~~SECRET//NOFORN~~

Investigations Staff

Case Closing Memorandum

I. Administrative Data

Case No.:	17-10122-I	Case Title:	Alleged Computer Misuse
Investigator:	SA	Supervisor:	ASAC
Date Received:	23 May 2017	Date Opened:	1 June 2017
Date Assigned:	1 June 2017	Case Type:	Full Investigation

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

II. Summary of Investigative Actions

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

1. ~~(S//NF)~~ On 23 May 2017 the Office of Inspector General (OIG) received a referral from of an allegation involving Agency contractor assigned to The referral alleged used his Agency Internet Network (AIN) from to post, converse, solicit, and engage in sexual activity with females, The referral further alleged engaged in conversations of a sexual nature with both teenage females and other females whose ages were unknown.

(b)(3) CIAAct
(b)(3) CIAAct
(b)(3) CIAAct
(b)(6)
(b)(7)(c)

2. ~~(S//NF)~~ On OIG initiated an investigation into this matter. The OIG's investigation of this matter included reviews of relevant Agency Records, Office of Security records, and information systems

(b)(3) CIAAct
(b)(6)
(b)(7)(c)
(b)(7)(e)

III. Findings

3. ~~(S//NF)~~ The OIG investigated for violations of Solicitation of a Minor (for sex), VA State Code: §18.2-346, Solicitation of a Prostitute, §18.2-346-18.2-359, Use of Communication Device to Facilitate Offenses Involving Children, §18.2-374.3. Federal Criminal Code; Fraud and Related Activity in Connection with Computers, 18 U.S.C. § 1030, and Agency Regulation (AR) 12-14 – Limited Personal Use of Government Office Equipment/Information Technology.

(b)(3) CIAAct
(b)(6)
(b)(7)(c)
(b)(7)(e)

(b)(3) CIAAct
(b)(3) NatSecAct

~~SECRET//NOFORN~~

(b)(3) CIAAct
(b)(6)
(b)(7)(c)
(b)(7)(e)

(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)
(b)(7)(e)

5. ~~(S//NF)~~ All investigative activity by CIA OIG has been completed. Should additional information be developed, the OIG may consider reopening the matter.

IV. Review and Approval

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

Case Closing Memo submitted by Investigator to Supervisor:

Case Closing Memo approved by Special Agent in Charge:

~~SECRET~~ (b)(3) (b)(7)(c)

Office of Inspector General
Investigations Staff

Case Closing Memorandum

I. Administrative Data

(b)(3) CIAAct
(b)(6)

Case No.:	2013-11352 (b)(7)(c)	Case Title:	OS Crime Report: Child Pornography (b)(3) CIAAct (b)(6)
Investigator:	SA	Supervisor:	SAC (b)(7)(c)
Date Received:	13 May 2013	Date Opened:	13 May 2013
Date Assigned:	28 May 2013	Case Type:	Preliminary Investigation

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

II. Summary of Investigative Actions

(b)(3) NatSecAct

1. ~~(S)~~ On 13 May 2013, the CIA Office of Security informed the Office of Inspector General – Investigations Staff (OIG INV) that during 22 February 2013 and 27 February 2013 interviews, , a contractor , currently working at made admissions of viewing potential child pornography on US government computer systems some time between 2004 and 2006, and again some time between 2009 and 2011.

(b)(6)
(b)(7)(c)

2. ~~(S)~~ self admitted to viewing adult pornography on US government computer systems while employed at indicated he may have accidentally viewed potential child pornography during that time while on government computer systems and/or on personal computer systems.

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

(b)(6)
(b)(7)(c)

3. (U) The CIA Office of Security made referrals of the allegations to the on or about 03 April 2013, as well as to the US Department of Justice on or about 04 April 2013. According to the Office of Security, will be initiating an investigation into the allegations of viewing of potential child pornography with regard to

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

III. Findings

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

(b)(6)
(b)(7)(c)

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

4. ~~(S)~~ According to the Office of Security, was in the process for upgrading to an Industrial Security Staff Approval/Top Secret (ISSA/TS) clearance. As part of this process, was undergoi(b)(3) NatSecAct interviews on 22 February and 27 February 2013, when he made the admissions of viewing adult pornography on US government systems while employed at in the summers of 2004 and 2005. During that time frame admitted to accidently viewing potential

(b)(6)
(b)(7)(c)

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

(b)(3) CIAAct
(b)(3) NatSecAct

~~SECRET~~

15 December 2010

DISPOSITION MEMORANDUM

SUBJECT: (U) Viewing Child Pornography With An Agency-Issued Laptop Computer

CASE: 2010-09815-IG

(b)(3) CIAAct
(b)(6)
(b)(7)(c)
(b)(7)(d)

INTRODUCTION:

1. (~~S//NF~~) On 30 July 2010, [redacted] reported to the Office of Inspector General (OIG) that an Agency employee had viewed child pornography on a US Government (USG) laptop computer. Reportedly, [redacted] made admissions [redacted] that he used his USG laptop computer to view pornographic images and video images of females ages 10 to 16.

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

(b)(3) NatSecAct

SUMMARY:

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

2. (~~C~~) The OIG investigation focused on [redacted] activities from [redacted] entry on duty date, through [redacted]

(b)(6)
(b)(7)(c)

3. (~~C~~) The investigation found that [redacted] first accessed child pornography on his personal computer when he was in college [redacted] The investigation also found that [redacted] continues to view child pornography with his personal computer. The investigation further found that [redacted] used a USG computer to view child pornography [redacted]

(b)(6)
(b)(7)(c)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

[redacted]

(b)(3) CIAAct
(b)(3) NatSecAct

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

~~SECRET//NOFORN~~

4. (~~C~~) OIG interviewed [redacted] who admitted to viewing child pornography with a USG computer [redacted] In a signed sworn statement, [redacted] stated that he viewed pornography on USG-issued laptops, including looking at pictures, thumbnails, and video clips of underage girls as young as 10-12 years of age.

(b)(6)
(b)(7)(c)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

5. (~~C~~) On 23 September 2010, the United States Attorney's Office declined prosecution of [redacted] in favor of administrative action by the Agency.

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(5)
(b)(6)
(b)(7)(c)

6. (~~C~~) On 5 November 2010, a Personnel Evaluation Board (PEB) commended [redacted]

BACKGROUND:

(b)(6)
(b)(7)(c)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

7. (~~C~~) [redacted] was hired by CIA on [redacted] and was a member of the [redacted] Since [redacted] has been assigned to [redacted] and [redacted]

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

8. (~~S//NF~~) [redacted] was in temporary duty (TDY) status from [redacted] was in TDY status from [redacted]

PROCEDURES AND RESOURCES:

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

9. (~~S//NF~~) OIG reviewed [redacted] Official Personnel Folder, security file, Performance Appraisal Reports, Lotus Notes, Agency Internet Network [redacted] OIG conducted a [redacted] review of two Agency laptops computers that [redacted] may have used and a [redacted] review of [redacted] personal laptop computer. OIG interviewed [redacted] OIG also reviewed applicable federal criminal statutes and Agency regulations and policies.

(b)(7)(e)
(b)(7)(e)

(b)(1)
(b)(3) NatSecAct
(b)(7)(e)

~~SECRET//NOFORN~~

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

FINDINGS:

10. (~~S~~) During the interview, said he used a USG laptop to view pornography and that there were approximately five instances in which the pornography depicted individuals between the ages of 14 and 16 engaged in sexual activity. In two of those instances, where the individuals appeared "too young," stated that he watched videos in their entirety.

11. (~~C~~) he provided additional details about viewing pornography on an unclassified USG laptop. stated that he used this laptop to view pornographic images two to three times per night for a total of approximately 100 occasions. Although said the majority of the pornography he viewed was adult pornography, he admitted that on approximately 10-20 occasions he watched videos where the girls appeared to be "middle school aged or about 10-13 years of age." described the girls as being undeveloped with small or no breasts and no hair (presumably no pubic hair).

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

12. (~~S//NF~~) **Denies To The FBI That He Viewed Child Pornography.** On was returning on the flight when he was met by two FBI Agents. After consenting to an interview, told the FBI that he looks at adult pornography in which there are occasions where it is not clear whether the young women are under 18 years old. However, denied viewing pornography involving prepubescent children. consented to a search of his personal laptop computer. A joint FBI and CIA/OIG analysis did not find any child pornography on the laptop.

(b)(1)
(b)(3) NatSecAct
(b)(7)(e)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

13. (~~S//NF~~) **Admissions to OIG.** On 27 September 2010, Special Agents (SA) and interviewed said that he used a USG-issued computer to access pornography while on TDY and continued to access child pornography during his TDYs estimated 10 percent of his browsing of pornography involved viewing underage individuals. The

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

(b)(1)
(b)(3) NatSecAct

youngest individuals he sought out were 13 or 14 years of age but he also encountered 10-12-year-olds. [redacted] said he viewed pornography one to two hours a night during [redacted] TDY and estimated viewing between 50 to 100 images per hour. Ten percent of these images were under age females. [redacted] viewed embedded movies of girls 10 to 12 years of age performing oral sex on an "older guy." In total, [redacted] estimated that he viewed approximately 14,000 images of pornography on his government computer while on his TDYs, of which 1,400 were of underage individuals. Of the 1,400 underage individuals, 280 were under the age of 15. [redacted] also viewed 20 movies of individuals under the age of 18 in which three to five movies were of individuals under the age of 15. [redacted] began viewing underage pornography on his personal computer when he was in college. [redacted] said he has viewed approximately 2,000 images of underage individuals engaged in sexual activity on his home machine, of which 200 to 300 were under the age of 15. At home [redacted] has viewed approximately 200 pornographic movies with individuals under the age of 18, of which 10 videos involved individuals under the age of 15. With respect to being interviewed by the FBI [redacted] said he misunderstood the FBI and thought the FBI was only asking him if he had viewed child pornography while [redacted]

14. ~~(C)~~ [redacted] **Sworn Statement.** On 27 September 2010, [redacted] submitted a statement under oath to OIG. In this statement, [redacted] stated that he used his USG laptop while on TDY to browse pornography [redacted] He said that web searches for pornography eventually led him to a [redacted] site, which in turn, let him see images of younger girls, including girls 10 to 12 years of age. According to [redacted] the majority of images were embedded flash or other video clips of younger girls in "pornographic and oral sexual situations." Of all the pornography that [redacted] viewed during his TDYs, he estimated that roughly 10 percent were underage with 10-20 percent of them being young girls 10-12 years of age. [redacted] stated that he viewed some video clips but states that he watched none of the clips in their entirety.

15. ~~(C)~~ [redacted] **Position on Using a USG Computer to View Pornography.** In his sworn statement, [redacted] said that he recognized it was wrong to use a USG computer to view pornography and that it was

(b)(1) (b)(3) CIAAct (b)(3) NatSecAct (b)(6) (b)(7)(c)

against Agency regulations. He also said that he provided the information voluntarily to OIG and OS. [redacted] said he did not understand that it was a violation of Agency policy to access child pornography until he took the Agency Information Security Course after his TDYs [redacted] said he was drawn to the child pornography sites out of a morbid curiosity and claims that he feels horrible for having viewed images and clips that exploit young people. [redacted] said that he is "truly sorry" for having viewed child pornography with an Agency-issued laptop computer.

16. ~~(C)~~ **Computer** (b)(7)(e) **Analysis.** On 3 August 2010, OIG took custody of a USG laptop computer from OS, which OS believed [redacted] may have used. No child pornography was found on that computer. On 1 September 2010, OIG took custody of seven USG laptop computers from [redacted] to which [redacted] may have had access. However, [redacted] did not have controls, such as individual logins, to indicate who had access to a particular laptop during a specific period of time. OIG was [redacted] one of the laptops [redacted] determined that the one laptop had accessed adult pornography, but there was no indication of child pornography. OIG wiped all seven laptops and returned the laptops to [redacted] On 27 September 2010, [redacted] voluntarily turned over to OIG a laptop computer that he represented was his personal computer. OIG's [redacted] review of this laptop did not find any child pornography. (b)(3) NatSecAct

(b)(1) (b)(3) CIAAct (b)(3) NatSecAct (b)(6) (b)(7)(c)

(b)(3) CIAAct (b)(6) (b)(7)(c)

(b)(1) (b)(3) CIAAct (b)(3) NatSecAct (b)(6) (b)(7)(c)

(b)(3) CIAAct (b)(3) NatSecAct (b)(6) (b)(7)(c)

(b)(3) CIAAct (b)(6) (b)(7)(c)

(U) What Federal Criminal Laws and CIA Regulations Pertain to Accessing Child Pornography?

(b)(1) (b)(3) CIAAct (b)(3) NatSecAct (b)(6) (b)(7)(c)

17. (U//~~FOUO~~) Title 18 U.S.C. § 2252A (*Certain activities relating to material constituting or containing child pornography*) states in pertinent part:

> (a) Any person who—
>
> ....
>
> (5) either—
>
> ....

(B) knowingly possesses, or knowingly accesses with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate of foreign commerce by any means, including by computer . . . .

18. (U) Agency Regulation 7-21, *Limited Personal Use of Government Office Equipment including Information Technology*, states in pertinent part:

(e) Unauthorized Personal Use

...

(6) The creation, downloading, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials.

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

19. (U//~~FOUO~~) On 23 September 2010, OIG presented the findings of this investigation to the United States Attorney for the Eastern District of Virginia. Assistant United States Attorney (b)(6) declined prosecution of [redacted] for viewing child pornography in favor of administrative action by the Agency.

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

20. (~~S~~) On 5 November 2010, a PEB was convened as a result of a rererral from OS that was based on [redacted] admissions. SA [redacted] informed the PEB that [redacted] had admitted to OIG that he, [redacted] had accessed child pornography with his USG laptop computer. SA [redacted] also informed the PEB that [redacted] signed a sworn statement admitting to accessing child pornography with a USG computer.

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

21. (~~C~~) On 5 November 2010, the PEB recommended [redacted]

CONCLUSION:

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

22. (~~C~~) [redacted] appears to have violated federal criminal law and Agency regulations by viewing and possessing child pornography on an Agency laptop computer on multiple occasions.

RECOMMENDATION:

23. (U) In view of the PEB recommendations, it is recommended that this case be closed with no further action.

[redacted]
(b)(3) CIAAct
(b)(6)
(b)(7)(c)
Special Agent

[redacted]
(b)(3) CIAAct
(b)(6)
(b)(7)(c)
for Division Chief

7 January 2011

DISPOSITION MEMORANDUM

SUBJECT: (U) Allegation of Misuse of Government Computer Systems and Sexual Exploitation of Minors

CASE: 2010-09636-IG

(b)(3) NatSecAct
(b)(6)
(b)(7)(c)
(b)(7)(d)

ISSUES UNDER INVESTIGATION:

1. (U//~~FOUO~~) On 8 April 2010, Special Agent (SA) [redacted] contacted the CIA Office of Inspector General (OIG) regarding Agency contractor [redacted] SA [redacted] advised OIG that [redacted] had allegedly solicited an undercover SA from the FBI in an online chat room in an attempt to travel interstate for the purposes of having sex with what he believed to be an underage child.

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

2. (U//~~FOUO~~) OIG investigated [redacted] for violations of Title 18 U.S.C. 2252 (*Certain activities related to material involving the sexual exploitation of minors*).

(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

INVESTIGATIVE EFFORTS:

4. (U//~~FOUO~~) OIG obtained and reviewed [redacted] biographical information and work history.

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

5. (U//~~FOUO~~) OIG obtained and reviewed [redacted] security file.

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

[redacted]

(b)(3) CIAAct
(b)(3) NatSecAct

[redacted]

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

(b)(3) NatSecAct

8. (U//~~FOUO~~) OIG obtained and executed a search warrant for laptop computer.

9. (U//~~FOUO~~) OIG reviewed (b)(3) CIAAct (b)(6) (b)(7)(c) cell phone contact list and recent phone history.

10. (U//~~FOUO~~) OIG reviewed the computer of (b)(3) CIAAct (b)(6) (b)(7)(c) for contacts with

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

11. (U//~~FOUO~~) OIG obtained subpoenas for individuals on Yahoo chat list.

12. (U//~~FOUO~~) OIG obtained subpoenas for the IP addresses associated with chat contacts.

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

13. (U//~~FOUO~~) OIG obtained a search warrant for (b)(3) CIAAct (b)(6) (b)(7)(c) Yahoo chat history.

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

RESULTS:

15. (U//~~FOUO~~) OIG determined that (b)(3) CIAAct (b)(6) (b)(7)(c) was an Agency contractor with the

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

was employed as an Agency contractor through since 24 September 2009.[1]

16. (U//~~FOUO~~) A review of the chat transcripts provided by the FBI indicated that was engaged in a chat with an undercover SA from the FBI (UC) using the account name

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

entered the chat room (b)(6) (b)(7)(c) on (b)(6) (b)(7)(c) and (b)(6) (b)(7)(c)

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

began an instant messaging conversation with UC.

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

17. (U//~~FOUO~~) On 26 February 2010, entered into a conversation with the UC regarding images of young females.

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

20. (~~S//NF~~) OIG traced the IP addresses used by in his communications back to Agency IP addresses

(b)(1)
(b)(3) NatSecAct

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

22. (~~S//NF~~) OIG coordinated with OS

(b)(1)
(b)(3) NatSecAct

OIG obtained a search warrant for computer, and the Department of Justice (DOJ) authorized an exigent seizure of the laptop OIG requested the assistance of declined to assist OIG based on the exigent circumstances finding by DOJ, writing

(b)(1)
(b)(3) NatSecAct

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

24. (U//~~FOUO~~) On 16 April 2010 at 2340 hours, SA and SA met at and requested he return to discuss issues related to his behavior. agreed and was brought to for an interview related to his Internet activities.

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

(b)(3) CIAAct

25. (U//~~FOUO~~) On 17 April 2010, admitted to using the Internet to trade child pornography. stated that he had been dealing with a pornography addiction since he was 8-years-old and that the child pornography was related to that addiction.

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

(b)(7)(e)

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

29. (~~S//NF~~) A [redacted] examination of [redacted] laptop on 17 April 2010 showed that there were no hard drives present. When questioned, [redacted] indicated that he had removed the hard drives and thrown them away [redacted] A search of [redacted] failed to yield any laptop hard drives.

(b)(1)
(b)(3) NatSecAct

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

30. (U//~~FOUO~~) [redacted] laptop was returned and he was driven to a local hotel at his request, following the interview.

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

31. (U//~~FOUO~~) A review of [redacted] phone records indicated that he had placed a call to [redacted]

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

[redacted] laptop showed that [redacted] was seeking Agency employment as a [redacted] No indication of child pornography was found with [redacted]

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

[redacted]

DISPOSITION:

(b)(3) NatSecAct

33. (U//~~FOUO~~) On 19 April 2010, [redacted] received a declination from the Eastern District of Virginia US Attorney's Office regarding [redacted] for lack of evidence. The District of Columbia US Attorney's Office agreed to re-open the case in their district if any future physical evidence was found.

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

34. (U//~~FOUO~~) On 27 April 2010, OS revoked [redacted] clearances and his contract with the Agency was terminated.

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

35. (U//~~FOUO~~) The case is being closed and will be re-opened in the future if there is any receipt of physical evidence of [redacted] activities.

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

Special Agent

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

Acting Supervisory Special Agent

22 January 2008

DISPOSITION MEMORANDUM

SUBJECT: Child Pornography

CASE: 2005-7858-IG

(b)(1)
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

INTRODUCTION:

1. (~~S~~) In December 2004, an Agency laptop computer and several flash drives were found unattended at [redacted] The computer and associated electronic media were sent from [redacted] to Agency Headquarters where they were examined to determine if the computer or electronic media contained classified information. During the review, images of possible child pornography were discovered. The review was terminated and the computer and electronic media were turned over to the Office of Inspector General (OIG). The CIA/OIG determined that the last person who had possession of the computer and associated electronic media was [redacted] an Agency employee.

(b)(1)
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

2. (~~C~~) At OIG's request, the FBI reviewed the images from the Agency equipment and determined there were images of child pornography. On 21 November 2005, the FBI provided an Eastern District Court of Virginia (EDVA) Assistant United States Attorney (AUSA) with its conclusion that at least 10 images of child pornography had been found on Agency-owned equipment.[1]

---

1 (U//~~AIUO~~) At the request of OIG, the FBI did not provide the AUSA the name of the person who was allegedly in possession of the computer and electronic media until EDVA made a decision regarding whether to prosecute.

(b)(3) CIAAct
(b)(3) NatSecAct

Between 21 November 2005 and 16 May 2006, the AUSA made no determination regarding whether EDVA wanted to pursue an investigation of this matter. On 16 May 2006, the FBI advised the AUSA it considered "EDVA's evident lack of prosecutive interest in the matter" to be a declination for prosecution. On 16 May 2006, the FBI closed its case. OIG decided to continue investigation of this matter until it could interview [redacted] regarding the child pornography found on Agency-owned equipment that was once in his possession. [redacted]

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

PROCEDURES AND RESOURCES:

3. (~~C~~) OIG entered an Agency computer and all electronic media associated with this matter into evidence. OIG coordinated with the FBI throughout the portion of the investigation having FBI primacy, interviewed an Agency security chief who had knowledge of how the computer and media came to Agency attention and knowledge of [redacted] involvement with the computer and media. OIG interviewed [redacted] OIG was unsuccessful in its attempts to coordinate its investigative activities, regarding [redacted] with [redacted], the AUSA assigned to this case. [redacted] did not respond to contact overtures made by OIG.

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

(b)(6)
(b)(7)(c)

(b)(6)
(b)(7)(c)

FINDINGS:

4. (~~S~~) In December 2004, an Agency laptop computer and other electronic media associated with the laptop was found unattended at [redacted]

(b)(1)
(b)(3) NatSecAct

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)
(b)(7)(e)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)
(b)(7)(e)

5. (U//~~AIUO~~) Between 18 January 2005 and 11 April 2005, OIG performed internal preliminary inquiries and coordinated investigative information with the FBI. On 11 April 2005, OIG met wi(b)(6)d fully briefed FBI Special Agent (SA) (b)(7)(c) (b)(6) (b)(7)(c) regarding this matter. SA reviewed the recovered images provided by OIG, opined the images constituted images of child pornography, and took possession of the images as evidence.

(b)(3) NatSecAct

6. (U//~~AIUO~~) On 29April 2005, the FBI obtained a search warrant to search the Agency computer and media evidence provided by OIG. The warrant was served on the Office of General Counsel, Litigation Division, on 4 May 2005, and was executed by FBI Computer Analysis and Response Team examiner SA The laptop computer and electronic media were released to the FBI for (b)(7)(e) examination.

(b)(6)
(b)(7)(c)

(b)(6)
(b)(7)(c)

7. (U//~~AIUO~~) The FBI completed its examination of the Agency computer and associated electronic media on 12 October 2005, and on 17 October 2005, SA reviewed the examination results. On 21 November 2005, SA provided the evidence to AUSA for an EDVA prosecutive decision. According to SA AUSA felt that EDVA would not prosecute the case, but he wanted to review the matter with his supervisor, AUSA (b)(6) (b)(7)(c)

(b)(6)
(b)(7)(c)

(b)(6)
(b)(7)(c)

(b)(6)
(b)(7)(c)

8. (U//~~AIUO~~) On 1 February 2006, SA contacted AUSA to obtain an update regarding a decision of whether EDVA would prosecute this matter. According to SA AUSA (b)(6) had not yet reviewed the child pornography images (b)(7)(c)

(b)(6)
(b)(7)(c)

(b)(3) NatSecAct

with his supervisor. She said AUSA [redacted] told her that he would review the material and provide her an EDVA decision on the matter by 15 February 2006.

9. (U//~~AIUO~~) On 16 May 2006, SA [redacted] advised AUSA [redacted] that she was transferring to another position and that the FBI planned to close this matter.[3] She advised OIG that AUSA [redacted] had not contacted her regarding a course of action EDVA wanted to take, i.e., decline the case or accept the case for prosecution. According to SA [redacted] she told AUSA [redacted] that she was going to close the case unless he wanted to "do something with it." SA [redacted] said she told AUSA [redacted] that she would notify OIG of the FBI's action to close the case.

10. (U//~~AIUO~~) On 23 May 2006, at the FBI's Office, Falls Church, Virginia, OIG SA [redacted] retrieved the evidence regarding this case from SA [redacted] On 23 May 2006, SA [redacted] entered the equipment into evidence at the OIG.

[redacted]

3 (U//~~AIUO~~) SA [redacted] informed OIG that AUSA [redacted] had not contacted her regarding his prosecutive intent.

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

CONCLUSIONS:

23. ~~(S)~~ (b)(1) (b)(3) CIAAct (b)(3) NatSecAct (b)(6) (b)(7)(c)

(b)(1) (b)(3) CIAAct (b)(3) NatSecAct (b)(6) (b)(7)(c) (b)(1) (b)(3) NatSecAct He says the computer he transported back from is not the computer he initially took with him to said at no time did he download child pornography to an Agency-owned computer, and he has never viewed child pornography. He reported (b)(1) (b)(3) NatSecAct that the computer he brought back to the US was not the computer that he transported to and the computer he transported (b)(1) (b)(3) NatSecAct to was not a computer personally assigned to him.

24. ~~(C)~~ There is insufficient information (b)(7)(e) to (b)(1) (b)(3) CIAAct (b)(3) NatSecAct (b)(6) (b)(7)(c) link or anyone else to the child pornography images found on Agency equipment. There is no further investigative action for OIG in this matter. This case is closed.

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

Special Agent

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

Supervisory Special Agent

(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

9 December 2009

DISPOSITION MEMORANDUM

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

SUBJECT:

CASE: (U) 2008-9086-IG, Child Pornography – ICE Support

ISSUES UNDER INVESTIGATION:

(b)(6)
(b)(7)(c)

1. (~~C~~) On 14 November 2008, CIA Office of Inspector General (OIG) received a referral from Immigration and Customs Enforcement (ICE) Special Agent (SA) regarding an ongoing ICE investigation

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

into purchased child pornography from a commercial provider under investigation by ICE and was referred to CIA OIG once he was identified as an Agency employee.

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

2. (U//~~FOUO~~) Operation Koala, coordinated by Interpol, identified two underage girls in who had been sexually abused on camera by their father. When confronted by authorities, the father admitted to being paid to make sexually explicit movies of his daughters by (b)(6) (b)(7)(c) the proprietor of the Web site

(b)(6)
(b)(7)(c)

paid multiple individuals in return for their filming of sex acts by minors in their custody and then sold the videos on his Web site. took e-mailed requests by members of the Web site, which he used to direct further exploitation videos.

(b)(6)
(b)(7)(c)

(b)(3) CIAAct
(b)(3) NatSecAct

(b)(1) (b)(3) CIAAct (b)(3) NatSecAct (b)(6) (b)(7)(c)

3. (~~C~~) In 2005, Interpol agents identified an individual using the e-mail address [redacted] who purchased three videos from [redacted] The e-mail address was traced back to the home of [redacted] in the United States, and the lead was passed to the Department of Justice (DOJ) and ultimately provided to ICE.

(b)(6) (b)(7)(c)

(b)(1) (b)(3) CIAAct (b)(3) NatSecAct (b)(6) (b)(7)(c)

4. (~~C~~) Following the lead information, ICE SAs confirmed [redacted] purchase of the videos through credit card records, but the information was considered stale for the purposes of obtaining a search warrant. ICE SAs drove to [redacted] home and requested a voluntary interview with him. [redacted] spoke briefly with the SAs, but refused a [redacted]rch of his home and requested an attorney. At that point [redacted] identified himself as an Agency employee, prompting ICE to forward the referral to CIA OIG.

(b)(1) (b)(3) CIAAct (b)(3) NatSecAct (b)(6) (b)(7)(c)

INVESTIGATIVE EFFORTS:

(b)(1) (b)(3) CIAAct (b)(3) NatSecAct (b)(6) (b)(7)(c)

5. (U//~~FOUO~~) CIA OIG contacted the Federal Bureau of Investigation and obtained from them detailed information on Operation Koala received from Interpol, including copies of the e-mail messages from [redacted]

(b)(1) (b)(3) CIAAct (b)(3) NatSecAct (b)(6) (b)(7)(c)

6. (~~C~~) CIA OIG reviewed [redacted] security file [redacted] for any pertinent information. [redacted] communications were also reviewed.

(b)(6) (b)(7)(c)

(b)(1) (b)(3) CIAAct (b)(3) NatSecAct (b)(6) (b)(7)(c) (b)(7)(e)

[redacted]

(b)(1) (b)(3) CIAAct (b)(3) NatSecAct (b)(6) (b)(7)(c) (b)(7)(e)

8. (~~C~~) CIA OIG contacted the DOJ and confirmed that [redacted] was represented for the purposes of interviewing him. In a 17 March 2009 meeting, Assistant US Attorney [redacted] confirmed there w[redacted] no likely criminal prosecution and that administrative action should be pursued.

(b)(6) (b)(7)(c)

(b)(1) (b)(3) CIAAct (b)(3) NatSecAct (b)(6) (b)(7)(c)

[redacted]

(b)(1) (b)(3) CIAAct (b)(3) NatSecAct (b)(6) (b)(7)(c)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

RESULTS:

10. (~~C~~) Through DOJ administrative subpoenas, the e-mail address was conclusively linked to residence. Information from Interpol confirmed the individual using that address purchased videos of three underage individuals engaged in sexual activity (b)(6) (b)(7)(c) All of the girls were from and paid their respective mothers to film the girls in sexually explicit conduct.

(b)(6)
(b)(7)(c)

11. (~~C~~) admitted to purchasing the videos identified in Operation Koala. additionally admitted to having sexual relations with numerous prostitutes overseas to emotionally hurt his then-wif

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)
(b)(7)(e)

DISPOSITION:

12. (~~C~~) When confronted by his component's management with the issues, resigned on (b)(6) in lieu of Agency administrative action being initiated (b)(7)(c)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

(b)(3) CIAAct
(b)(6)
(b)(7)(c)
Special Agent

(b)(3) CIAAct
(b)(6)
(b)(7)(c)
Supervisory Special Agent

22 March 2009

DISPOSITION MEMORANDUM

SUBJECT: (U//~~AIUO~~) Inappropriate Sexual Contact with Children and Importation of Child Pornography

CASE: 2008-9085-IG

ISSUES UNDER INVESTIGATION:

1. (~~S//NF~~) On 13 November 2008, the Office of Security (OS) referred allegations to Office of Inspector General (OIG) (b)(3) CIAAct (b)(6) (b)(7)(c) (b)(7)(e) that [redacted] had inappropriate sexual contact with an eight-year-old female, and an unnamed two-year-old female. [redacted] (b)(3) CIAAct (b)(6) (b)(7)(c) reported the inappropriate sexual contact as occurring in [redacted] Additionally, [redacted] admitted as having downloaded a movie containing child pornography while working [redacted] for the Agency. (b)(1) (b)(3) CIAAct (b)(3) NatSecAct (b)(6) (b)(7)(c)

2. (U//~~AIUO~~) The specific issues under investigation were whether [redacted] was in possession of child pornography in violation of Title 18 U.S.C. § 2252A (*Certain Activities Relating to Material Constituting or Containing Child Pornography*) and whether [redacted] violated Title 18 U.S.C. § 2242 (*Sexual Abuse*). (b)(3) CIAAct (b)(6) (b)(7)(c) (b)(3) CIAAct (b)(6) (b)(7)(c)

[redacted] (b)(3) CIAAct (b)(3) NatSecAct

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

INVESTIGATIVE EFFORTS:

3. (U//~~AIUO~~) OIG obtained CWE and AIN activity records for [redacted] and analyzed both the files present, as well as his Internet and
(b)(3) NatSecAct [redacted] ile usage.
(b)(7)(e)

4. (U//~~AIUO~~) OIG obtained the Lotus Notes e-mails [redacted]
(b)(3) CIAAct [redacted] from [redacted] accounts and analyzed their contents.
(b)(6)
(b)(7)(c)

5. (U//~~AIUO~~) On 17 November 2008, CIA OIG Special Agent (SA) [redacted] interviewed [redacted] (b)(3) CIAAct
(b)(3) CIAAct (b)(6) (b)(7)(c)
(b)(6)
(b)(7)(c)

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

6. (U//~~AIUO~~) On 17 February 2009, CIA OIG SAs [redacted] [redacted] interviewed [redacted] a second time [redacted] [redacted] provided a sworn, written
(b)(3) CIAAct statement following the interview.
(b)(6)
(b)(7)(c)

[redacted]

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)
(b)(7)(d)
(b)(7)(e)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)
(b)(7)(e)

RESULTS:

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

12. (U//~~AIUO~~) As detailed below, admitted to OIG inappropriate sexual contact with one child victim, and inappropriate sexual activity with a second child victim. Additionally, (b)(7)(e) examination confirmed was found to have extensively downloaded child pornography.

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

13. (U//~~AIUO~~) During his 17 November 2008 interview with OIG, admitted to SA that on or about had inappropriate sexual activity with an unidentified two-year-old girl (b)(6) (b)(7)(c)

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

(b)(6)
(b)(7)(c)

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

The Police department was unable to identify the female victim's name.

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

14. ~~(C)~~ In his 17 February 2009 statement to SA admitted to having inappropriate sexual contact with the then six-year-old on two separate occasions.

(b)(6)
(b)(7)(c)

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

18. ~~(C)~~ During his 17 November 2008 interview with OIG, admitted to SA that he had viewed a digital photo containing naked images of a five-year-old and an eight-year-old girl in a bathtub.

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

(b)(7)(e) review of hard drives conducted by OIG confirmed the presence of the photo on his laptop and backup hard drive.

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

19. ~~(S//NF)~~ The majority of the movies identified on [redacted] laptop were copied to multiple backup devices, including external hard drives and a second computer. The original images appear to have been downloaded primarily [redacted] using a government-provided Internet connection. [redacted] confirmed he searched for 12 to 14-year-olds, and confirmed he sought this material looking at sites such as [redacted]

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

20. ~~(S//NF)~~ During his 17 November 2008 interview with OIG, [redacted] confirmed downloading a child pornography video using Limewire during the summer [redacted] According to [redacted] the video contained images of a 14-year-old and an eight-year-old engaging in oral sex with adults. [redacted] stated that [redacted] he deleted the movie shortly after downloading it.

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

21. ~~(S//NF)~~ [redacted] admitted to SA [redacted] during his 17 February 2009 interview with OIG that, in July or August 2008, [redacted] distributed his pornography collection to [redacted]

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)
(b)(7)(d)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

22. ~~(S//NF)~~ [redacted] imported child pornography into the United States when he brought the laptop obtained by OIG during the 17 November 2008 visit to his residence [redacted] confirmed in his 17 November 2008 that he hand carried the laptop on the plane.

(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)
(b)(7)(e)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

24. (U//~~AIUO~~) Based on the OIG (b)(7)(e) examination of electronic media, personal laptop was found to contain movies with child pornography present. Approximately 63 unique movies depicting girls with a developmental state consistent with that of eight to sixteen-year-olds were identified.

(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

DISPOSITION:

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

25. (U//~~AIUO~~) On 7 March 2009, a Personnel Evaluation Board (PEB) was convened at the request of the OS OIG provided (b)(7)(e) reports as input to the proceedings. The PEB voted unanimously to recommend termination of and the revocation of his clearances. (b)(3) CIAAct was terminated and his clearances revoked (b)(6) (b)(7)(c)

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

(b)(6)
(b)(7)(c)

26. (U//~~AIUO~~) On 19 August 2009, Assistant US Attorney of the Eastern District of Virginia US Attorney's Office, declined prosecution of based on taint issues from the information and the lack of previously identified child pornography victims in his videos.

(b)(3) NatSecAct
(b)(7)(e)

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

27. (U//~~AIUO~~) The evidence obtained and found not to contain contraband was shipped back to [redacted] in 19 and 23 February 2009. The evidence containing contraband will be securely destroyed.

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

Special Agent

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

Division Chief

14 January 2010

DISPOSITION MEMORANDUM

SUBJECT: (U//~~AIUO~~) Alleged Computer Misuse

CASE: 2008-9099-IG

(b)(3) NatSecAct
(b)(6)
(b)(7)(c)
(b)(7)(e)

ISSUES UNDER INVESTIGATION:

1. (~~C~~) On 26 November 2008, the Office of Security (OS) Legal notified the Office of Inspector General (OIG) via Lotus Notes that [redacted] staff officer [redacted] reportedly admitted using an unclassified Agency laptop computer and his personal laptop to view adult pornography while on Temporary Duty assignments (TDY) and Permanent Change of Duty Station (PCS) assignments overseas.

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

2. (~~S//NF~~) OS/Legal's information was based on a referral from OS [redacted] (b)(3) CIAAct which detailed admissions that [redacted] used an Agency issued laptop and his personal laptop to connect to the Internet to view adult pornography, bestiality, and images of children that [redacted] stated "appeared to be between the ages of 0 and 17 years old." [redacted] Furthermore, [redacted] stated he acquired pornographic images and vide[redacted] on the Agency laptop and his personal laptop. [redacted]

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

(b)(3) CIAAct
(b)(3) NatSecAct

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

OS Special Investigations Branch did not recover the Agency computer from

3. (~~C~~) The specific issue(s) under investigation was whether the laptop(s) used to view pornography could be retrieved, and if so, if information on the drive(s) indicates misused Agency computers by viewing unauthorized information, and if he was in possession of child pornography. OIG was unable to locate the laptop(s) accessed while on TDY and PCS (b)(3) NatSecAct (b)(7)(e) OIG located the Agency-issued assigned to on and conducted an investigation into personal use of it to determine if has misused this computer (Exhibit A). OIG found no evidence of adult pornography or child pornography on the laptop in the form of tures or movies.

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

INVESTIGATIVE EFFORTS:

5. (~~C~~) OIG reviewed all existing documentation on this matter,

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)
(b)(7)(e)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)
(b)(7)(d)
(b)(7)(e)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

6. ~~(S//NF)~~ OIG interviewed [redacted] on 9 June 2009 and on 16 July 2009. During his initial interview, [redacted] stated he carried his personal laptop on his [redacted] TDY in [redacted] stated he carried an unclassified [redacted] laptop on his [redacted] TDY in [redacted] On each TDY, [redacted]

(b)(1)
(b)(3) NatSecAct

stated he would use a station-provided [redacted] or his personal laptop to view pornography via the Internet in his [redacted] sleeping quarters.

7. ~~(C)~~ [redacted]

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

[redacted] stated he also watched pornographic videos online. The video aspect of the web cam was an added "perk," [redacted] commented.

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

10. ~~(C)~~ estimated that 99.9 percent of the time he accessed and viewed adult pornography and the remaining time child pornography. stated he accidentally clicked on sites but denied deliberately seeking out child pornography. contended that he only viewed the images for a split second a couple times. remarked on those occasions the child images "popped up" randomly and "things hiccupped." further contended he did not view the child pornography for pleasure. explained that child pornography is not his preference. stated he looked at the images and thought they were disgusting and closed out of them. contended the last time he viewed images of children was around

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

12. (~~C~~) When asked if he would voluntarily bring in his personal laptop used overseas to access pornography, [redacted] responded the IBM laptop belonged to his spouse and he would have to obtain her permission. [redacted] queried the legal consequences if the laptop contained incriminating information. [redacted] also pondered how accidental or intentional storage could be discerned. [redacted] decided not to bring in the laptop stating it might be incriminating.

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)
(b)(7)(d)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)
(b)(7)(d)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

(b)(7)(e)

17. (~~C~~) OIG conducted a [redacted] examination of [redacted] hard drive after removing it from the [redacted] computer received as evidence from [redacted] The evidence received was reviewed for the presence child pornography.

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)
(b)(7)(e)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)
(b)(7)(d)

RESULTS:

20. (U//~~AIUO~~) The hard drive was found to contain numerous images of various subject matter but none that appeared to contain adult or child pornography. There were no movies present on the hard drive that appeared to contain adult or child pornography. The Internet browsing history found on the laptop showed no indications of Web sites containing adult pornography. None of the sites visited appeared to be related to child pornography. An additional review of the searches performed using the laptop did not fit the profile of an individual seeking adult or child pornography.

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

DISPOSITION:

22. (~~C~~) The allegations regarding viewing child pornography were based exclusively on admissions (b)(7)(e) An OIG(b)(7)(e) analysis into the allegations determined nothing on the laptop retrieved indicative of viewing child pornography. OIG found no evidence of child pornography on the unclassified laptop issued to and the exact laptops may have accessed prior to while he was TDY and PCS were not located Additionally, no other evidence supporting the allegation was provided.

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

23. (~~C~~) OIG concluded its preliminary review due to a lack of physical evidence supporting the allegation that viewed child pornography. A full investigation is not warranted at this point, pending receipt of any further information. OS Legal has been notified of the final disposition. OS/Legal notified OIG they are going forward with a Crimes Referral to the Department of Justice concerning this matter.

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

24. (~~S~~) OIG referred information concerning possible suitability issues to the Office of Security for any action they deem appropriate. OIG has no further action in this matter.

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

Special Agent

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

Supervisory Special Agent

Exhibit A

Hand Receipt

(Expires one year from loan date)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

Exhibit B

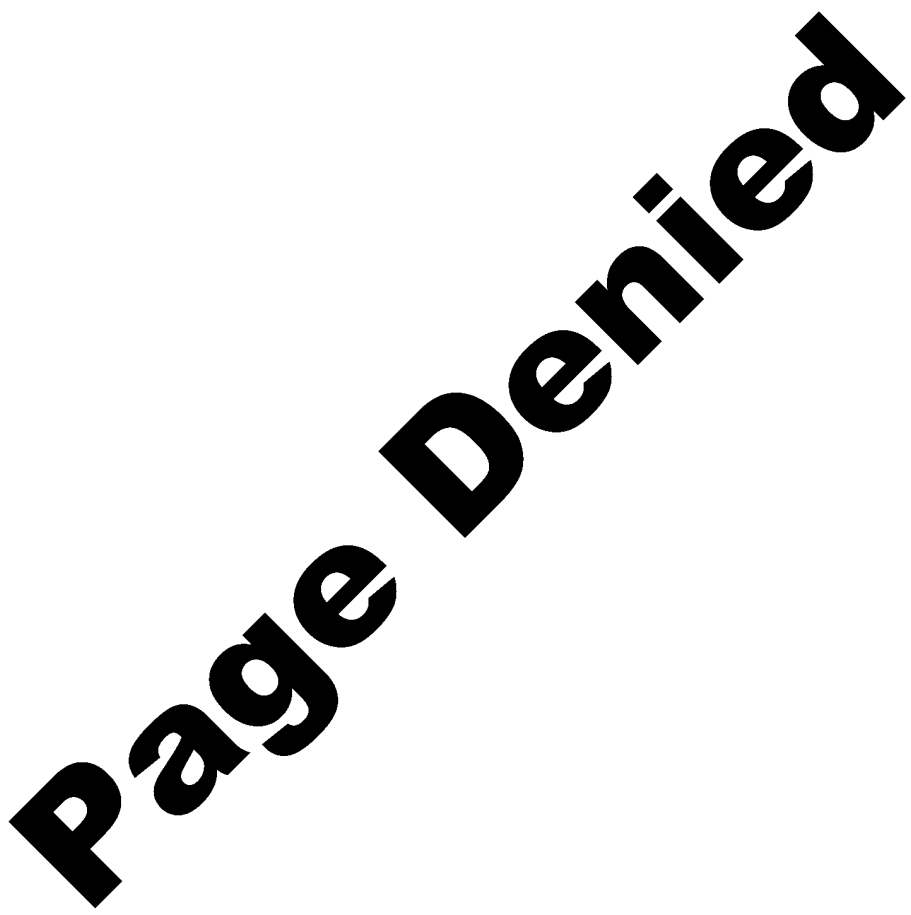
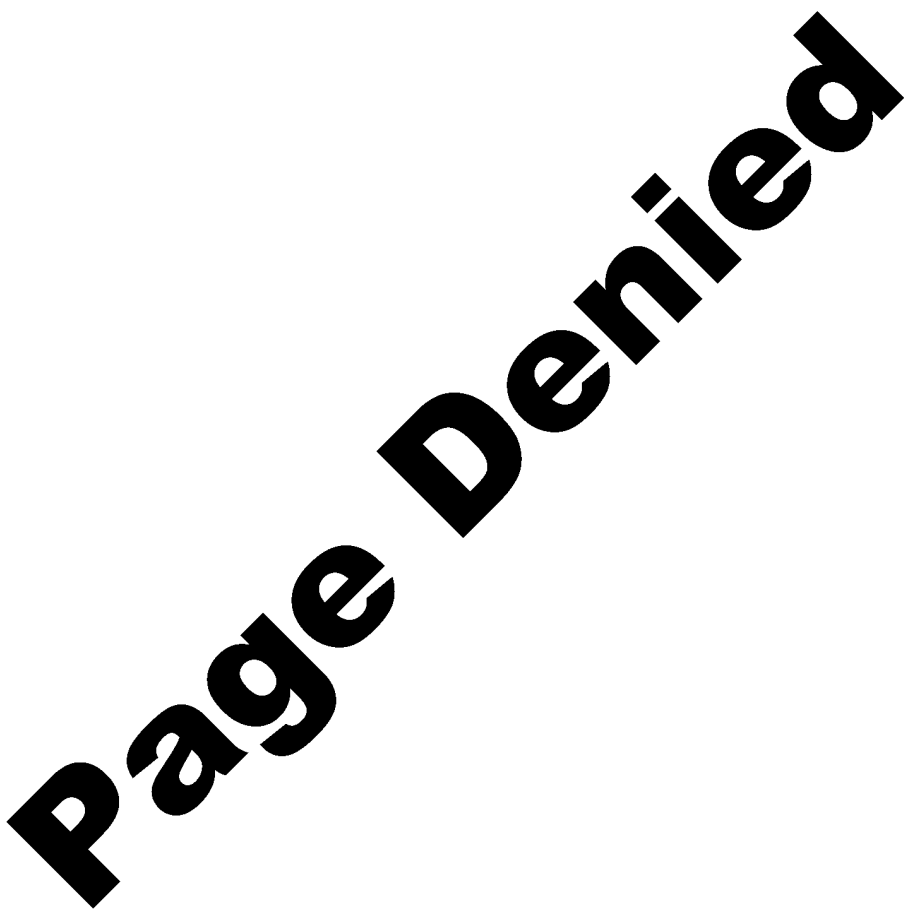
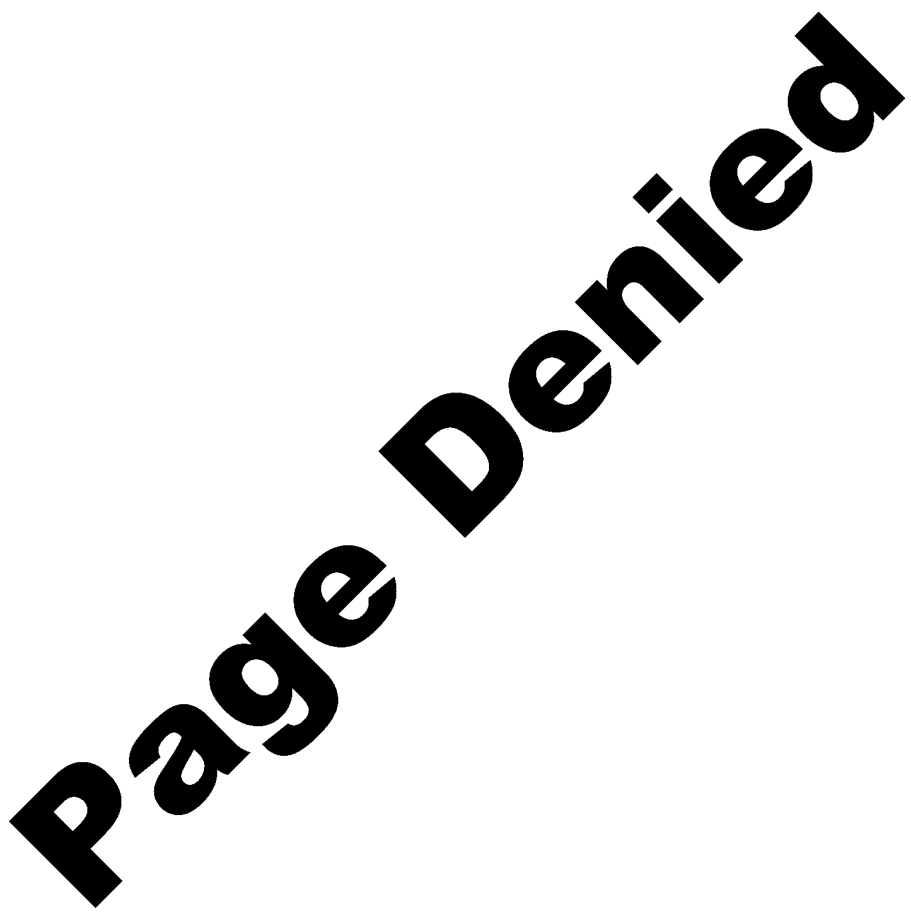


Exhibit C



Approved for Release: 2017/06/29 C06659658



Approved for Release: 2017/06/29 C06659658

~~SECRET~~

19 January 2010

DISPOSITION MEMORANDUM

SUBJECT: (U) Possessing and Creating Child Pornography

CASE: 2009-9458-IG

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

INTRODUCTION:

1. ~~(C)~~ This investigation was initiated on 15 October 2009 based upon an allegation that [redacted] Staff employee, and [redacted] Staff employee, possessed and created child pornography. [redacted] assigned to the [redacted]

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

[redacted] assigned to the [redacted]

2. ~~(S)~~ The allegation first surfaced [redacted] where he admitted that he and [redacted] viewed and created child pornography. From [redacted] the Office of Security (OS) investigated [redacted] and [redacted] for suitability purposes. On 24 September 2009, OS/Legal forwarded a Crimes Report to the Department of Justice (DOJ).

(b)(6)
(b)(7)(c)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)
(b)(7)(e)

[redacted]

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

[redacted]

(b)(3) CIAAct
(b)(3) NatSecAct

[redacted]

~~SECRET~~

(b)(1) (b)(3) CIAAct (b)(3) NatSecAct (b)(6) (b)(7)(c)

(b)(1) (b)(3) CIAAct (b)(3) NatSecAct (b)(6) (b)(7)(c)

According to OS, proceeded to copy the images onto his personal external hard drive and his Agency-issued laptop. OS then noted and used a computer software program to create a DVD that strung the explicit images into video clips.

4. (U//~~AIUO~~) On 16 October 2009, OIG presented this case to the US Attorney's Office (USAO), Eastern District of Virginia (EDVA), for potential prosecution. On 16 November 2009, EDVA declined to prosecute in lieu of administrative action. On 16 November 2009, OIG referred this case back to OS for consideration of further action for suitability purposes.

PROCEDURES AND RESOURCES:

(b)(1) (b)(3) CIAAct (b)(3) NatSecAct (b)(6) (b)(7)(c)

5. (~~C~~) The investigation included the following:

- A review of security files and Agency employee biographical information.
- A review of OS' investigative reports involving
- A presentation of the case to the USAO.

(b)(1) (b)(3) CIAAct (b)(3) NatSecAct (b)(6) (b)(7)(c)

(b)(6) (b)(7)(c)

FINDINGS:

(b)(3) CIAAct (b)(6) (b)(7)(c)

6. (~~S~~) **Initial Complaint.** On 14 October 2009, Supervisory Special Agent received an informational copy of an OS Crimes Reports sent to DOJ. The Crimes Report alleged that and possessed and created child pornography.

(b)(1) (b)(3) CIAAct (b)(3) NatSecAct (b)(6) (b)(7)(c)

(b)(1) (b)(3) CIAAct (b)(3) NatSecAct (b)(6) (b)(7)(c)

OS further documented proceeded to copy the images onto his personal external hard drive and his Agency-issued laptop. OS then noted and used a computer software program to create a DVD that strung the explicit images into video clips.

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)
(b)(7)(e)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)
(b)(7)(e)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)
(b)(7)(e)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)
(b)(7)(e)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

29. (U//~~AIUO~~) On 15 September 2009, SIB referred their case to OS/Legal for review to determine if a DOJ crimes report was warranted. On 24 September 2009, OS/Legal forwarded the crimes report to DOJ.

(b)(6)
(b)(7)(c)

30. (U//~~AIUO~~) **Presentation of the Case.** On 16 October 2009, OIG met with Assistant US Attorney (AUSA) [redacted] USAO/EDVA, to discuss the case. At the conclusion of the meeting, [redacted] said OIG needed to brief his supervisor, AUSA [redacted] USAO/EDVA, to determine if EDVA intended to prosecute the case. On 5 November 2009, OIG formally presented the case to [redacted] and [redacted]

(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)
(b)(7)(e)

(b)(6)
(b)(7)(c)

(b)(6)
(b)(7)(c)

On 16 November 2009, contacted OIG and formally declined to prosecute the case in lieu of administrative action.

(b)(3) NatSecAct
(b)(6)
(b)(7)(c)
(b)(7)(e)

31. ~~(S)~~ **Chronology of Investigative Activity.** The following is a chronology of investigative activity relating to this case:

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)
(b)(7)(e)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)
(b)(7)(e)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

CONCLUSIONS:

32. (~~S~~) On 14 October 2009, OIG obtained an informational copy of an OS crimes report that alleged [redacted] and [redacted] possessed and created child pornography. [redacted] According to OS, [redacted] proceeded to copy the images onto his personal external hard drive and his Agency-

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)
(b)(7)(e)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

issued laptop. OS then noted [redacted] and [redacted] used a computer software program to create a DVD that strung the explicit images into video clips. [redacted]

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

33. (U//~~AIUO~~) On 16 October 2009, this case was referred to the USAO for prosecution, whereupon it was declined on 16 November 2009 in lieu of administrative action.

34. (U//~~AIUO~~) On 16 November 2009, OIG referred the matter back to OS for consideration of further action for suitability purposes.

RECOMMENDATIONS:

35. (U) It is recommended that this case be closed with no further action.

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

Special Agent

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

Division Chief

19 July 2010

DISPOSITION MEMORANDUM

SUBJECT: (~~S//NF~~) Child Pornography (b)(1) (b)(3) CIAAct (b)(3) NatSecAct

CASE: 2009-9429-IG

ISSUES UNDER INVESTIGATION:

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

2. (U//~~AIUO~~) The specific issue under investigation was whether (b)(3) CIAAct (b)(6) (b)(7)(c) accessed child pornography in violation of Title 18 U.S.C. § 2252A (*Certain Activities Relating to Material Constituting or Containing Child Pornography*).

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

(b)(3) CIAAct
(b)(3) NatSecAct

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)
(b)(7)(e)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)
(b)(7)(e)

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

DISPOSITION:

19. (U//~~AIUO~~) On 29 October 2009, the Office of Security revoked clearance and his employment was terminated by (b)(3) CIAAct (b)(6) (b)(7)(c). (b)(3) CIAAct appealed his clearance revocation and was denied.

20. (U) On 4 May 2010, Assistant US Attorney (b)(6) of the Eastern District of Virginia US Attorney's Office, declined prosecution of (b)(3) CIAAct based on prosecutorial discretion.

21. (U//~~AIUO~~) All evidence collected from (b)(3) CIAAct (b)(6) (b)(7)(c) was returned to him on 15 October 2009.

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

Special Agent

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

Division Chief

Office of Inspector General
Office of Investigations

Case Closing Memorandum

I. (U) Administrative Data

Case No.:	2016 - 13337	Case Title:	Alleged Unauthorized Use of USG Computer
Investigator:		Supervisor:	
Date Received:	8 November 2016	Date Opened:	8 November 2016
Date Assigned:	8 November 2016	Case Type:	Full Investigation

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

II. (U) Summary of Investigative Actions

1. (~~S//NF~~) On 08 November 2016, the Office of Inspector General (OIG) received an allegation that staff employee, , utilized a USG computer to view child pornography. This matter was investigated as potential violation(s) of 18 U.S.C. 2252A, 18 U.S.C. 1466A, and AR 4-1.

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

2. (~~S//NF~~) On 08 November, 2016, OIG initiated an investigation into this matter. The OIG's investigation of this matter included

(b)(7)(e)

III. (U) Findings

3. (~~S//NF~~) The OIG's investigation into the allegation of utilizing a USG computer to view child pornography could not be independently corroborated with the predicating information originally referred by the Office of Security;

(b)(3) CIAAct
(b)(6)
(b)(7)(c)
(b)(7)(e)

4. (~~S//NF~~) The OIG investigation until this point, revealed a consistent interest and pattern of conversations, involving sexual activities between adults and minors. Potential security and accountability issues were identified involving

(b)(3) CIAAct
(b)(7)(e)

(b)(3) CIAAct
(b)(6)
(b)(7)(c)
(b)(7)(e)
(b)(1)

(b)(1)
(b)(3) CIAAct
(b)(3) NatSecAct
(b)(6)
(b)(7)(c)
(b)(7)(e)

(b)(3) CIAAct
(b)(3) NatSecAct

Case Closing Memorandum

6. (~~S//NF~~) The findings of this investigation will be referred to the Directorate of Science and Technology (DST) and the Office of Security (OS) for information only. Should additional information be developed, the OIG may consider reopening the matter.

IV. Review and Approval

(b)(3) CIAAct
(b)(6)
(b)(7)(c)

Case Closing Memo submitted by Investigator to Supervisor:

Case Closing Memo approved by Special Agent in Charge:

~~SECRET//NOFORN~~

Office of Inspector General
Investigations Staff

Case Closing Memorandum

I. Administrative Data

(b)(3) CIAAct

Case No.:		Case Title:	Unauthorized Disclosure of Classified
Investigator:	SA	Supervisor:	SAC (b)(3) CIAAct
Date Received:	17 October 2012	Date Opened:	19 October 2012
Date Assigned:	19 October 2012	Case Type:	Full Investigation

II. Summary of Investigative Actions

1. ~~(S//NF)~~ On 17 October 2012, the Office of Inspector General (OIG) received notification from the Office of Security (OS) that (b)(6) had found classified material on personal hard drive seized from (b)(7)(c) e of a former Agency contractor. The classified data was (b)(6) by examiners during their analysis of the hard drive as part of an unrelated investiga (b)(7)(c) hild pornography. The subject was identified as a contractor was terminated and his clearances revoked for misusing government systems related to the sexual exploitation of children.

(b)(3) CIAAct (b)(6) (b)(7)(c) (b)(6) (b)(7)(c) (b)(3) CIAAct (b)(6) (b)(7)(c)

2. ~~(S//NF)~~ The OIG obtained a copy of the data from OS and reviewed it to confirm the classification. The OIG confirmed that documents labeled "Top Secret" were present and contacted the Federal Bureau of Investigation (FBI) to obtain a search warrant to review the computer equipment in the custody The OIG seized the equipment The OIG referred the findings to the FBI and to the Counterintelligence Center (CIC), and supported their investigative efforts. The FBI and CIC stopped providing updates t IG and have not requested assistance from the OIG since that date.

(b)(6) (b)(7)(c) (b)(6) (b)(7)(c) (b)(1) (b)(3) CIAAct (b)(3) NatSecAct (b)(7)(c) (b)(7)(e)

III. Findings

3. ~~(S//NF)~~ On (b)(7)(c) the OIG notified the Department of Justice of the t classified material. On the OIG formally referred the matter to the FBI. On the OIG executed a search warrant for possession of child pornography to seize the computer equipment belonging to that was in the possession of the the

(b)(6) (b)(7)(c) (b)(6) (b)(7)(c)

4. ~~(S//NF)~~

(b)(3) CIAAct (b)(6) (b)(7)(c) (b)(1) (b)(3) CIAAct (b)(3) NatSecAct (b)(7)(c) (b)(7)(e)

(b)(3) NatSecAct

~~SECRET//NOFORN~~

Case Closing Memorandum

- [redacted] personal laptop contained files with personal data including social security numbers, dates of birth, and clearances on [redacted] Agency-affiliated individuals. [redacted]
- [redacted]
- Numerous technical documents related to Agency systems were found on [redacted] laptop.

5. ~~(S//NF)~~ Based on the results of the initial review, OIG referred the matter to the Counterintelligence Center's [redacted] The CIC [redacted] and the FBI began a joint counterintelligence investigation into [redacted] activities. [redacted]

6. ~~(S//NF)~~ On [redacted] the OIG turned over all of the evidence gathered to the FBI at their request. [redacted]

7. ~~(S//NF)~~ Th[redacted]ntified approximately [redacted] classified documents present on [redacted] personal systems, which were confirmed by a subject matter expert [redacted] Additionally, more than [redacted] images allegedly containing child pornography were identified on [redacted] computers. [redacted]

9. ~~(S//NF)~~ On [redacted] pleaded guilty [redacted] counts of possession of child pornography. [redacted] was sentenced [redacted] and registration as a sex offender.

10. ~~(S//NF)~~ On [redacted] the Office of General Counsel notified the OIG that the FBI had executed a search warrant on [redacted] residence and obtained an 8GB flash drive [redacted] The OGC advised that the FBI would be completing the forensic analysis of the flash drive and closing the case, pending the receipt of additional information.

11. ~~(S//NF)~~ The FBI has assumed the investigation as the primary investigative agency and the OIG has not received any requests for additional support since March 2013. As a result of no further OIG investigative activity occurring and the FBI jurisdiction over the case, the OIG is closing this investigation. Should additional information be developed, the OIG may consider reopening the matter.

Case Closing Memorandum

IV. Review and Approval

Case Closing Memo submitted by Investigator to Supervisor: (b)(3) CIAAct 6 Aug 2013
(Sign / Date)

Case Closing Memo approved by Supervisor: (b)(3) CIAAct 6 Aug 2013