Department of Veterans Affairs
Office of Inspector General

Administrative Investigation
Failure to Safeguard and Misuse of VA Equipment and Lack of Candor
Office of Information & Technology
Fayetteville, Arkansas

Redacted

Report No. 10-02858-102 **February 23, 2011**

VA Office of Inspector General
Washington, DC 20420

DEPARTMENT OF VETERANS AFFAIRS
Office of Inspector General
Washington, DC 20420

TO: Deputy Assistant Secretary for Information Security

SUBJECT: Administrative Investigation, Failure to Safeguard and Misuse of VA Equipment and Lack of Candor, Office of Information & Technology, Fayetteville, Arkansas (2010-02858-IQ-0176)

Summary

We substantiated that Mr. Charles Gephart, Director of IT Field Security Operations, Office of Information and Technology (OI&T), violated VA policy when he failed to properly safeguard and to report the theft of a VA-issued laptop computer in September 2007. We also found that he misused his VA-issued computers, cellular telephone, and email to create and send messages and pornographic images to another person and failed to testify freely and honestly about his past behavior and actions.

Introduction

The VA Office of Inspector General (OIG) Administrative Investigations Division investigated allegations that Mr. Gephart "covered up" the theft of a VA-issued laptop computer and misused his VA-issued computer, cellular telephone, and information technology resources for inappropriate activities. To investigate these allegations, we interviewed Mr. Gephart and other OI&T staff; reviewed email, cellular telephone, personnel, travel, and VA information technology records. We also reviewed a local law enforcement report and applicable Federal law, regulations, and VA policy. We investigated another allegation; however, we addressed it in a separate memorandum.

Results

Issue 1: Whether Mr. Gephart Failed to Safeguard and Report the Theft of a VA-Issued Laptop

VA policy states that users of VA information and information systems are responsible for complying with all Department information security program policies, procedures, and practices and reporting all security incidents immediately to the system or facility ISO and their immediate supervisor. They are also required to acknowledge that they read, understood, and agreed to abide by the VA National Rules of Behavior on an annual

basis. VA Directive 6500, Paragraph 3(f), (August 4, 2006). Information Security policy states that VA employees are to protect information technology equipment assigned to them and to implement physical security safeguards to reduce opportunities for its unauthorized access, use, or removal. Policy also states that portable computers having sensitive information stored on them or having software that provides access to VA private networks are to be secured under lock and key whenever the equipment is not in the immediate vicinity of the employee. VA Handbook 6500, Paragraph 6, Policies and Procedures, (September 18, 2007). Further, this policy requires that employees immediately report any incident of theft, loss, or compromise of VA sensitive information or information systems to their Information Security Officer (ISO) and/or Privacy Officer (PO) and to their supervisor. The ISO/PO is then required to report the incident within 1 hour to the VA Network and Security Operations Center (NSOC). If the incident is believed to involve criminal activity, the NSOC must then file a report with VA OIG Hotline. Id., at Paragraph 6(b), Section 10(b).

Mr. Gephart told us that his VA-issued laptop computer was stolen several years ago from his residence [redacted]; however, he said that he could not recall the date of the theft. He said that it occurred on a Friday night and that he discovered and reported it to local law enforcement officials the next morning. He further said that 2 days later, the following Monday, law enforcement officials told him that they recovered the laptop. Mr. Gephart told us that the laptop did not have sensitive information stored on it and that the investigating law enforcement officer told him that the [redacted] who stole it was unable to access its contents, due to the encryption software. Mr. Gephart said that the laptop was later returned to him. **(b)(6)**

A [redacted] Sheriff's Office report reflected that on September 22, 2007, Mr. Gephart reported that his VA-issued laptop computer and encrypted thumb drive, as well as other personally owned items, were stolen from his residence. According to the report, Mr. Gephart initially told the investigating officer that he left the VA equipment in a bag on the front seat of his vehicle which he parked overnight in the driveway of his residence, but he later said that he thought he took the bag out of the vehicle and placed it in his garage overnight. However, Mr. Gephart also reported that he left the garage door partially open. He told the officer that in the past, he had trouble with raccoons entering the garage [redacted] and by keeping the garage door partially open, it kept the raccoons from causing damage. The report further said that the following Monday, September 24, [redacted] who lived nearby reported that she found suspicious items [redacted] These turned out to be the same items that Mr. Gephart reported stolen from his residence. The report documented that the VA laptop and thumb drive were recovered and later released to Mr. Gephart on the afternoon of September 24.

Mr. Gephart said that he reported the theft to his supervisor, the former Deputy Assistant Secretary for Information Protection and Risk Management, and that although he knew

(b)(6)

that he was also required to report the theft to his ISO, he did not. Security Operations Center records, consisting of 34 incident reports dating from midnight September 22 to midnight September 25, 2007, reflected no report of a VA-issued laptop being stolen [redacted]. Further, OIG Hotline records reflected no report of a stolen laptop within 30 days after the reported theft date of September 22.

Mr. Gephart told us that the VA-issued laptop that he kept in his Fayetteville, Arkansas, office was the same one that was stolen and recovered from his residence. We found that the serial number on that laptop matched the one listed in the [redacted] Sheriff's Office report. A forensic review of that laptop revealed that the contents of the entire drive had been wiped.

Conclusion

We concluded that Mr. Gephart failed to follow VA policy when he did not take reasonable measures to safeguard VA-issued equipment in his possession. VA policy required Mr. Gephart to secure his laptop computer whenever it was not within his immediate possession; however, he left it, as well as a VA thumb drive, overnight in his unsecured garage, leaving it unnecessarily exposed to risks greater than those existing in the workplace. Further, Mr. Gephart acknowledged that he failed to make the proper notifications within VA even though he was fully aware of the requirements. Although Mr. Gephart claimed that he reported the theft to his immediate supervisor, he admitted that he failed to notify his ISO. As the Director of OI&T's IT Field Security Operations, Mr. Gephart was fully aware of the reporting requirements in cases of theft of VA IT assets. While his failure to make the proper internal notifications within VA may have at the time saved him from some embarrassment or possible disciplinary actions, his decision to not properly notify VA officials, especially in light of the May 2006 massive breach of VA data, resulted in VA not being able to respond to the situation in real time, to conduct the necessary risk assessments, and to properly notify OIG. Moreover, his former supervisor, the Deputy Assistant Secretary for Information Protection and Risk Management, also had a responsibility to ensure that the theft of VA assets was properly reported to the ISO and OIG. However, since this individual is no longer with VA, we made no recommendations for appropriate administrative action.

Recommendation 1. We recommend that the Deputy Assistant Secretary for Information Security take appropriate administrative action against Mr. Gephart for his failure to follow VA policy.

Issue 2: Whether Mr. Gephart Misused VA-issued Equipment and IT Resources

Standards of Ethical Conduct for Employees of the Executive Branch state that an employee has a duty to protect and conserve Government property and shall not use such property, or allow its use, for other than authorized purposes. 5 CFR § 2635.704(a). VA policy states that employee conduct, on or off the job, which reflects adversely on the

Federal Government as the employer, may be grounds for disciplinary action in addition to whatever penalty is prescribed by law. VA Handbook 5025, Part III, Paragraph 5 (April 15, 2002). VA policy also requires that employees conduct themselves professionally in the workplace and to refrain from using Government office equipment, including information technology, for activities that are inappropriate. It expressly prohibits employees from using VA computers and other resources for creating, downloading, viewing, storing, copying, or transmitting sexually explicit or sexually oriented materials. VA Directive 6001, Paragraph 2 (c) (5).

Mr. Gephart told us that he used his VA-issued cellular telephone and his VA-assigned email account to create and send pornographic images to an unidentified person. He said that on Thursday, June 17, 2010, while on official travel, he received what he described as a "benign" email from an individual who supposedly wanted to meet with him to discuss his job. Mr. Gephart said that their messages started out "very casual" with the unknown person asking to meet him for coffee to "pick his brain." He said that the messages escalated when the individual sent him explicit images (photographs) and asked him to comment on them and reciprocate with like-kind images. He said that he "unfortunately" responded. Although they never physically met, Mr. Gephart said that the exchanges continued through June 20 at which point he felt "it got out of control," and he said that he ended the communications. Mr. Gephart told us that he never did anything like that before and that it was out of character for him.

A forensic examination of the hard drives from Mr. Gephart's two VA-issued computers (one laptop and one desktop) and a VA-issued cellular telephone confirmed the existence of email fragments and digital images that were sexually explicit in nature. We found email fragments containing sufficient information to determine that between June 17 and June 22, 2010, Mr. Gephart used his VA-assigned email account to send and receive sexually explicit messages to or from a person with a non-VA email account. VA records that document all email traffic sent between VA and non-VA email accounts reflected that between June 17 and June 22, Mr. Gephart sent 48 email messages to, and received 66 email messages from, that same non-VA email account. Subject lines found in the emails located on Mr. Gephart's VA-issued hard drives matched the subject lines of the email messages reflected in the VA records. In addition, many of Mr. Gephart's emails contained his automated signature to include his official title "Director IT Field Security Operations." Federal regulations state that an employee shall not engage in criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct or other conduct prejudicial to the Government. 5 CFR § 735.203.

In a forensic examination of Mr. Gephart's VA-issued cellular telephone, we found four emails with sexually explicit digital images attached and sent from a non-VA email account on June 20, 2010, using his VA-issued cellular telephone. Mr. Gephart acknowledged that he took the photographs and then sent them to the non-VA personal email account of an unknown person. In a forensic examination of a floppy disk

containing wiping software, *Ontrack Dataeraser*, located in Mr. Gephart's Fayetteville office, we found that this software was used to erase files on his VA-issued desktop computer on June 24, 2010. We also found that Mr. Gephart used a wiping software program, *Windows Cleanup*, on June 21, 2010, to erase files on the VA-issued laptop that he kept at his Washington, DC, office. Mr. Gephart told us that he used the software programs to erase inappropriate emails.

Finally, with respect to his June 2010 activities, Mr. Gephart told us that he never did "anything like that" before and that it was "really out of character" for him and he could not give a reason why he used his VA-issued cellular telephone when he had a personal cellular telephone. Contrary to Mr. Gephart's claims of this being the only time he engaged in this type of activity, a forensic examination recovered additional images and email fragments from his VA-issued cellular telephone reflecting that he engaged in similar activities dating back to 2002. Recovered data showed that he stored messages from his private email account dating back to 2002 on his VA-issued cellular telephone, with some of these emails containing sufficient text to determine that they were sexually explicit communications between Mr. Gephart, using his private email account, and an unidentified individual's private email account. While the VA-issued cellular telephone was not used to create and send the older emails, it was used to access and store them. Additional recovered information reflected that Mr. Gephart, in the past, subscribed to email lists from adult websites. Federal regulations state that employees will furnish information and testify freely and honestly in cases respecting employment and disciplinary matters and that willfully inaccurate testimony in connection to an investigation may be grounds for disciplinary action. 38 CFR § 0.735-12.

Conclusion

We concluded that Mr. Gephart misused his VA-issued computers, cellular telephone, and email account to create, store, and transmit sexually explicit messages and images to an unidentified person and that Mr. Gephart used computer wiping software to erase his computer files in an attempt to hide evidence of his misconduct. Further, Mr. Gephart failed to testify freely and honestly. Contrary to what he told us about having never engaged in these activities previously, forensic evidence reflected that he engaged in this type of activity going back to 2002. Mr. Gephart, being the Director of Field Security Operations, was fully aware that his activities violated VA policy, yet, he chose to send 48 messages, some with sexually explicit images, to someone he did not know and with whom he had email contact for only a few hours, demonstrating a level of comfort with this type behavior. Moreover, he sent these email messages, some with attached sexually explicit images, with his official VA title, implying that VA sanctioned or endorsed these activities. Given Mr. Gephart's position and responsibility to ensure the security of VA information systems, his actions, whether on or off-duty, reflected adversely on the VA, and could reasonably cause his supervisors to lose confidence in his ability to properly perform his duties as the Director of IT Field Security Operations.

Recommendation 2. We recommend that the Deputy Assistant Secretary for Information Security take appropriate administrative action against Mr. Gephart for misusing VA-issued equipment and information technology resources and for conduct prejudicial to the Government.

Recommendation 3. We recommend that the Deputy Assistant Secretary for Information Security take appropriate administrative action against Mr. Gephart for not testifying freely and honestly about his past conduct.

Recommendation 4. We recommend that the Deputy Assistant Secretary for Information Security ensure that all VA equipment and information technology systems accessed by Mr. Gephart are examined to ensure that all inappropriate materials are removed.

Comments

The Deputy Assistant Secretary for Information Security concurred with the recommendations and said that appropriate administrative and corrective actions will be taken. The Deputy Assistant Secretary's response can be found in Appendix A. We will follow up to ensure all actions are fully implemented.

(original signed by:)

JAMES J. O'NEILL
Assistant Inspector General for
Investigations

Appendix A

Deputy Assistant Secretary Comments

Department of Veterans Affairs **Memorandum**

Date: February 11, 2011

From: Deputy Assistant Secretary for Information Security (005R)

Subject: **Administrative Investigation, Failure to Safeguard and Misuse of VA Equipment and Lack of Candor, OI&T, Fayetteville, Arkansas**

To: Assistant Inspector General for Investigations (51)

1. The VA Office of Information Technology (OI&T) acknowledges receipt of the Office of Inspector General's draft report. OI&T's response and proposed next steps regarding the recommendations made in the draft report are attached.

2. Thank you for the opportunity to review this draft report and comment on your recommendations. If you have questions or need further information you may contact me at 202-461-6400.

(original signed by:)

Jerry L. Davis

Deputy Assistant Secretary's Comments to Office of Inspector General's Report

The following Deputy Assistant Secretary's comments are submitted in response to the recommendation(s) in the Office of Inspector General's Report:

OIG Recommendation(s)

Recommendation 1. We recommend that the Deputy Assistant Secretary for Information Security take appropriate administrative action against Mr. Gephart for his failure to follow VA policy.

Concur **Target Completion Date:** 04/11/2011

Recommendation 2. We recommend that the Deputy Assistant Secretary for Information Security take appropriate administrative action against Mr. Gephart for misusing VA-issued equipment and information technology resources and for conduct prejudicial to the Government.

Concur **Target Completion Date:** 04/11/2011

Recommendation 3. We recommend that the Deputy Assistant Secretary for Information Security take appropriate administrative action against Mr. Gephart for not testifying freely and honestly about his past conduct.

Concur **Target Completion Date:** 04/11/2011

I concur in recommendations 1 thru 3 to take appropriate administrative action for these various violations. I intend to discuss these matters with the appropriate Human Resources officials and the General Counsel to ensure that the actions taken are appropriate.

Recommendation 4. We recommend that the Deputy Assistant Secretary for Information Security ensure that all VA equipment and information technology systems accessed by Mr. Gephart are examined to ensure that all inappropriate materials are removed.

Concur **Target Completion Date:** 03/11/2011

I concur with this recommendation. I will direct appropriate OI&T staff to examine all VA equipment and information technology systems accessed by Mr. Gephart and ensure that all inappropriate materials are removed.

Appendix B

OIG Contact and Staff Acknowledgments

OIG Contact	Linda Fournier
Acknowledgments	Charles Millard Christopher Holcombe Charles Knorr Leanne Shelly

Appendix C

Report Distribution

VA Distribution

Deputy Secretary (001)
Chief of Staff (00A)
Executive Secretariat (001B)
Deputy Assistant Secretary for Information Security (005R)

To Report Suspected Wrongdoing in VA Programs and Operations:
Telephone: 1-800-488-8244
E-Mail: vaoighotline@va.gov
(Hotline Information: http://www4.va.gov/oig/contacts/hotline.asp)