODT staff; (2) whether network privileges had been abused; and (3) whether retaliation had occurred against a contractor.[4]

Upon receipt of the June 4, 2015, letter, we began an investigation to address the issues identified by the IRT Report and any others that might come to light.[5] Due to the technical nature of the investigation, we contracted with the United States Postal Service Office of the Inspector General ("USPS OIG") to lead the forensic analysis of relevant computer systems and to assist with interviews of witnesses. USPS OIG assigned three Special Agents from their Computer Crimes unit.

Between June 9, 2015, and August 6, 2015, we interviewed 13 individuals within the CFTC, including management and staff within ODT, OGC, and OED. During that time, we also obtained and reviewed CFTC computer and network policies[6] and researched best practices in the area.

USPS OIG imaged and analyzed certain CFTC hard drives and the personal hard drives of a CFTC staff member. The first forensic report was completed on December 3, 2015, and two

---

[1] Letter from CFTC Senior Leadership Response Team, dated June 4, 2015. (Reproduced in Appendix 1.)

[2] Potential Incident Report: Notice of Potential Incident and Request for Approval of Recommendations, May 27, 2015. (Reproduced in Appendix 2.)

[3] The IRT is a group comprised of senior staff in the Office of General Counsel ("OGC"), the Office of Data and Technology ("ODT"), and the Office of the Executive Director ("OED"), and tasked with investigating computer security incidents at the CFTC. See CFTC Policy: Responding to Incidents Involving CFTC Confidential Information. The members of the IRT during the investigation here were: [redacted], OGC; [redacted], [redacted] ODT; [redacted], OED; and [redacted], [redacted] OED.

[4] Letter from CFTC Senior Leadership Response Team, dated June 4, 2015.

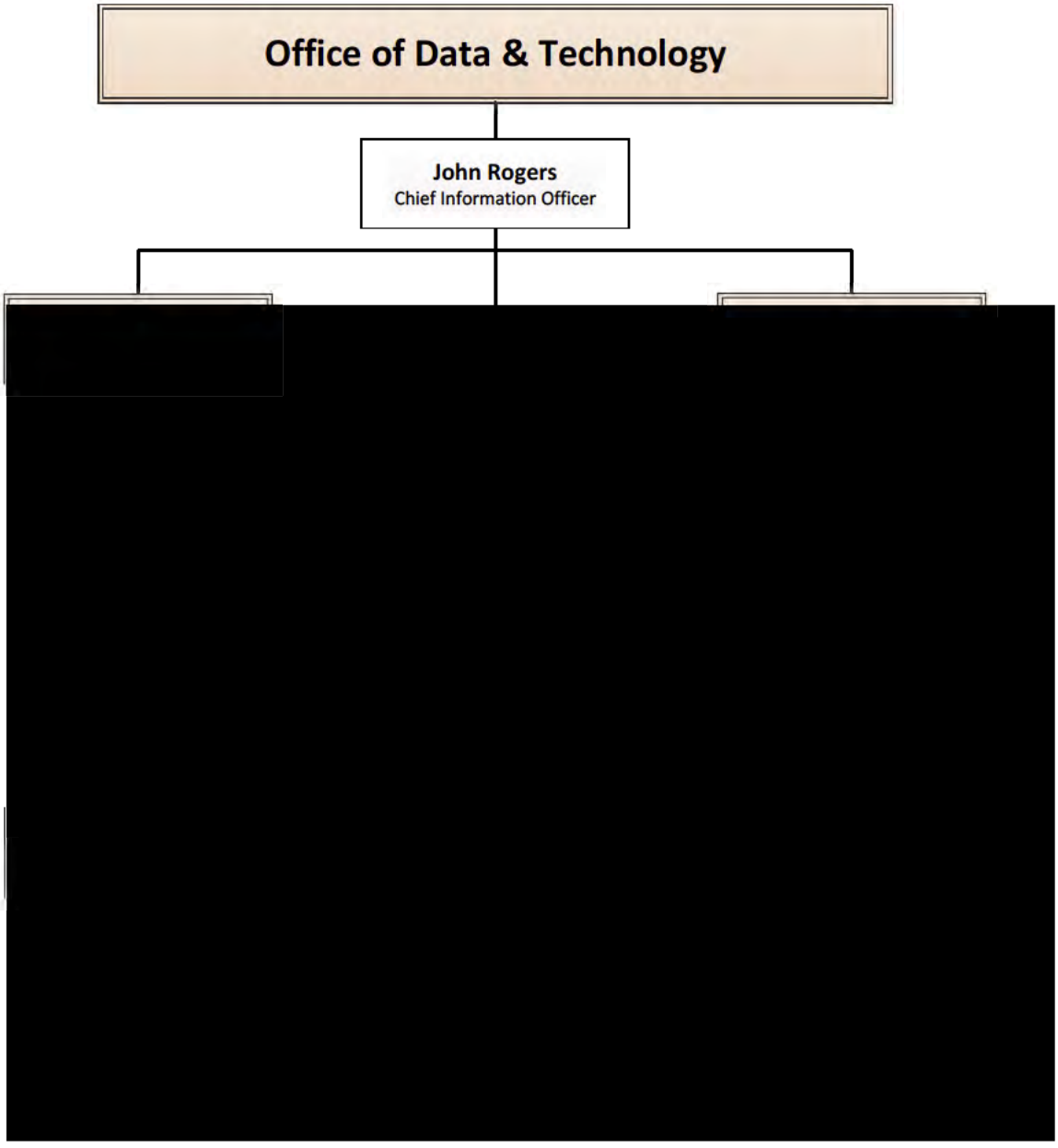
[5] OIG has independent authority to investigate all instances of fraud, waste, and abuse within the agency. Inspector General Act of 1978 § 4. Citations to confidential sources have been removed from this report.

[6] The CFTC's computer security policies are available via the CFTC's internal website, http://cftcnet/Commission/About/Policies/Pages/default.aspx.

additional forensic reports were completed in February 2016. We conducted a follow-up interview on February 2, 2016, and three more interviews on May 25–26, 2016.

RELEVANT PERSONNEL

The figure below shows CFTC personnel relevant to this investigation, as of March/April 2015:



SUMMARY OF THE INCIDENT

In August 2014, and again in January 2015, a contractor ("the Contractor") [redacted] between CFTC systems and external non-CFTC servers. The data transmissions were frequent and large and occurred through both commonly and uncommonly used network ports.[7]

The Contractor brought these data transfers to the attention of his CFTC supervisor, [redacted].[8] The Contractor says [redacted] knew about the connections and was aware of the traffic.

The remote destinations of these connections were personal, non-CFTC servers that [redacted] and [redacted], had set up at their respective residences. [redacted] had been using these home servers for a couple years to test network connectivity, DNS routing, mail throughput, and other issues. [redacted] the direct supervisor of both [redacted], was aware of the practice.

In March 2015, the Contractor again saw the unusual traffic and again raised the issue with [redacted]. According to the Contractor, [redacted] said he would speak with [redacted] and later told the Contractor not to document the unusual traffic and not to investigate the activity further. [redacted] allegedly said the practice was acceptable because the ports were open only for testing purposes, but the practice would be stopped.

The Contractor saw the traffic continue a week or two later, and believed the traffic to be inconsistent with the specific claims of test work, based on the availability of more commonly used ports for testing and the size and timing of the transfers. The Contractor believed it was his duty to report the unusual traffic because of the risks to the CFTC of large quantities of encrypted[9] data being sent via unusual network connections [redacted]

The Contractor therefore resolved to inform [redacted] but was concerned about sending an email through the CFTC email system. The Contractor knew [redacted] involved in the data transmissions in question, had access to all agency emails and therefore could potentially discover the Contractor's email raising an alert. The Contractor therefore transferred the logs from his CFTC computer to his company laptop via a CFTC flash drive, then emailed his

[7] Ports not commonly used by installed network applications are ordinarily kept closed, as part of a firewall to prevent unauthorized access. Use of such ports therefore requires [redacted] to open the port to get through the firewall.

[8] Witnesses dispute whether the Contractor brought the data transfers to the attention of [redacted] in August 2014, but agree that the issue was raised in 2015.

[9] To be clear, encryption of communication channels between external and internal systems is not improper; indeed it is mandated that remote system administration be done over encrypted connections. The fact that the data transfers in question were encrypted is mentioned solely because the encryption prevented review of the data.

company supervisor the logs showing the unusual network traffic. The Contractor's email to his company supervisor included an explanation that he was not using the CFTC email system for fear of retaliation.

On March 31, 2015, the Contractor's supervisor sent an email to [redacted] ("the March 31 email") that alerted [redacted] to the data transmissions on uncommon ports. The email included the supporting network logs but did not identify the Contractor by name. [redacted] concluded from a review of the logs that they showed transmissions using uncommon ports between CFTC systems and external servers.

[redacted] raised the issue of unusual traffic to the attention of John Rogers, the CFTC's Chief Information Officer (CIO). With Rogers's knowledge, [redacted] spoke to [redacted] to discuss the unusual traffic. [redacted] informed [redacted] that the ports were open only for testing purposes and that they remained open all day for convenience. [redacted] said he believed they were open outside of normal business hours because staff failed to close the ports, and [redacted] assured [redacted] the practice would stop.

[redacted] also raised the matter with [redacted], and with [redacted] questioned how [redacted] had obtained the information, but [redacted] did not disclose his source.

[redacted] requested additional network logs but was informed by the [redacted]—that the system storing the requested logs had been corrupted and previous logs had been lost.[10] Although there should have been backups of the logs, [redacted] was informed that attempts to recover the logs failed.

[redacted], after learning of the incident, informed [redacted] and asked him to investigate. [redacted] confirmed with [redacted] that open ports to his home server were being used for testing and instructed [redacted] to discontinue the practice.

In a meeting with Rogers, [redacted] and [redacted], [redacted] was again asked how he obtained the logs and he again refused to say. Instead, he told them that his team performs network scans. [redacted] stated they had reason to believe the source was the Contractor. [redacted] did not at the time know the identity of the source, only the sender of the March 31 email. He therefore replied that he did not believe it was the Contractor. After the meeting, [redacted] called the Contractor's supervisor to ask the identity of the source and was told it was the Contractor.

[redacted] discussed with [redacted] and [redacted] the claim that [redacted] the discovery of the suspicious traffic. Both [redacted] believed [redacted] lacked the tools to make the discovery. [redacted] then took it upon himself to investigate. He suspected the Contractor was the source of the discovery, based on prior work with the Contractor and his past disclosure to the Contractor that [redacted] used home servers for testing. [redacted] then used

[10] The loss of logs is suspicious—security tools had been knocked offline and rebooted, despite what should have been standard practice of having redundancies to ensure connectivity and uptime. It is possible that someone was trying to cover their tracks.

his [redacted] access to [redacted]—effectively searching the email accounts of CFTC Commissioners, the Chief Privacy Officer, senior management and employees, OIG personnel, etc.—and discovered the email to [redacted] that confirmed his suspicion of the Contractor. [redacted] informed [redacted] of his finding, and they reported it to [redacted].

After his email was discovered, the Contractor sensed that his working relationship with [redacted] changed. Projects seemed to be on hold, he was getting more push-back on recommended policy improvements, and no new projects were coming his way.

[redacted] was surprised and angry when he learned the Contractor had raised the alert to [redacted]. [redacted] was also angry with the Contractor. [redacted] decided to "be careful" around the Contractor. [redacted], too, was upset at the Contractor and upset that the incident would cause hostility issues within the business unit.

After learning of the email search, [redacted] advised [redacted] to stop investigating on his own, and reported the Contractor's email to [redacted]. [redacted] and [redacted] apprised Rogers and [redacted] of the discovery of the Contractor's email. In a meeting with [redacted] and Rogers—the highest officials within ODT—[redacted] said that the Contractor "had to go," and brought up the concept of "gapping" the contract with the Contractor's company. Gapping a contract involves not immediately re-contracting with a company at the end of the existing contract—i.e., leaving a gap in service coverage. Gapping the contract would likely have resulted in the Contractor no longer working in [redacted] and [redacted] unit, and possibly not at the CFTC at all. But Rogers and [redacted] decided not to gap the contract—Rogers saw no business justification for doing so, and [redacted] believed there should be no impact on the Contractor and that a gap in [redacted] was an unacceptable operational risk.

Rogers, [redacted], and [redacted] collectively made the decision to report the Contractor's email—but nothing else—as a computer security incident. On April 21, 2015, [redacted] sent an email to the IRT reporting the potential computer security incident. The incident report only included the existence of an email potentially containing confidential or sensitive agency information "sent to the corporate email account of an on-staff contractor who has a signed NDA on file with Commission by another on-staff contractor who also has a signed NDA on file."[11] The incident report made no mention of the suspicious [redacted] that motivated the email in question, or of the email search that lead to discovery of the Contractor's email, and it did not include the Contractor's email.

Upon receipt of the April 21 incident report, the IRT began investigating. On April 22, the IRT met with members of ODT to inquire further about the incident report and the unusual network traffic that motivated the Contractor's email. However, the IRT was troubled by inconsistencies (a "changing story") and responses that seemed to communicate the message "don't look behind the curtain"—i.e., don't investigate the unusual [redacted], only the Contractor's emailing of CFTC network logs. [redacted], who had not disclosed to anyone the

[11] IRT Report, p.1.

existence of the March 31 email reporting the suspicious [redacted], began to suspect someone had accessed his email account.

On May 6, the IRT interviewed the Contractor, who looked, according to an IRT member, "visibly scared for his job."

On May 7, members of the IRT and Rogers, [redacted], General Counsel Jonathan Marcus, [redacted], Executive Director Tony Thompson, [redacted] and others met to discuss the IRT investigation ("the May 7 meeting"). Based on [redacted] surmise that someone had accessed his email, a member of the IRT asked how ODT discovered the Contractor's email. Both [redacted] and Rogers were by then aware of [redacted], but both stated they did not know how the email was discovered. In response to speculation someone may have abused network privileges, neither Rogers nor [redacted] volunteered their knowledge of [redacted] search. Rogers stated only that such a search would be an abuse of network privileges and would be a "serious" issue. An attendee reported that [redacted] advised "they are good employees, be careful of accusing people."

The May 7 meeting also included a discussion regarding the advisability of referring the matter to OIG.

FORENSIC ANALYSES

[redacted] consented to our search of his home computer equipment. The first forensic report by the USPS OIG Computer Crimes Division Special Agents was completed on December 3, 2015, of [redacted] work station and home computers. It states:

> [A]nalysis identified a pattern of artifacts generally consistent with the use of the system for legitimate network testing and remote access purposes. The examination did not locate artifacts that might indicate the network connections between [redacted] workstation and home computer were used for inappropriate purposes or the exfiltration of CFTC information.
>
> While the examination did locate a small number of CFTC documents, they appear to be present on the examined systems due to normal use of CFTC's remote access solutions and do not indicate malicious activity.[12]

[12] Computer Forensic Report, Dec. 3, 2015 (signed by [redacted]). The forensic analyses focused on [redacted] connections to home servers because those connections, unlike [redacted], used unusual ports normally kept closed and unmonitored. Because the forensic analyses of [redacted] hard drives corroborated claims about work testing and showed no evidence of malicious activity, and because forensic analyses consume valuable resources within USPS OIG's Computer Crimes unit, we opted, after careful consideration, not to request a similar analysis of [redacted] hard drives.

However, a hard drive from [redacted] home computer contained an encrypted image of a CFTC laptop, requiring further review.

Second and third forensic reports were delivered by USPS OIG in early February 2016. The second forensic analysis, completed February 3, 2016, focused on text searches for personally identifiable information ("PII") and sensitive CFTC market data. The report "did not locate any relevant PII data [or] any direct information related to CFTC restricted information . . . ."[13]

The third forensic analysis, completed February 5, 2016, focused on the encrypted laptop image on [redacted] home server. The image was of a system installed on a CFTC laptop on July 14, 2014, and used infrequently until July 31, 2014. The laptop image was transferred to the home server on August 2, 2014, and "was never opened or executed." [14] The forensic analysis "did not locate any direct information related to CFTC restricted information, PII, or gross misuse[,]" but it did find evidence [redacted] had accessed personal Gmail accounts from the laptop.[15]

FINDINGS

USPS OIG Found No Evidence that CFTC Systems or Data Were Compromised by Use of Connections to Home Servers

Forensic analyses showed no evidence that CFTC systems were compromised or sensitive information exfiltrated. We find, however, that the ad hoc use of network connections to home servers for legitimate work-related testing falls short of best practices, NIST principles, and agency policies.[16]

---

[13] Computer Forensic Report, Feb. 3, 2016 (signed by [redacted]).

[14] Computer Forensic Report, Feb. 5, 2016 (signed by [redacted]).

[15] Id. [redacted] attended a conference that required him to have a different version of Microsoft Windows on his laptop. He therefore imaged his laptop before the conference so that he could restore the laptop later. Forensic analysis found no evidence that CFTC systems were compromised or sensitive information exfiltrated. Nevertheless, the practice was improper for the same reasons the use of home servers to conduct testing was improper.

[16] The Federal Information Security Management Act of 2002 (FISMA) requires federal agencies to meet minimum information security standards as developed by the National Institute of Standards and Technology (NIST). 40 U.S.C. § 11331(b)(1). NIST develops standards and guidelines relevant for information systems, including standards to provide "adequate information security for all agency operations and assets." 15 U.S.C. § 278g-3(a). NIST guidelines establish, among other things, principles emphasizing proper documentation, open communication and coordination with senior leadership, and balancing of the security risks and advantages of particular methods of system administration and testing. See, e.g., NIST Federal Information Processing Standards 200; NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations; NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment; NIST Special Publication 800-84: Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities; NIST Special Publication 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems; NIST Special Publication 800-41: Guidelines on Firewalls and Firewall Policy. The CFTC has developed internal policies assigning roles and responsibilities for agency personnel and establishing rules and procedures for accessing

Testing using external servers presents heightened risks and challenges to the agency. Both NIST guidelines and multiple CFTC policies emphasize deliberation, documentation, and communication among relevant personnel in establishing baseline security practices and enacting modifications to them.[17] [redacted] plays a central role in both NIST guidelines and CFTC policies in developing and updating security policies and auditing and ensuring their implementation. [redacted] have the responsibility to, among other things, "configur[e] information systems to provide only required capabilities and specifically prohibit[] and/or restrict[] the use of all other functions, ports, protocols, and or services";[18] "ensur[e] configuration changes to information systems are only made by authorized personnel";[19] and "coordinat[e] with the CISO appropriate steps to reduce or eliminate vulnerabilities."[20] Firewall configurations must have "adequate controls," and changes to the firewall configuration must be authorized, "tested for effectiveness and lack of negative impact," and logged (including the reason for the rule change).[21]

Yet t[redacted] was not made aware of the use of connections to home servers and would not have approved had he known of them. Even if the CFTC policies lack a specific, explicit prohibition on connections to his home servers, [redacted] connections to his home server used [redacted] ports not commonly opened, presumably requiring changes to the firewall which were not approved according to the proper procedures and not documented as required. Indeed, it was the encrypted traffic on these [redacted] ports, typically kept closed per CFTC policy and NIST guidelines (and therefore left unmonitored by the CFTC's security tools), that aroused the Contractor's suspicions.

We also find, and [redacted] admits, that he used the connections to his home server to access a personal email account from within the CFTC network. He did so on at least 50 occasions. Accessing personal email accounts from agency equipment is explicitly prohibited by CFTC policies.[22]

We further find that Rogers, [redacted], and [redacted]—all leaders within ODT—failed to report the unusual network connections as a computer security incident. CFTC policy dating back to

---

agency computer systems and networks. Agencies may adopt more stringent standards provided they are cost-effective, contain at a minimum the provisions of the mandatory NIST guidelines, and are "otherwise consistent" with the mandatory NIST guidelines. 40 U.S.C. § 11331(c). In addition to laying out specific requirements, rules, and responsibilities, CFTC policies also state that system administrators "shall follow industry best practices in the use of defensive tools and procedures." CFTC Policy: Computer Incident Response Capability, Nov. 9, 2004.

[17] CFTC Policy: IT Security and Privacy Program, Oct. 2011.

[18] CFTC Policy: IT Configuration, Mar. 2012.

[19] Id.

[20] CFTC Policy: IT Security and Privacy Program, Oct. 2011.

[21] CFTC Policy: Firewall, Jun. 9, 2005. Although the policy states that it is intended to prevent violations by someone *outside* the CFTC, the firewall policy does not discriminate between incoming and outgoing traffic.

[22] We also note that the undetected circumvention of the agency firewall and access of a prohibited email site demonstrates that such connections indeed pose a real security risk, even if no sensitive information or systems were compromised in this instance.

2004 defines a computer security incident as "a violation of standard computer security policies, acceptable use policies, or standard security practices," and provides for reporting of computer security incidents to, and investigation of such incidents by, the IRT.[23] Rogers states he felt the matter had been addressed internally. Indeed, orders eventually were issued to cease use of the connections. However, the purpose of reporting incidents is not solely to resolve them but also to document the incidents and their resolutions and to ensure systematic review and control takes place, lest the resolution prove short-lived or otherwise insufficient. In this matter, in fact, although ODT senior leadership may have believed internal actions had resolved the matter, the Contractor reported that the connections had not ceased by May 2015, over a month after the Contractor's supervisor forwarded the Contractor's concerns to [redacted].

The Contractor's External Emailing of Network Logs Did Not Violate CFTC Policies or Agreements

We concur with the IRT Report that the Contractor's email did not compromise confidential or sensitive CFTC information, despite the Contractor's use of an external email account.[24] As stated in the IRT Report:

> The [C]ontractor's employer has signed a contract with the Commission that contains the standard Federal government privacy and confidentiality protections, including required compliance with Privacy Act of 1974, Federal Information Security Mangement Act[,] . . . and NIST Standards. These standards include provisions for handling and securing information which the [C]ontractor must follow. Although the information [CFTC network logs] was sent using the [C]ontractor's company email, there was no loss of control because the [C]ontractor is bound by these provisions.
>
> . . .
>
> The IRT has determined that this event does not rise to the level of an incident. CFTC confidential information was not compromised. Regardless of whether the information was confidential, the access to and use of the information was authorized and there was not a loss of control of the information. We recommend closing this incident as to this issue.[25]

There Was an Abuse of Network Privileges and a Failure to Report the Abuse

We find that it was an abuse of network privileges, and therefore a violation of CFTC policies, for [redacted] to use his [redacted] privileges to search the enterprise mail system to discover the Contractor's identity. In addition, we find there was a failure to report the abuse.

---

[23] CFTC Policy: Computer Incident Response Capability, Nov. 9, 2004.

[24] It is worth emphasizing that the Contractor's work at the CFTC was focused on [redacted] and the appraisal of [redacted].

[25] IRT Report, p. 7-8.

The ability to access CFTC computer systems is distinct from authorization to perform particular operations on that system.[26] We do not see, in the written CFTC policies we reviewed, a clear description of what operations by the [redacted] require special authorization, or of what procedures must be followed to secure such authorization. However, CIO Rogers stated that approval to search the enterprise email system by someone with [redacted] privileges would ordinarily go through himself, Human Resources, and OGC, and all witnesses with an opinion, including the Executive Director, agreed that conducting a search without obtaining that approval would constitute an abuse of privileges. [redacted] acknowledged that he knew his search was inappropriate, and therefore his search was a *knowing* abuse of privileges in violation of CFTC policies.

We find that those who knew of [redacted] search failed to comply with agency policy by not reporting the search as an "incident." At the time that Rogers, [redacted], and [redacted] agreed to file a report to the IRT regarding the Contractor's email of CFTC network logs, each was aware that [redacted] had abused his network privileges to determine the Contractor's identity. [redacted] and [redacted], too, were aware of the unauthorized search. Yet no one reported that unauthorized search as a computer security incident.

[redacted] initially directed [redacted] to cease his personal investigation immediately, and Rogers separately instructed [redacted] to "address" the issue with [redacted]. [redacted] passed the instruction along to [redacted], who "verbally counseled" [redacted]. But no corroborating written evidence exists of the counseling or its content. Notably, [redacted]s performance evaluation for the performance year ending April 30, 2015, signed by [redacted] and [redacted] within a month of the incident and alleged counseling, makes no mention of the unauthorized search of the email system.[27] These appear rather peculiar omissions.

We recommend that management take the appropriate steps to address the abuse of network privileges by [redacted] relating to the unauthorized email search and the use of CFTC equipment to access personal email.

Actions of a Retaliatory Nature Were Taken Against the Contractor

Actions of a retaliatory nature impair the integrity, economy, and efficiency of CFTC's programs and operations.[28] We therefore take a broad view of whistleblowing and retaliation, and we do not limit our analysis to the explicit statutory prohibitions contained in the

[26] CFTC policy defining computer security incidents, for example, provides separately for "attempts to gain unauthorized access to a system or its data," and "the unauthorized use of a system for the processing or storage of data[.]" CFTC Policy: Computer Incident Response Capability, Nov. 9, 2004. Similarly, the Computer Fraud and Abuse Act provides criminal penalties for "[w]hoever . . . intentionally accesses a computer without authorization *or exceeds authorized access*, and thereby obtains information from any department or agency of the United States[,] or information from any protected computer." 18 U.S.C. § 1030(a)(2).

[27] CFTC Performance Assessment Form for [redacted], signed by [redacted] (5/11/15) and [redacted] (5/27/15). The performance evaluation makes no mention of the connections to a home server, either.

[28] Inspector General Act of 1978 § 4(a)(5).

Whistleblower Protection Act of 1989 and the National Defense Authorization Act of 2013. The fact that the Contractor's whistleblowing may not fall under the protection of those statutes, despite deserving such protection, suggests the potential for further Congressional action to protect those who raise bona fide complaints of wrongdoing.[29]

The Contractor chose to route his concerns to [redacted] via an external email to his company supervisor because he feared an email sent via the CFTC email system might be discovered and lead to retaliation. As noted earlier, an IRT member reported the Contractor looked visibly scared for his job during his IRT interview.

We identify three acts as retaliatory in nature, irrespective of whether they are statutorily prohibited:

1. [redacted] willfully exceeded [redacted] authority in order to discover the complainant's identity, then disclosed that identity within ODT. Unmasking an individual who reports potential wrongdoing is retaliatory in nature.

2. [redacted] felt that the Contractor "had to go," and recommended to ODT's senior leadership the possibility of gapping the contract on which the Contractor was paid. Such action is retaliatory in nature.[30]

3. Third, Rogers, [redacted], and [redacted] agreed to file, and [redacted] filed, an incident report focused solely on the actions of the Contractor. Both the IRT and our investigation found the allegations against the Contractor meritless. Meanwhile, Rogers, [redacted], and [redacted] had knowledge of two other possible violations of CFTC policy—the abuse of administrative privileges by [redacted], and the ongoing connections to personal servers located at private residences. Yet these violations went unreported. Worse still, Rogers and [redacted] avoided the IRT's attempts to investigate these other violations, keeping the focus on the Contractor. Reporting an individual's actions taken to report potential wrongdoing, but not reporting the potential wrongdoing the individual sought to report, is retaliatory in nature.[31]

We are concerned that contractors who blow the whistle on suspicious conduct by CFTC employees or disclose potentially improper activity at CFTC have little protection under existing whistleblower provisions. We recommend that CFTC work toward adoption of an Agency-wide

[29] The Whistleblower Protection Act of 1989, 103 Stat. 16, Pub. Law 101-12 (Apr. 10, 1989), offers protection to federal employees, but not to contractors. Protection afforded to contractors in the National Defense Authorization Act of 2013 applies only with respect to "gross mismanagement of a federal contract, gross waste of federal funds, an abuse of authority relating to a federal contract or grant, a substantial or specific danger to public health or safety, or a violation of law, rule, or regulation related to a Federal contract . . . or grant." 41 U.S.C. § 4712.

[30] That [redacted] recommendation was not accepted is irrelevant to the fact that it was retaliatory in nature.

[31] Investigations can be retaliatory in nature. See *Russell v. Dept. of Justice*, 76 M.S.P.R. 317, 323-324; 1997 MSPB LEXIS 1010 (1997) ("The [Merit Systems Protection] Board will consider evidence regarding the conduct of an agency investigation when the investigation was so closely related to the personnel action that it could have been a pretext for gathering evidence to retaliate against an employee for whistleblowing activity").

policy that prohibits retaliation against contractors who in good faith report any wrongdoing by CFTC employees or any perceived deficiencies in CFTC operations.

Senior ODT Personnel Displayed a Lack of Candor and Made False and Misleading Statements

Rogers, [redacted], and [redacted] participated in the referral to the IRT. Only the Contractor's emailing of network logs was referred. The open connections between CFTC and foreign servers and the unauthorized email access were also network security incidents. Rogers initially believed everything should be reported to the IRT. Nevertheless, Rogers, [redacted], and [redacted] collectively determined that the report would cover only the Contractor's external email of network logs.

At the May 7 meeting with the IRT and the Senior Leadership Response Team, Rogers and [redacted] already knew how the Contractor's email containing network logs of the suspicious connections had been discovered, but withheld that information when asked and in fact misled and lied to the IRT by affirmatively stating they did not know how the Contractor's email was discovered. Rogers and [redacted] do not dispute the recollection of their statements by other attendees at the meeting. They also do not dispute that they knew of [redacted] email search before the May 7 meeting. Neither provided an adequate explanation to our Office for their statements at the May 7 meeting.

Although Rogers asserted in a recent interview that he had separately disclosed the email search to the Executive Director and to the Chairman's Chief of Staff around the time of the May 7 meeting, neither the Executive Director nor the Chief of Staff recalled being so notified and both stated they do not know how the Contractor's email was discovered.

Rogers was one of three signers of the letter of referral to OIG, which requested our investigation into "whether network privileges had been abused," even while he knew network privileges had been abused. This wasted OIG time and resources, just as the initial referral wasted the IRT's. It also placed the other signers of the letter of referral, the General Counsel and the Executive Director, in a potentially awkward position of having to explain their role in a referral that contained incomplete and misleading information.

We recommend Management take the appropriate steps to address the conduct of senior ODT leadership in this matter.

CFTC Information Technology Policies & Practices Need Review

Although this report focuses on a specific computer security incident, we find that the incident revealed potentially significant shortcomings in the CFTC's IT security policies and practices. Among them:

- Current IT policy documents are sparse, vague, and lacking in coverage. Several appear to be over a decade old and refer to obsolete positions, teams, etc. In addition,

as the IRT noted, there appear to be inconsistencies between contracts and policy documents.[32]

- Adherence to and application of current IT security policies is lacking.[33] Multiple interviewees also suggested computer security training is insufficient.

- The network firewall changes, lost and/or corrupted logs, and search of the email system suggest a lack of controls relating to IT security policies and practices.[34]

- Multiple interviewees referred to friction over computer security issues between ODT's Policy and Planning Branch and its Network Operations Branch.[35]

CONCLUSION AND RECOMMENDATIONS

We commend the IRT in its handling of this matter. We concur in its conclusions and recommendation regarding the Contractor's use of a company email system to send CFTC network logs. With regard to the other issues that arose during the course of its investigation, we believe the IRT made the right decision in recommending referral to a third party for investigation.

We recommend that management determine the appropriate steps to take regarding the retaliatory actions taken against the Contractor, the abuse of network privileges by [redacted], and the lack of candor and false and misleading statements by Rogers and [redacted]. We recommend that CFTC undertake the creation of an Agency-wide policy that prohibits retaliation against and protects contractors who in good faith report any wrongdoing by CFTC employees or any perceived deficiencies in CFTC operations. We will follow up in six weeks.

[32] IRT Report, p. 8.

[33] For example, a policy describing the IRT function has been in place since 2004 and requires the CIO to "coordinate the development and execution of mock incidents to provide opportunities for [IRT] members to develop skills in responding to incidents." CFTC Policy: Computer Incident Response Capability, Nov. 9, 2004. It appears these mock incidents have not taken place as mandated.

[34] We are especially disturbed at the loss of network logs in this instance, as it hindered the CISO's efforts to learn the content of data transferred to external servers.

[35] We understand that security operations have already been moved under the CISO to ameliorate this issue.

APPENDIX 1

U.S. COMMODITY FUTURES TRADING COMMISSION
Three Lafayette Centre
1155 21st Street, NW, Washington, DC 20581
Telephone: (202) 418-5160
Facsimile: (202) 418-5541
www.cftc.gov

June 4, 2015

VIA HAND DELIVERY

A. Roy Lavik
Inspector General
U.S. Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street, NW
Washington, DC 20581

Re: Potential Security Incident

Dear Roy,

Attached is a report regarding a potential security incident presented to the agency's Incident Response Team (IRT) on April 21, 2015. The reported incident involved the transmission of computer security logs between contractors on their non-CFTC corporate accounts. In the course of investigating the reported incident, the Incident Response Team identified an additional underlying potential security incident, as well as allegations of a fear of retaliation, and the possible improper use of system privileges, all of which are set forth in further detail in the attached report. While the Office of Data Technology (ODT) would generally perform an investigation of a reported security incident, because these matters all arise in ODT, we concur with the IRT's recommendation that an independent third party should investigate the issues identified in the attached report. Therefore, we are transmitting the report and recommendations to you for further review.

We, and IRT staff, are available at your convenience to brief you or your staff in more detail on our review and the issues set forth in the attached report. If, after reviewing, you determine that further review by the Office of the Inspector General is not warranted, we respectfully request that you advise us so that we can determine the appropriate next steps to address the issues identified in the attached report.

If you have any questions, please do not hesitate to contact us. Thank you for your attention to this matter.

Sincerely,

Jonathan L. Marcus

John L. Rogers

Anthony C. Thompson

APPENDIX 2

U.S. COMMODITY FUTURES TRADING COMMISSION
Three Lafayette Centre
1155 21st Street, NW, Washington, DC 20581
Telephone: (202) 418-5160
Facsimile: (202) 418-5541
www.cftc.gov

CONFIDENTIAL

POTENTIAL INCIDENT REPORT

TO: CFTC Senior Leadership Response Team
Anthony Thompson, Executive Director, Senior Agency Official for Privacy
Jonathan Marcus, General Counsel
John Rogers, Chief Information Officer

FROM: CFTC Incident Response Team
[redacted]

DATE: May 27, 2015

SUBJECT: Notice of Potential Incident and Request for Approval of Recommendations

---

Summary

On April 21, 2015, the [redacted] in the Office of Data Technology (ODT) reported a potential incident to the agency's Incident Response Team (IRT). The incident reported concerned an email that contained agency information that "was sent to the corporate email account of an on-staff contractor who has a signed NDA on file with Commission by another on-staff contractor who also has a signed NDA on file." The IRT began a review of the potential incident and through its investigation identified four distinct but interrelated issues: the reported use of a non-CFTC email account to transmit CFTC information; a contractor's allegation that he used the non-CFTC email account to send information about a potential incident to his supervisor, relying on the non-CFTC account out of fear of retaliation for reporting suspicious activity; a possible abuse of system administrator privileges that raises concerns about possible unauthorized access to CFTC information; and suspicious activity involving transmissions between CFTC systems and the home server of at least one CFTC staff member. The IRT only was presented with the first issue, which the IRT has concluded did not compromise CFTC information, as discussed below. Because the remaining issues are

inextricably intertwined and raise more questions, the IRT recommends that these issues be referred to an independent third party for investigation.

A. Background

1. Report to the IRT

The report on April 21, 2015 stated that a CFTC contractor sent information from his non-CFTC corporate account to another contractor on their employer's corporate account and described the information sent: "the workstation IP addresses, the names, residential destination IP addresses, and ports and protocol used to communicate--for [redacted] over the period of 30 days" and asked whether there were concerns about information-security or personally identifiable information (PII) and whether it should be reported as an incident. To fully understand the data that was sent from the contractor's corporate account, two members of the IRT [redacted] met the same day with the [redacted] and a representative of the [redacted]. The [redacted] reported that the data sent from the contractor consisted of activity logs that showed traffic between ports on CFTC systems and the home servers of two CFTC [redacted] In addition to discussing the reported incident, when asked about the underlying activity in the logs, the [redacted] stated that the ports referenced in the logs were open for system testing and that there was not a problem with this activity. The [redacted] representative indicated that the activity was unusual and could pose a high security risk. Both members of the IRT believed that the underlying activity could be a reportable security incident and requested more information about the underlying activity, including the logs. With respect to the reported incident itself, the IRT asked whether the contractor regularly used his corporate account to transmit data.

On April 22, 2015, via email, the [redacted] provided the following information about the contractor email:

> Was the contractor emailing potentially sensitive information to a corporate email address a one-time occurrence or was there a pattern and practice?
> *This was the only time.*

That same day, via email, the [redacted] provided the following information about the underlying incident:

> What was the information originally sent externally by the [redacted]?
> *Information was not sent, connections were established to troubleshoot/test network operations connectivity issues.*
>
> Was there a pattern and practice to network administrator activity?
> *Will continue to establish connections for testing purposes.*
>
> Has the information been sent externally by the network administrators been destroyed?
> *Not applicable. Information was not transferred.*

On April 23, 2015, the [redacted] provided copies of the non-disclosure agreements signed by both contractors. Additionally, the [redacted] notified the IRT that the employees at the contractor's company and server engineers had all deleted copies of documents and logs that were sent between the two contractor employees.[1] In response, the IRT noted that we do not usually recommend deleting the files until the investigation is closed.

The IRT requested copies of the logs that the contractor sent, and the [redacted] offered to review the logs, stating: "It's my understanding that the email in question contained log files containing a capture of suspicious traffic. If possible and since I am experienced with analyzing log files, I'd like the opportunity to take a closer look to better understand the outbound connections and to rule out any foul play."

2. Review of the Logs

The [redacted] reviewed the logs and provided his analysis. In pertinent part, the logs demonstrated transmissions between CFTC network systems and at least one residential address. Specifically, in a 30 day period, there were 22,612 entries and over 50 CFTC source ports used [redacted], and the CFTC ports changed day-by-day. In addition, the endpoint for the [redacted] which is an fcopy-server[2]; the outbound traffic was SSH traffic[3] which was encrypted and sent to two IP addresses registered to Verizon FIOS at what appear to be at least one residential address in [redacted] Virginia.

> The [redacted] provided additional information about [redacted] specifically:
>
> [redacted] uses the Datagram protocol, a communications protocol for the Internet network layer, transport layer, and session layer. This protocol when used of [redacted] makes possible the transmission of a datagram message from one computer to an application running in another computer. Like TCP (Transmission Control Protocol), UDP is used with IP (the Internet Protocol) but unlike TCP on [redacted] is connection less and does not guarantee reliable communication; it's up to the application that receives the message on [redacted] to process any errors and verify correct delivery. Because protocol [redacted] was flagged as a virus (colored red) does not mean that a virus is using [redacted] but that a Trojan or Virus has used this port in the past to communicate.

In summary, [redacted] uses User Datagram Protocol (UDP) for transmissions over the internet which makes it possible to transmit data from one computer to another computer.

---

[1] "All [contractor] employees associated with the security event under review have deleted all copies of the documents and logs related to the incident in question. Furthermore, [contractor's] server engineers have deleted all copies of the documents from the corporate email server and backup solutions. If you should require any other statements from us please don't hesitate to ask." [redacted] email to IRT 4/23/15, quoting information from the contractor's employer.

[2] The **fcopy** command copies data from one I/O channel, *inchan* to another I/O channel, *outchan*.

[3] **Secure Shell**, or **SSH**, is a cryptographic (encrypted) network protocol for initiating sessions on remote machines in a secure way.

Additionally, the [redacted] provided information about the fcopy Command, most notably:

[redacted]

The [redacted] noted that fcopy-servers are typically used to copy data from one channel to another and can be used to copy and transfer large files.[4]

After reviewing the logs and assessing the information about the ports, the [redacted] provided the following summary to the IRT[5]:

> Based on the information contained in at least one of the log files, it appears that there is some type of automated application or service establishing connections from CFTC to the external IP addresses noted above. The logs did not contain data size counts that would indicate how much data was transferred over the last 30 days. This information should be available in the event that a more in-depth investigation is necessary. If the communication channel was actually encrypted and data was transmitted, this would result in an inability to replay exactly what left the organization.

3 Interview with Contractor

On May 6, 2015, the [redacted] met with the contractor who sent the logs. The contractor provided a summary of facts about the logs and the actions taken that date back to August 2014. According to the contractor, in August 2014, an information technology "data loss prevention" tool under evaluation by ODT detected unusual traffic between ports on CFTC systems and the home server of at least one ODT [redacted] The traffic continued over full days, and at times overnight and on weekends outside of business hours. The contractor noted that this is atypical behavior and could pose a security risk to the agency. The contractor noted the findings and spoke with the [redacted], the [redacted] whose home server was involved, and [redacted] management. The [redacted] replied that he was aware of the traffic.

In early 2015, the contractor detected the same type of traffic to the same home server and again raised the issue with the [redacted] ead. According to the contractor, the [redacted] ead instructed the contractor not to document the unusual traffic in the incident ticketing system[6], not to report it, and not to investigate the activity further. The [redacted] lead stated that the practice

[4] The "channel" connects two ports together.
[5] He noted that: "Please beware that this analysis is highly speculative based only on the information provided and what is typically associated with the traffic detected. There is a chance that something different was taking place on the network due to the ability to utilize various ports to support different types of communications. [redacted] s a standard according to the Internet Assigned Numbers Authority (IANA)." [redacted] email to IRT 4/23/15.
[6] The contractor stated that the general procedure for reporting suspicious activity is to document it and open a ticket in the agency's "Footprints" system.

was acceptable, he was aware of it, and that the ports were open only for testing purposes, but that this arrangement would be stopped.

A week or two later, the contractor found that the unusual traffic continued. He stated that he felt that the traffic was inconsistent with testing, noting among other things that other ports were available and often used for testing, the traffic at times appeared to be transmitting gigabytes of data and often occurred outside business hours. The contractor stated that he felt it was his duty to report the unusual traffic because he felt the CFTC faced the following risks:

(a) an open port on CFTC systems without the typical monitoring or security controls for many hours a day, often outside business hours;
(b) because the traffic was encrypted and the port was not monitored by the CFTC security web filtering tools, the agency's tools were unable to detect or analyze the staff activity on the connection;
(c) the home server was not a tested and trusted server and thus, possible malware, viruses or other issues on the home server could transmit back into and harm CFTC systems; this risk is high given the [redacted] access privileges to the CFTC network and resources;
(d) possible data loss, with gigabytes of traffic possibly travelling between the CFTC and home server; and
(e) the established connection did not follow the CFTC normal operating procedures.

The contractor stated he was concerned about reporting to the [redacted] through the CFTC email system because the [redacted] involved in the use of the ports has the ability to access and read his emails, and he feared retaliation since he had been told not to document or report the issue by the [redacted] lead.[7] He saved the logs showing the unusual traffic to a CFTC-issued and encrypted flash drive, plugged the flash drive into his company-provided laptop, and emailed the logs to his supervisor through the contractor's corporate email account (corporate email address to corporate email address).[8] He stated that in his email he explained to his supervisor that he was not using the CFTC email system and instead was using his company's email because he feared retaliation.[9] His supervisor then sent an email from his corporate account to the CFTC [redacted] containing the logs, without identifying the contractor.

The contractor asserted that he used the company email because he feared retaliation and he felt the subsequent report of his email as a potential incident was itself retaliation. He also stated that he felt the ODT [redacted] cad was trying to dismiss and "cover up" the original transmissions to the home server. He stated that he was concerned about his professional reputation and concerned about risks to the CFTC because of these transmissions and possible data loss. He stated that the transmissions did not appear to be consistent with approved testing and did not follow the ODT normal operating procedures and should be investigated further.

---

[7] The staff involved [redacted] and possess full CFTC network administrator privileges.
[8] The contractor's company is under confidentiality obligations and must comply with the Privacy Act of 1974, FISMA and other Federal privacy and security standards. The individual contractors at issue personally signed non-disclosure agreements with the CFTC, as provided by the [redacted]
[9] Although the contractor agreed to provide the email to the IRT, [redacted] after the interview.

4. [redacted] Receipt of Logs

On March 31, 2015, the [redacted] received the logs from the contractor's supervisor. After a preliminary review by the [redacted] the [redacted] reported the activities to his supervisor [redacted] and also to the management of the [redacted]. The [redacted] then met with the [redacted] involved in the activity and the [redacted] management to discuss the unusual traffic. The [redacted] asserted that the ports were open only for testing purposes, they remained open all day for convenience, and that they remained open outside business hours at times because the staff neglected to close the ports. The [redacted] stated he would ensure the practice stopped. In a meeting on April 29 between the [redacted] chain of command and the Chief Information Officer (CIO), the CIO agreed that the practice of using these transmissions should stop.

In the [redacted] meeting with his supervisor and the management of the [redacted], the management asked how the [redacted] found out about the situation. The [redacted] responded that how he found out was irrelevant. Shortly thereafter, one or more [redacted] staff, including the [redacted] involved and [redacted] manager, learned that the contractor had emailed his supervisor outside the CFTC email system, and that the contractor's supervisor had contacted the [redacted]. At least one individual questioned how the [redacted] and his management team could have learned that without having reviewed the [redacted] email.

5. [redacted] Assessment

Following the interview with the contractor, the [redacted], [redacted], [redacted], and [redacted] met. The [redacted] and [redacted] discussed the security risks identified by the contractor. They noted that the use of the fcopy port is "suspicious" as the port is designed to be able to do "call backs" to the original server to ask for data. Further, they explained that the combination of encryption and lack of web filters could allow viruses, malware, or prohibited content to enter our servers.[10] Finally, both the [redacted] and the [redacted] stated that the combination of opening the ports all day (and sometimes longer), using the fcopy server, and the volume of data transferred are suspicious and inconsistent with testing, based on their review at that point and without drawing any conclusions about the purpose of the transmissions.

The [redacted] also reported that he had reviewed the logs and requested additional logs.[11] He learned that one of the systems containing the logs had been corrupted and all previous logs had been lost. Also, while there were back-ups of the logs, the [redacted] and other ODT staff stated that attempts to recover the logs failed.

[10] In at least one instance the [redacted] has a document that shows- over 2 gigabytes of traffic flowing from the home server to the CFTC.

[11] The [redacted] reports to the [redacted], while the [redacted] reports to the [redacted]. The [redacted] requested the logs from the [redacted].

B. Issues Concerning the Reported Potential Incident

Regarding whether the use of the contractor's email was an "incident" that risked compromise of CFTC confidential information, under the Agency's draft Incident Response Policy,[12] all potential incidents must be reported to the IRT. The policy defines potential incident as: "an observable change to the normal behavior of, or deviation from applicable law or regulations related to, a system, environment, process, workflow or person that is deemed to be suspicious." The policy further states that the IRT will determine whether an event is an incident, which is defined as: "the **actual or suspected** loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to confidential information, whether physical or electronic."[13]

Upon review of the facts, the contractors iovolved in sending and receiving the information were both authorized users accessing it for an authorized purpose. The questions posed in the initial report seem to indicate that there may have been loss of control (through use of the corporate email accouot) and a violation of the contractor's non-disclosure agreement (NDA) if the information seot was confidential information. We address the two issues below.

1. Was there a loss of control?

The contractor's employer has signed a contract with the Commission that contains the standard Federal government privacy and confidentiality protections, including required compliance with the Privacy Act of 1974, Federal Information Security Management Act (FISMA) and NIST Standards. These standards include provisions for handling and securing information which the contractor must follow. Although the information was sent using the contractor's company email, there was no loss of control because the contractor is bound by these provisions.[14] Additionally, the contractor and the contracting company have confirmed that the documents and logs have been purged.

2. Was there a violation of the contractor's non-disclosure agreement ("NDA") if the information sent was confidential information?

Although the IRT does not consider the situation to have raised risks to the CFTC, there is a question of whether the contractor violated any CFTC policies, the applicable non-disclosure agreement or the contractor's contract with the CFTC. The information included publicly

[12] The draft policy has been approved by the CIO, GC, and SAOP for union consultation. Although the policy is not finalized, the IRT is, and has been, operating under the procedures and definitions established in the policy. The current policy is consistent, stating: "Any incident, whether confirmed or suspected, involving the real or potential loss or compromise of PII must be reported to the CISO and CPO as soon as the incident is discovered." Reporting Incidents Involving PII Policy.

[13] See draft Incident Response Policy; see also OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information.

[14] We note that not all contractors have CFTC email accounts, and if not, the contractors perform work for the CFTC using their corporate email accounts with CFTC information stored on the contractor's system in accordance with the terms in the contract.

available names of two CFTC employees and Internet Protocol addresses which are generally dynamically assigned by internet service providers to computers, and therefore, do not constitute PII.[15] The IRT notes that the information transmitted, in a vacuum, generally is not considered "sensitive PII" under CFTC policies.[16] That being said, if the context of this information included accusations of wrongdoing, then in context, it could be considered "sensitive PII," but even in this event, there was no loss of control of the information. Although the information is likely not sensitive PII in this context, the definition of confidential information is much broader and the security logs are likely confidential under another agency policy which requires specific methods of transmission.[17] The IRT has noticed that applicable policies and contract documents appear to include inconsistencies, however, whether any policies or the contract terms were violated is not for the IRT to decide.

Recommendation:

The IRT has determined that this event does not rise to the level of an incident. CFTC confidential information was not compromised. Regardless of whether the information was confidential, the access to and use of the information was authorized and there was not a loss of control of the information. We recommend closing this incident as to this issue.

C. Contractor Concern about Retaliation

In his meeting with the [redacted] and [redacted] on May 6, the contractor stated that he raised the issues about the unusual traffic in August 2014 and again just over a month earlier. He states that he was told again the activity would stop, but was also instructed not to document the situation into the event logs (the "Footprints" system), not to report it and not to investigate further. A week or so later when he learned the traffic had not stopped, he stated that he felt he had a duty to document the situation, but because both CFTC staff and management were aware of the situation and told him not to document it, he was concerned that he would face retaliation from CFTC staff. He then sent the email to his supervisor. He stated that he felt the incident report of his email to his supervisor was itself retaliation.

Recommendation:

Because this issue is outside the purview of the IRT, the IRT recommends that an independent third party investigate.

[15] See, e.g., Johnson v. Microsoft Corp., No. C06-0900RAJ, 2009 WL 1794400 (W.D. Wash. June 23, 2009) (an IP address identifies a computer; "an IP address is not personally identifiable").
[16] See CFTC Safeguarding Personally Identifiable Information policy (sensitive PII "means a subset of PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual").
[17] The IRT notes that other policies may apply including: Handling and Disclosure of Confidential Information, Interim Policy Concerning Records Requirements for Electronic Communications, Mobile Device Policy, and the Commission procedures for removable devices.

D. Possible Abuse of Network Privileges

As described above, the contractor stated the he did not provide or discuss the email he had sent to his supervisor to anyone at the CFTC. The day after he discussed the practice and the unusual activities with the [redacted] management, the [redacted] stated that management asked him how he found out about the practice and how he obtained the log file. The [redacted] told management that how he found out was not relevant. At some point, the staff of the [redacted] became aware that the contractor used his company email to send the information to his supervisor. It is unknown how the staff determined that the contractor emailed his supervisor on a non-CFTC email address. It has been stated that it is possible that the [redacted] or another [redacted] reviewed the emails of the [redacted] and the emails between the [redacted] and the contractor's supervisor. This is mere speculation. However, ODT management agrees that if anyone used [redacted] credentials to view an employee's email without explicit authorization, that behavior could constitute an abuse of network privileges. Such an act could be an unauthorized accessing of CFTC information and could itself constitute an incident.

Recommendation:

The IRT notes that this issue was mentioned in the course of the investigation into the original potential incident. The IRT has not investigated this further because this issue is intertwined with the allegations of a fear of retaliation, which the IRT recommends that an independent third party investigate.

E. Transmissions from CFTC System to Home Servers

The [redacted] has reviewed the available logs and met with the [redacted] and his management concerning the transmissions and feels he has exhausted that avenue of investigation. Without a forensic analysis, the IRT cannot glean any additional information about the traffic between the CFTC and home server. It is unknown whether the connections were open solely for testing; whether malware could have been transmitted to CFTC systems; whether the staff members involved were using the web without web filtering for other purposes; or whether CFTC data was exfiltrated.

Recommendation:

Although this type of investigation would ordinarily fall under ODT's direction, because the activity originated in ODT, to avoid any appearance of a conflict, the IRT recommends that an independent third party conduct a forensic review of the systems involved to determine whether there were risks to CFTC systems and information.

Notification to US-CERT:

The ODT Information Security Team has not contacted US-CERT concerning the contractor's email to his supervisor because there was no compromise of CFTC information. If a later finding on other issues indicates that US-CERT should be notified, the Information Security Team will provide the notification.

Notification to OIG:

The Senior Leadership Response Team will ensure that this Report is provided to the CFTC Inspector General.

Recommendations:

1. The IRT has determined that the reported potential incident related to the contractor's email to his supervisor does not rise to the level of an incident. CFTC confidential information was not compromised. The IRT recommends that the SLRT close this issue.

2. As indicated above, to understand risks to the Commission and/or individuals based on the issues described above, the IRT recommends that the remaining matters be jointly referred to an independent third party for investigation.

3. The IRT recommends that management approve the draft Incident Response Policy. Among other things, the draft Policy provides a means for employees and contractors to anonymously report potential incidents to the IRT members.

4. Once the Incident Response Policy is signed, the IRT recommends training for all staff on reporting potential incidents.

5. The IRT recommends that management conduct a review to determine whether issues raised in this report require further action.