



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

December 16, 2016

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

FROM: A. Roy Lavik, Inspector General *ARL*

SUBJECT: Follow-up to OIG's Investigation into a Potential Information Technology Security Incident

On June 27, 2016, my Office completed an investigation into allegations concerning a potential computer security incident. In the investigative Report,¹ we made recommendations and promised to follow up on actions taken by the CFTC. These are our findings.

Employee Discipline

Our investigation revealed that the Chief Information Officer (CIO) and four Office of Data & Technology (ODT) employees variously engaged in inappropriate network activity, and/or actions of a retaliatory nature (or improper consideration of such actions) against a contractor, and/or deceptive responses in our investigation. The CFTC has expressed no disagreement with these findings. We recommended that CFTC management "determine the appropriate steps to take regarding the retaliatory actions taken against the Contractor, the abuse of network privileges by [ODT staff], and the lack of candor and false and misleading statements by [the CIO and ODT staff]." The CFTC concurred with this recommendation.²

The Chairman's Office sent "Memorand[a] of Warning and Instruction" to the CIO and each of the four ODT employees. Each memorandum contained remonstrative language and instructions to address policy and behavioral deficiencies. Some also included temporary revisions of recipients' work responsibilities.³ However, we were surprised that each letter specifically disclaimed any disciplinary action, stating, "This letter is not a disciplinary action and will not be placed in your Official Personnel Folder."⁴

¹ CFTC OIG, Investigation into a Potential Information Technology Security Incident, June 27, 2016.

² Letter from Anthony C. Thompson, Executive Director, to A. Roy Lavik, Inspector General, "Response to Investigation into a Potential Information Technology Security Incident," September 20, 2016 [hereinafter "September 20 Letter"].

³ I note, though, that the [REDACTED] who conducted a search of the entire CFTC email system in violation of agency policy retains his position and access. We have received conflicting information regarding the implementation of safeguards that would prevent or detect a future breach.

⁴ We were also quite surprised to learn that a sixth Memorandum of Warning and Instruction was sent to [REDACTED] containing similarly remonstrative language faulting him for failing to live up to standards and practices (regarding the internal reporting of information technology incidents) that, according to our understanding, were not fully in place at the time. The [REDACTED] initial investigation, timely reports to his immediate supervisor, and later cooperation with our investigation aided in the uncovering and reporting of wrongdoing, and we made no findings challenging the propriety of his actions.

With regard to the CIO, while the Chairman's memorandum addressed the CIO's failure to disclose certain information to the CFTC's incident response team, it neither acknowledged nor addressed our findings regarding his affirmative misrepresentations to the incident response team and to OIG investigators.

Retaliation

We recommended that management "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 deficiencies in CFTC operations." The CFTC concurred with our recommendation.⁵

Shortly after receiving the Report, the Chairman sent a memorandum to all CFTC personnel affirming the CFTC's commitment to complying with "all Federal laws, regulations, and agency policies, including those that prohibit retaliation and uphold the fair and equal treatment of Federal employees and contractors who make good faith reports of potential wrong doing."⁶ In November, the CFTC's Executive Director circulated an email to all CFTC personnel "to ensure all agency employees and contractors are aware of and understand prohibited personnel practices and whistleblower protections."⁷ The Chairman and Executive Director's memoranda together summarize the legal framework on whistleblower protection and prohibition of retaliation, direct personnel to relevant resources provided by the U.S. Office of Special Counsel, and urge agency staff to address questions and report wrongdoing to appropriate parties.

The CFTC is currently developing two formal policies relating to retaliation prohibitions, and has also revised Contracting Officer's Representative (COR) training programs to include discussion of retaliation.

CFTC Information Technology Policies

We found that "CFTC's information technology policies and practices need review." The CFTC has made changes to the organization of ODT to consolidate network security operations under the CISO and is revisiting various computer security policies to address deficiencies.⁸

As always, I appreciate your continuing support of my Office.

Attachments

Cc (with attachments): Tony Thompson

⁵ September 20 Letter, p. 2.

⁶ Memorandum from Timothy G. Massad to All CFTC Employees and Contractors, "Anti-Retaliation and Reprisal Statement," July 22, 2016.

⁷ Email from Anthony C. Thompson to [All CFTC Personnel], "CFTC Announcement: Prohibited Personnel Practices and Whistleblower Protections," Nov. 2, 2016.

⁸ We will continue to review the CFTC's IT security efforts as part of our required annual FISMA compliance audits.