REPORT OF INVESTIGATION

SUBJECT	CASE NUMBER
(b) (6), (b) (7)(C) United States Marshal (retired) (b) (6), (b) (7)(C)	(b) (6), (b) (7)(C)

OFFICE CONDUCTING INVESTIGATION	DOJ COMPONENT
Detroit Area Office	United States Marshals Service

DISTRIBUTION	STATUS
☒ Field Office CFO	☐ OPEN ☐ OPEN PENDING PROSECUTION ☒ CLOSED
☒ AIGINV	PREVIOUS REPORT SUBMITTED: ☐ YES ☒ NO
☒ Component USMS	Date of Previous Report:
☐ USA	
☐ Other	

SYNOPSIS

The Department of Justice (DOJ) Office of the Inspector General (OIG) initiated this investigation upon the receipt of information from the United States Marshals Service (USMS) Office of Professional Responsibility (OPR) alleging that on (b) (6), (b) (7)(C), the USMS Information Technology Division (ITD) received a security alert from the DOJ Security Operations Center (JSOC) regarding a misuse threshold violation that occurred on (b) (6), (b) (7)(C). The security alert concerned attempts to access Internet sites containing pornography by a laptop computer located at the USMS (b) (6), (b) (7)(C) and assigned to United States Marshal (USM) (b) (6), (b) (7)(C).

During the course of the investigation, the OIG found indications that (b) (6), (b) (7)(C) used his government iPad to search the Internet for terms associated with (b) (6), (b) (7)(C) pornography on the Internet, using other government electronic devices assigned to him. The OIG also found indications that (b) (6), (b) (7)(C) made false statements when questioned about searching the Internet for inappropriate content with his government laptop and iPad by denying having done so. (b) (6), (b) (7)(C)

The OIG investigation substantiated the allegation that (b) (6), (b) (7)(C) misused his government devices by searching for and viewing sexually explicit material on his government laptop and iPad. The OIG investigation substantiated that

DATE	April 9, 2021	SIGNATURE (b) (6), (b) (7)(C)
(b) (6), (b) (7)(C)		
PREPARED BY SPECIAL AGENT		
DATE	April 12, 2021	SIGNATURE William Hannah Digitally signed by WILLIAM HANNAH Date: 2021.04.12 07:29:32 -05'00'
William J. Hannah		
APPROVED BY SPECIAL AGENT IN CHARGE		

[redacted] made false statements during his OIG interview when he denied that he searched for inappropriate content using any of his government devices. [redacted], the OIG was unable to review the sexually explicit material that [redacted] accessed, as that data was overwritten when [redacted] government laptop [redacted] and therefore the OIG was unable to assess whether any of the images [redacted].

Three witnesses from the USMS ITD told the OIG that, based on their forensic work on [redacted] laptop computer, they did not believe the laptop had been infected by a virus, and two of the witnesses opined that the downloading of sexually explicit material from Internet websites by [redacted] laptop had been caused by the user of the laptop. The forensic analysis conducted by the USMS ITD staff showed that searches for several inappropriate sexually explicit websites were conducted while [redacted] was logged onto his government laptop. Additionally, one of the USMS ITD witnesses specifically recalled seeing hundreds of pornographic images that were recreated on a standalone USMS-ITD computer by searching websites previously identified as being observed by [redacted] assigned government laptop. The OIG Cyber Investigations Office (CIO) conducted a forensic analysis of [redacted] government iPad which showed that sexually explicit search terms, including terms [redacted], had been entered by the user. The CIO determined that during the forensic imaging of [redacted] government laptop, [redacted], which resulted in the overwriting of hundreds of previously deleted files and the potential loss of evidence in this matter.

[redacted]

In a voluntary interview, [redacted] falsely told the OIG that he did not search the Internet for any sexually explicit content using any of his government devices, and he did not use search terms [redacted]. [redacted] contended that he had searched for a celebrity, innocently clicked on an image, and afterward his government laptop inadvertently downloaded several pornographic images.

The United States Attorney's Office [redacted] declined criminal prosecution of [redacted].

[redacted] retired from his position at the USMS [redacted]

The OIG has completed its investigation and all criminal and administrative actions are complete. The OIG is providing this report to the USMS for its information.

Unless otherwise noted, the OIG applies the preponderance of the evidence standard in determining whether DOJ personnel have committed misconduct. The Merit Systems Protection Board applies this same standard when reviewing federal agency's decision to take adverse action against an employee based on such misconduct. See 5 U.S.C. § 7701(c)(1)(B); 5 C.F.R. § 1201.56(b)(1)(ii).

ADDITIONAL SUBJECTS

(b) (6), (b) (7)(C)

DETAILS OF INVESTIGATION

Predication

The Department of Justice (DOJ) Office of the Inspector General (OIG) initiated this investigation upon the receipt of information from the United States Marshals Service (USMS) Office of Professional Responsibility (OPR) alleging that on (b) (6), (b) (7)(C), the USMS Information Technology Division (ITD) received a security alert from the DOJ Security Operations Center (JSOC) regarding a misuse threshold violation that occurred on (b) (6), (b) (7)(C). The security alert concerned attempts to access Internet sites containing pornography by a laptop computer located at the USMS (b) (6), (b) (7)(C) and assigned to the United States Marshal (USM) (b) (6), (b) (7)(C) (b) (6), (b) (7)(C).

During the course of the investigation, the OIG found indications that (b) (6), (b) (7)(C) used his government iPad to search the Internet for terms associated with (b) (6), (b) (7)(C) pornography on the Internet, using other government electronic devices assigned to him. The OIG also found indications that (b) (6), (b) (7)(C) made false statements when questioned about searching the Internet for inappropriate content with his government laptop and iPad by denying having done so. (b) (6), (b) (7)(C)

Investigative Process

The OIG's investigative efforts consisted of the following:

Interviews of the following USMS personnel:

- (b) (6), (b) (7)(C), ITD (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C), ITD (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C), ITD (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C), ITD (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C), ITD (b) (6), (b) (7)(C)
- (b) (6), (b) (7)(C), USM, (b) (6), (b) (7)(C) (retired)

Review of the following:

- The OIG Cyber Investigations Office (CIO) report of forensic examination of (b) (6), (b) (7)(C) government laptop, iPhone, and iPad.
- Information from the USMS (b) (6), (b) (7)(C) regarding the imaging of (b) (6), (b) (7)(C) laptop by the USMS ITD.
- (b) (6), (b) (7)(C) .
- (b) (6), (b) (7)(C)
- USMS ITD Security Response procedures.
- Information received from the JSOC regarding the initial incident alert and the search for previous violation records for (b) (6), (b) (7)(C).

(b) (6), (b) (7)(C) Misuse of USMS Information Technology Resources

The information provided to the OIG alleged that on (b) (6), (b) (7)(C), the USMS ITD received a security alert from the DOJ JSOC regarding a misuse threshold violation by (b) (6), (b) (7)(C) that occurred on (b) (6), (b) (7)(C) (JSOC Incident Alert DOJ-(b) (7)(E) per USMS.

There are multiple restrictions on the use of government-issued information technology resources. Federal regulations provide that "[e]mployees may use Government property only for official business or as authorized by the Government." 28 C.F.R. § 45.4(a). Additionally, both DOJ and USMS have policies that prohibit employees from using government computers to, among other things, view and transmit sexually explicit material. DOJ Order 2740.1A, "Use and Monitoring of DOJ Computers and Computer Systems," Section 3c(2)(c), prohibits "[t]he creation, download, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials." USMS Policy Directives, Information Technology, 12.2.1 Rules of Use for USMS Information Technology Resources (USMS Rules of Use) has a similar provision, which prohibits "[o]btaining, viewing, or transmitting sexually explicit material or other material inappropriate to the workplace." USMS Rules of Use, D(2)(a)(2).

The OIG reviewed JSOC Incident Alert DOJ (b) (7)(E) per USMS and determined that on (b) (6), (b) (7)(C) government laptop computer generated over 10,000 blocked inappropriate content sites in addition to several other inappropriate content websites that went unblocked and were recorded as being observed. The JSOC reported to the OIG that no other incidents of wrongdoing were on file for (b) (6), (b) (7)(C). The following terms were included in the JSOC Incident Alert attachment as being searched for and observed by the user of (b) (6), (b) (7)(C) government laptop computer:

(b) (6), (b) (7)(C)

On (b) (6), (b) (7)(C), USMS ITD (b) (6), (b) (7)(C) told the OIG that when (b) (6), (b) (7)(C) government laptop was taken offline, (b) (6), (b) (7)(C) called (b) (6), (b) (7)(C) and made an unsolicited statement that the adult nude pictures that were on his laptop were there by accident, caused by (b) (6), (b) (7)(C) inadvertently clicking on "fuzzy images." The following day, (b) (6), (b) (7)(C) asked (b) (6), (b) (7)(C) to come into his office and shut the door. (b) (6), (b) (7)(C) told the OIG that (b) (6), (b) (7)(C) wanted to know what was going to happen to him, asked (b) (6), (b) (7)(C) if he was in any real trouble, and requested that (b) (6), (b) (7)(C) give him with "the real scoop." (b) (6), (b) (7)(C) said he told (b) (6), (b) (7)(C) that he was following USMS procedure and would have to report his findings to the USMS Headquarters. (b) (6), (b) (7)(C) said that he initiated a (b) (7)(E) per USMS scan on (b) (6), (b) (7)(C) government laptop and determined it contained no viruses.

USMS ITD (b) (6), (b) (7)(C) told the OIG that after they conducted forensic website reviews of the JSOC Internet history log, they concluded the visits to sexually explicit content Internet websites by (b) (6), (b) (7)(C) government laptop were caused by the user and not by a virus directing the machine. Both (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) explained that the amount of time between some of the explicit website downloads was measured in minutes, and not seconds as typically seen with a computer virus. Furthermore, the date and time of (b) (6), (b) (7)(C) sign-in logs corresponded with the inappropriate website activity, indicating that he was logged into his computer at the time the explicit materials were searched for and viewed. (b) (6), (b) (7)(C) said that he specifically recalled seeing hundreds of pornographic images through an analysis of the websites visited by (b) (6), (b) (7)(C) government laptop computer, including images of (b) (6), (b) (7)(C) sexually suggestive positions. (b) (6), (b) (7)(C) said that they did not analyze any of the information stored on (b) (6), (b) (7)(C) government electronic devices, as the USMS OPR asked them to stop their examinations and send the devices to the OIG.

The CIO was unable to locate any pornographic images on any of [redacted] government electronic devices, and it was determined that every image in [redacted] government laptop internet cache had been deleted (for reasons discussed below[redacted] The Internet cache was last accessed on [redacted], at 5:24 p.m. by the user. The names of the images included:

[redacted]

The CIO also determined that [redacted] government iPad was used to search for several sexually explicit websites, including:

[redacted]

[redacted]

In a voluntary interview, [redacted] told the OIG that on [redacted], he had worked from approximately 11 a.m. until at least 6 p.m., that he had used his government laptop during that time period, and that he was not aware of anyone else who had accessed or attempted to access his government laptop computer. [redacted] claimed that he did not search for any pornographic content using any of his government electronic devices. However, [redacted] told the OIG that, while using his laptop on [redacted], he clicked on blurred images, which caused nude images to appear on his monitor. [redacted] said that once nude images appeared on his laptop monitor, he closed the webpage and reopened the browser to search for the same images to determine if there was an ongoing problem. [redacted] said that then another full page of nude images reappeared and were displayed on the laptop monitor. [redacted] said that he did not report either of the instances to his supervisors or the USMS ITD because he was embarrassed. [redacted] retired from his position with the USMS [redacted]

OIG's Conclusion

The OIG's investigation concluded that [redacted] misused his government devices in violation of 28 C.F.R. § 45.4(a), DOJ Order 2740.1A, and USMS Policy Directive Information Technology, 12.2.1, when he searched for and viewed sexually explicit material on his government-issued laptop and iPad. Although no nude images were recovered from his government devices (an issue addressed later in this report), an USMS ITD [redacted] who initially examined [redacted] government laptop computer specifically recalled seeing hundreds of pornographic images recreated on a standalone USMS-ITD computer, when conducting an analysis of the websites visited by [redacted]

government laptop computer. Additionally, the JSOC Incident Report and forensic analysis conducted by the USMS and the OIG established that sexually explicit search terms and websites were accessed using (b) (6), (b) (7)(C) government devices. The investigation further revealed that (b) (6), (b) (7)(C) laptop was not affected by a computer virus, and that (b) (6), (b) (7)(C) log-in activity corresponded with the date and time the explicit material was accessed on his computer. (b) (6), (b) (7)(C) the OIG was unable to review the sexually explicit material that (b) (6), (b) (7)(C) viewed and therefore was unable to assess whether any of the images (b) (6), (b) (7)(C).

(b) (6), (b) (7)(C) False Statements

During the investigation, the OIG found indications that (b) (6), (b) (7)(C) made false statements during his interview with the OIG.

Title 18 U.S.C. § 1001(a)(2) provides, in pertinent part, that "whoever, in any matter within the jurisdiction of the executive . . . branch of the Government of the United States, knowingly and willfully . . . makes any materially false, fictitious, or fraudulent statement or representation . . . shall be fined under this title, imprisoned not more than 5 years.

Additionally, USMS Policy Directive, General Management, 1.7(E)(23) Code of Professional Responsibility, directs, in pertinent part: "Do not knowingly give false or misleading statements or conceal material facts in connection with employment, promotion, travel voucher, any record, investigation or other proper proceeding."

The OIG investigation substantiated the allegation that (b) (6), (b) (7)(C) searched for and viewed sexually explicit material on his government devices in violation of federal regulations and agency policies governing the use of government information technology resources.

During his voluntary interview, (b) (6), (b) (7)(C) told the OIG that he had worked on (b) (6), (b) (7)(C), until at least 6 p.m. that day. (b) (6), (b) (7)(C) said that he did not search for anything inappropriate in the web browsers of his government laptop or iPad, and he did not include the words "nude", (b) (6), (b) (7)(C) in any of his searches. (b) (6), (b) (7)(C) said that while he was aware how to do so, he did not delete the Internet cache for his laptop on that date. (b) (6), (b) (7)(C) then said that he knew how to delete the Internet cache on his iPad, but he did not know how to delete the Internet history on his laptop (b) (6), (b) (7)(C) refused to submit to a voluntary OIG-administered polygraph examination, stating that he did not trust polygraph examinations.

The United States Attorney's Office (b) (6), (b) (7)(C) declined criminal prosecution of (b) (6), (b) (7)(C).

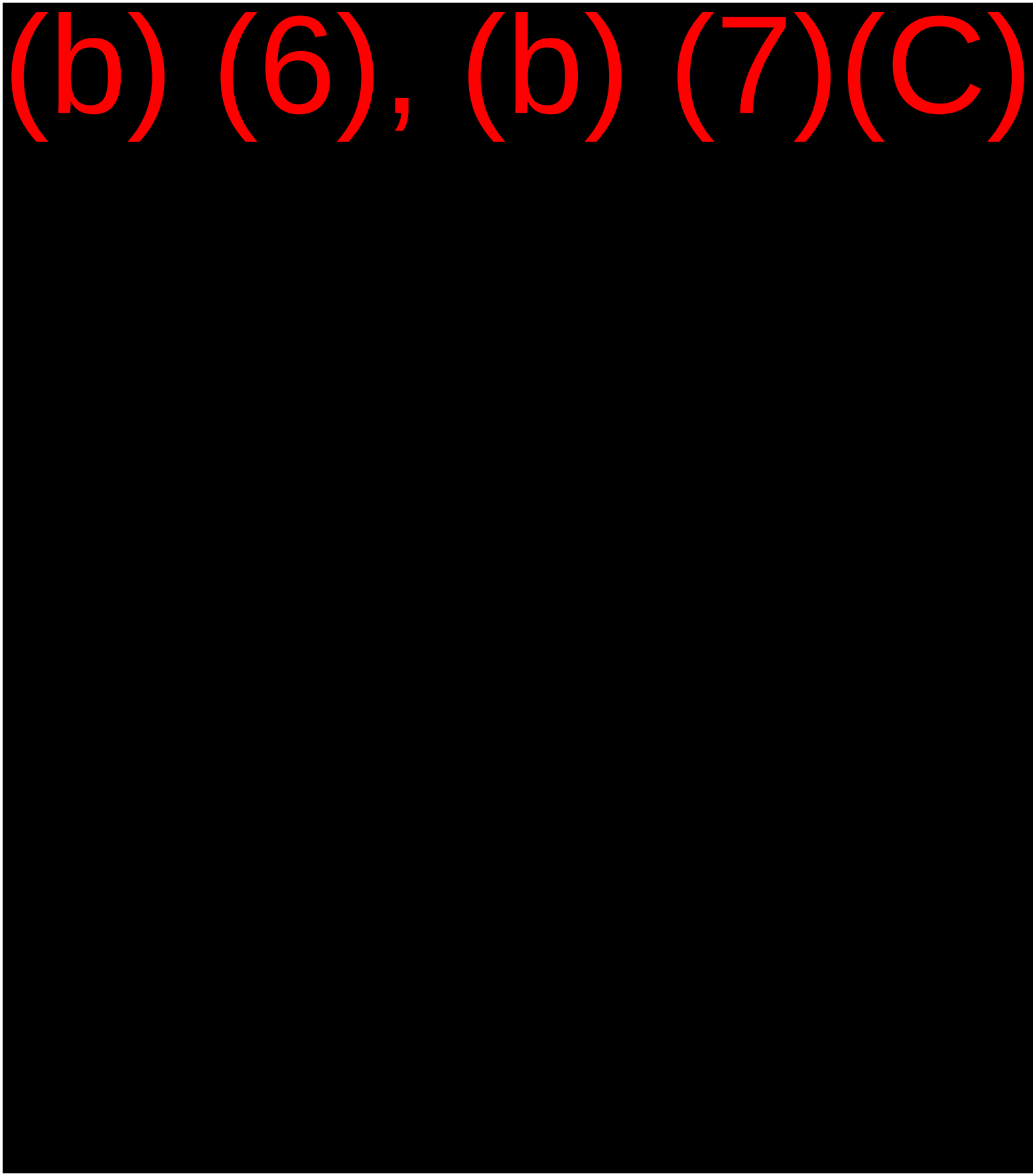
(b) (6), (b) (7)(C) retired from his position at the USMS effective (b) (6), (b) (7)(C).

OIG's Conclusion

The OIG investigation concluded that (b) (6), (b) (7)(C) made false statements during his OIG interview when he denied that he searched for anything inappropriate using his government laptop and iPad. Specifically, (b) (6), (b) (7)(C) falsely stated that he inadvertently "created some kind of portal for pornography" as he searched for celebrities, as he mistakenly clicked on a "blurred" images that appeared on his laptop. (b) (6), (b) (7)(C) also falsely denied using search terms such as "nude," "nudity," or (b) (6), (b) (7)(C) and further denied searching for anything "inappropriate" on his government laptop or iPad. (b) (6), (b) (7)(C) denial is refuted by the JSOC Incident Alert DOJ-(b) (7)(E) per DS, which determined that on (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) government laptop computer generated over 10,000 blocked adult content sites, including using search terms such as "nude," "nudity," and " (b) (6), (b) (7)(C) The JSCO Incident Alert also identified several inappropriate websites that went unblocked and were documented as observed by the user. (b) (6), (b) (7)(C) statements are further contradicted

by OIG CIO forensic analysis, which determined that (b) (6), (b) (7)(C) government iPad was used to search for several sexually explicit websites, and that (b) (6), (b) (7)(C) government laptop Internet cache had been deleted, and was last accessed on (b) (6), (b) (7)(C) at 5:24 p.m. Additionally, USMS ITD (b) (6), (b) (7)(C) concluded the sexually explicit content websites visited by (b) (6), (b) (7)(C) government laptop were generated by the user and not by a virus directing the machine and that (b) (6), (b) (7)(C) sign-in logs corresponded with the date and time of the inappropriate website activity. (b) (6), (b) (7)(C) said that he specifically recalled seeing hundreds of pornographic images through an analysis of the websites believed to have been visited by (b) (6), (b) (7)(C) government laptop computer, including images of (b) (6), (b) (7)(C) sexually suggestive positions. (b) (6), (b) (7)(C) false statements during the OIG interview related to the core misconduct allegation at issue in this investigation and therefore constituted a violation of 18 U.S.C. § 1001(a)(2) and USMS Policy Directive General Management 1.7(E)(23).

(b) (6), (b) (7)(C)


(b) (6), (b) (7)(C)