INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
RALEIGH RESIDENT AGENCY
3200 BEECHLEAF COURT, SUITE 810
RALEIGH, NC 27604

REPORT OF INVESTIGATION

201102271Z-01-SEP-2011-20CS- (b)(7)(E) **June 11, 2015**

(b)(6)&(7)(C)

DISTRIBUTION
DCIS Headquarters
Southeast Field Office

NARRATIVE

1. This investigation was initiated based on information derived from Defense Criminal Investigative Service (DCIS) Project: Operation Flicker (CCN: 200701199X). As background, in 2007, Immigration and Customs Enforcement (ICE) conducted a national investigation that identified over 5,000 U.S. individuals who subscribed to known child pornography websites. DCIS Project Flicker was initiated in May 2007 to identify any Department of Defense (DoD)-affiliated individuals and provide investigative assistance as needed to ICE. The DCIS, ICE, the Military Criminal Investigative Organizations (MCIOs), and other Federal, State, and Local law enforcement agencies investigated many of these subjects; however, several leads were either not examined or not fully investigated. In late 2010, DCIS Headquarters (HQ) rechecked all U.S. buyer names identified in the original ICE investigation. (b)(6)&(7)(C) Greenville, NC, was identified by DCIS-HQ as a DoD-affiliated individual who may be in need of further investigative activity.

2. Information provided by DCIS-HQ suggested that (b)(6)&(7)(C) subscribed to an Internet site believed to be connected to child pornography on or about May 29, 2007. (b)(6)&(7)(C) utilized the email address (b)(6)&(7)(C) and paid $79.95 to access the Internet site to view child pornography.

3. According to the Reenlistment Eligibility Data Display (REDD) database, (b)(6)&(7)(C) was listed as a former Active Duty and Reserve member of the United States Army. (b)(6)&(7)(C) (b)(6)&(7)(C)

4. On February 9, 2012, the Reporting Agent, Special Agent (SA) (b)(6)&(7)(C) Federal Bureau of Investigations (FBI), and FBI Task Force member (b)(6)&(7)(C) interviewed (b)(6)&(7)(C) During this interview, (b)(6)&(7)(C) admitted that (b)(6)&(7)(C) viewed child pornography and identified the computers that (b)(6)&(7)(C) used to view child pornography. These computers where then seized so that mirror images of the hard drives could be made and analyzed.

5. Agents completed a forensic analysis of (b)(6)&(7)(C) hard drive using the (b)(7)(E) system. This analysis identified 2 depictions of bondage/sadomasochism/violence against children, 26 depictions of pre-pubescent children and 1,110 depictions of children greater than 12 years of age but less than 18 years old.

6. On April 16, 2013, information developed during this investigation was briefed to Assistant United States Attorney (AUSA) (b)(6)&(7)(C) Eastern District of North Carolina. It was determined to pursue state charges with the assistance of the Greenville Police Department. AUSA (b)(6)&(7)(C) agreed to monitor the case for appropriate disposition.

7. On (b)(6)&(7)(C) was indicted on 10 felony counts of Third Degree Exploitation of a Minor (NC 14-190.17A). Assistant District Attorney (b)(6)&(7)(C) handled this case for the State of North Carolina. Subsequently, based on arrest warrant issued stemming from the Pitt county indictment, (b)(6)&(7)(C) in Harnett County, North Carolina.

8. On (b)(6)&(7)(C) entered a guilty plea to five counts of 3rd degree Exploitation of a minor in the State Court of North Carolina. (b)(6)&(7)(C) was subsequently sentenced to 48 months of probation and required to register for 30 years in the sex offender registry.

9. All possible criminal and administrative action has been taken and no fraud vulnerabilities were identified during this investigation. A query was conducted in the Joint Personnel Adjudication System (JPAS) for active clearances held by(b)(6)&(7)(C)with negative results. With the completion of all investigative activities, this investigation is closed with the submission of this report

IDENTITY OF SUBJECT

IDENTIFYING DATA

Name	:	(b)(6)&(7)(C)
Alias	:	
Social Security Number	:	
Date/Place of Birth	:	
Race	:	
Sex	:	
Height	:	Unknown
Weight	:	Unknown
Hair	:	Unknown
Eyes	:	Unknown
Residence	:	(b)(6)&(7)(C)
Employment/Occupation	:	
Telephone	:	Unknown

Prepared by SA (b)(6)&(7)(C) Raleigh Resident Agency

(b)(6)&(7)(C)

APPR: (b)(6)&(7)(C)

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
SAN ANTONIO RESIDENT AGENCY
10127 MOROCCO DRIVE, SUITE 250
SAN ANTONIO, TX 78216

(Investigations)

REPORT OF INVESTIGATION

201102156J-16-AUG-2011-30SA (b)(7)(E) **March 17, 2015**

(b)(6)&(7)(C)

DISTRIBUTION:

DCIS HQ 70CC (SA (b)(6)&(7)(C)
DCIS 30DV (SA (b)(6)&(7)(C)

NARRATIVE

1. On August 16, 2011, this case was initiated based on information derived from DCIS Project: Operation Flicker, Case Number: 200701199X. As background, in 2007, Homeland Security Investigations (HSI) conducted a national investigation that identified over 5,000 U.S. individuals who subscribed to known child pornography websites. Subsequently, in May 2007, DCIS initiated Project: Operation Flicker to identify DoD affiliated individuals. Subject (b)(6)&(7)(C) (b)(6)&(7)(C) San Antonio, TX, was identified as an individual who purchased subscriptions from known child pornography websites.

2. Investigative activity, which included a DODIG Subpoena, search warrant, computer forensic examination, interviews, and coordination with HSI, the Air Force Personnel Operations Agency, and the National Center for Missing and Exploited Children, resulted in confirmation that (b)(6)&(7)(C) was in possession of a laptop computer containing multiple pictures and a video of child pornographic material.

3. On December 13, 2012, pursuant to a subject interview, (b)(6)&(7)(C) admitted to purchasing access to websites containing child pornographic material. (b)(6)&(7)(C) was indicted on one count of Title 18 United States Code (USC), Section 2252(a)(4)(B): Possession of Child Pornography; and one count of 18 USC, Section 2252(a)(4)(B): Access with Intent to View Child Pornography, on (b)(6)&(7)(C)

4. (b)(6)&(7)(C) was arrested on (b)(6)&(7)(C) and pleaded guilty in the U.S. District Court, Western District of Texas, San Antonio, TX, to one count of Possession of Child Pornography in violation of 18 USC 2252(a)(4)(B), on (b)(6)&(7)(C)

5. On (b)(6)&(7)(C) was sentenced to 63 months in federal prison, ordered to pay a $100 special assessment fee, sentenced to 10 years supervised release upon release from prison, ordered to register as a sex offender for life, and ordered to forfeit the laptop computer (b)(6)&(7)(C) used to commit the crime. A DNA sample from (b)(6)&(7)(C) was obtained from the United States Marshall's Service for submission to the Federal Bureau of Investigation database.

6. On March 16, 2015, (b)(6)&(7)(C) Defense Human Resource Activity, confirmed (b)(6)&(7)(C) Secret Security Clearance was suspended on April 18, 2014. A revocation determination by the DoD Central Adjudication Facility remains pending.

7. All appropriate prosecutorial actions have occurred. This investigation is complete and closed with the imposition of sentence and submission of this report. No Fraud Vulnerabilities were identified during the course of this investigation.

IDENTITY OF SUBJECT

	IDENTIFYING DATA
Name Alias Social Security Number Date/Place of Birth Race Sex Height Weight Hair Eyes Residence Employment/Occupation Driver's License Number And Issuing State Education	(b)(6)&(7)(C)

Prepared by: SA (b)(6)&(7)(C) DCIS San Antonio RA

(b)(6)&(7)(C)

APPR: (b)(6)&(7)(C)

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
CYBER FIELD OFFICE, WESTERN RESIDENT AGENCY
4800 MARK CENTER DRIVE, SUITE 14G25
ALEXANDRIA, VIRGINIA 22350-1500

REPORT OF INVESTIGATION

2014000017-02-OCT-2013-70CW- (b)(7)(E) **December 4, 2014**

(b)(6)&(7)(C)

DISTRIBUTION:

DCAA-Ft. Belvoir

NARRATIVE

1. This investigation was initiated based upon information received from (b)(6)&(7)(C) (b)(6)&(7)(C) Defense Contract Audit Agency (DCAA), Ft. Belvoir, VA. (b)(6)&(7)(C) reported that during routine monitoring of DCAA's networks on October 1, 2013, DCAA employee (b)(6)&(7)(C) Palmdale, CA, appeared to be accessing pornographic websites from (b)(6)&(7)(C) unclassified computer that possibly contained pornographic images of children.

2. On October 2, 2013, reporting agent contacted (b)(6)&(7)(C) (b)(6)&(7)(C) DCAA, Ft. Belvoir, VA. (b)(6)&(7)(C) advised that (b)(6)&(7)(C) office is responsible for monitoring DCAA networks at Ft. Belvoir, VA. On October 1, 2013, one of the IA employee's in (b)(6)&(7)(C) office responsible for monitoring their web content filters noticed a high volume of web traffic to/from (b)(6)&(7)(C) DCAA laptop computer. As a result, they remotely connected to (b)(6)&(7)(C) computer and ran a virus scan against it to check if it was infected with a virus that might have been the cause for so much activity to pornographic websites. No viruses were detected. Encase Enterprise was then used to remotely connect to (b)(6)&(7)(C) computer. Over 40,000 files and pictures were found in (b)(6)&(7)(C) Internet Temporary history folder, many of them pornographic, including possibly pornographic images of children.

3. The reporting agent obtained (b)(6)&(7)(C) DCAA laptop. A forensic image was made of the laptop and was subsequently analyzed for possible pornographic images of children. A number of possible images of children were found and were provided to the National Center for Missing and Exploited Children's (NCMEC) Child Victim Identification Program. NCMEC did not find that any of the images from Grant's laptop were pornographic images of children.

4. (b)(6)&(7)(C) was interviewed and (b)(6)&(7)(C) said that (b)(6)&(7)(C) accidently accessed restricted web sites on (b)(6)&(7)(C) government laptop when (b)(6)&(7)(C) was searching the internet for celebrity gossip sites. (b)(6)&(7)(C) said that (b)(6)&(7)(C) does not look at child pornography and this was just a mistake and will never happen again. (b)(6)&(7)(C) has retired from his position at DCAA.

5. AUSA (b)(6)&(7)(C) was briefed on the investigation and the results from the NCMEC. As a result of none of the images from (b)(6)&(7)(C) laptop being identified as child pornography, AUSA (b)(6)&(7)(C) declined the investigation for criminal prosecution.

6. Since there is no loss to the U.S. Government and no criminal activity has been uncovered, this investigation is closed. No judicial or administrative action will occur. There were no fraud vulnerabilities identified during the course of this investigation.

IDENTITY OF SUBJECTS

	IDENIFYING DATA
Name Social Security Number Date/Place of Birth Sex Height Weight Hair Eyes Residence Phone Driver's License Number and issuing state	(b)(6)&(7)(C)

Prepared by (b)(6)&(7)(C) Cyber Crimes Program – Western Region

(b)(6)&(7)(C)

APPR: (b)(6)&(7)(C)

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
CYBER FIELD OFFICE, EASTERN RESIDENT AGENCY
4800 MARK CENTER DRIVE, SUITE 14G25
ALEXANDRIA, VIRGINIA 22350-1500

REPORT OF INVESTIGATION

201101608I-25-MAY-2011-70CE-(b)(7)(E) August 21, 2014

DISTRIBUTION
DCIS Cyber Field Office
Homeland Security Investigations, Bangor, Maine
Maine State Police Computer Crimes, Vassalboro, Maine
U.S. Attorney's Office, District of Maine, Bangor, Maine

Page Number

TABLE OF CONTENTS

SYNOPSIS

The Defense Criminal Investigative Service ("DCIS") initiated this investigation based on information provided by the Department of Homeland Security Investigations, ("HSI"), (legacy U.S. Immigration and Customs Enforcement or "ICE"). (b)(6)&(7)(C) was identified as a result Operation Flicker, a 2006 investigation conducted by ICE that investigated the criminal organization behind approximately 200 websites (member restricted) that hosted child pornography. Payments made by buyers seeking access, and payments to the criminal organization were made via PayPal, which is owned by eBay, Inc. Based on information developed by ICE regarding the U.S. buyers, DCIS identified (b)(6)&(7)(C) as U.S. Department of Defense ("DoD") affiliated individual because of (b)(6)&(7)(C) former military service.

(b)(6)&(7)(C) was interviewed two times during this investigation. In the first interview (b)(6)&(7)(C) denied that (b)(6)&(7)(C) purchased or downloaded child pornography and further consented to the search of (b)(6)&(7)(C) home computer. Subsequent analysis of the forensic image of the hard drive identified pictures consistent with the depiction of child pornography/sexual exploitation of children. Twenty-seven (27) series associated with known child victims of sexual exploitation were identified by the National Center for the Exploitation of Missing Children (b)(6)&(7)(C) was interviewed 8 months later and was asked about the contraband that was found. (b)(6)&(7)(C) denied responsibility and agreed to allow the removal of the hard disk drive for further analysis, which led to finding additional suspicious videos; however, analysts for the National Center for the Exploitation of Missing Children were unable to identify the children depicted.

The case is currently being considered for prosecution by the U.S. Attorney's Office, District of Maine ("USAO-MA").

STATUTES

Title 18 USC § 2252A(a)(5)(B) makes it illegal for someone to knowingly possess, or knowingly access 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 or foreign commerce by any means, including by computer.

For purposes of this report, any individual below the age of 18 will be referred to as a "child" or "minor," any visual depiction of a child or minor engaging in "sexually explicit conduct," as that term is defined in Title 18, U.S.C. § 2256(2)(A), will be referred to as "child pornography."

BACKGROUND

Beginning in 2006, ICE conducted a national investigation that identified several thousand U.S. individuals who bought member-restricted subscriptions to websites hosting child pornography. The ICE investigation identified a criminal organization operating over 200 websites hosting child pornography and established that (1) PayPal was used to process customer payments, (2) specific "Item ID" numbers contained in the PayPal records correlated to the child pornography collections, and (3) that specific email accounts were used by the criminal organization for processing and distributing access.

In May 2007, DCIS initiated an investigative project to determine whether any of the U.S. buyers identified by ICE were affiliated with the DoD. DCIS, ICE, the Military Criminal Investigative Organizations and other Federal, State and Local law enforcement agencies investigated many of the individuals identified as U.S. buyers. In late 2010, DCIS Headquarters checked all U.S. buyer names identified in the original ICE investigation for those buyers who had not been investigated. (b)(6)&(7)(C) was identified because of the apparent PayPal purchases for member restricted access and (b)(6)&(7)(C) DoD affiliation due to active duty (b)(6)&(7)(C) in the U.S. Army between (b)(6)&(7)(C)

NARRATIVE

1. The investigation of (b)(6)&(7)(C) was initiated by DCIS on May 25, 2011 based on information developed during Operation Flicker. (Exhibit 1)

2. On September 17, 2012, a report of investigation (ROI) was prepared administratively transferring the investigation from the DCIS Boston Resident Agency to the DCIS Cyber Field Office. (Exhibit 2)

3. The investigation identified PayPal purchases that were made with (b)(6)&(7)(C) account (b)(6)&(7)(C) for member restricted access to websites that had been previously identified during Operation Flicker. A review of PayPal transactional records demonstrated that (b)(6)&(7)(C) account was used to make purchases for access to member restricted websites between February and April of 2007.

4. Account information maintained by PayPay for the (b)(6)&(7)(C) account contained the following identifying information:

(b)(6)&(7)(C)

5. The information contained in the table which follows, *Table 1*, was distilled from PayPal records associated with (b)(6)&(7)(C) account. During the ICE investigation, Item IDs associated with specific collections of child pornography were identified and cataloged. For example, the

(b)(6)&(7)(C),(7)(E)

6. Based on PayPal transactional records obtained during the ICE investigation, certain business names were identified along with primary email addresses that were used to facilitate payments.

(b)(6),(7)(C)&(7)(E)

7. On October 4, 2012, DCIS coordinated this investigation with the U.S. Postal Inspection Service. The (b)(6)&(7)(C) performed address verification and reported that mail was received at (b)(6)&(7)(C) (b)(6), (b)(7)(C) ME 04640. (b)(6), (b)(7)(C) (b)(6)&(7)(C)) were included as recipients for this PO Box. Information provided suggested that the address (b)(6)&(7)(C) (b)(6), (b)(7)(C) ME (b)(6), (b)(7)(C) was a non-deliverable address. (Exhibit 3)

8. On December 1, 2012, surveillance was conducted in the vicinity of (b)(6), (b)(7)(C) (b)(6), (b)(7)(C) located behind (b)(6), (b)(7)(C) ME. Two vehicles were observed parked adjacent to (b)(6), (b)(7)(C) Records for the license plates indicate the vehicles were registered to (b)(6)&(7)(C) (Exhibit 4)

9. On February 26, 2013, the U.S. Attorney's Office, District of Maine, issued a 2703(f) preservation request to Yahoo!, Inc., for the email account (b)(6)&(7)(C) (Exhibit 5)

10. On March 7, 2013, (b)(6)&(7)(C) was interviewed by law enforcement officers at (b)(6)&(7)(C) residence, (b)(6)&(7)(C) (b)(6)&(7)(C), ME. (b)(6)&(7)(C) was informed regarding the nature of investigation and agreed to answer questions. (b)(6)&(7)(C) confirmed that (b)(6)&(7)(C) was (b)(6)&(7)(C) email address for the last six years. In sum and substance, (b)(6)&(7)(C) denied accessing or possessing child pornography. (b)(6)&(7)(C) provided written consent for the search of the home computer. A forensic evidence image was made of the computer's hard disk drive and the computer was returned to (b)(6)&(7)(C) as agreed. (Exhibit 6)

11. On March 18, 2013, the US DOJ issued a preservation letter for the Compliance Team, Facebook, Inc., 1601 Willow Road, Menlo Park, CA 94025. Note: As of the date of this report of investigation, Facebook records have not been requested. (Exhibit 7)

12. On May 29, 2013, DCIS prepared a Media Analysis Report that details the examination and identification of digital evidence. In addition to findings related to apparent contraband pictures, suspicious website history entries accessed in 2013 were observed, in particular for websites: (b)(7)(E) (Exhibit 8)

13. On April 17, 2013, DCIS submitted Digital evidence to the National Center for Missing Persons and Exploited Children for Child Victim Identification Program, ("CVIP"), and CyberTip line for analysis. (Exhibit 9)

14. On June 14, 2013, the National Center for Missing Persons and Exploited Children reported the results of the CyberTip search. ECD Technical Assistance Request, report ID: TA#71938 identified CT/TA results for (b)(6)&(7)(C) (Exhibit 10)

15. On July 12, 2013, the National Center for Missing Persons and Exploited Children reported the results of the CVIP analysis. ECD Technical Assistance Request, report ID: TA#70812 identified twenty-seven (27) series of known child sexual assault victims based on 110 identified pictures. (Exhibit 11)

16. On (b)(6)&(7)(C) DCIS prepared an Affidavit in Support for a Search Warrant and obtained search authorization from U.S. Magistrate Judge Margaret J. Kravchuk for the Yahoo!, Inc. email account associated with email address (b)(6)&(7)(C) (Exhibit 12)

17. On August 9, 2013, DCIS served the Legal Compliance Team, Yahoo! Inc., with the search warrant. Yahoo!, Inc. returned records on September 10, 2013. (Exhibit 13)

18. On November 22, 2013, (b)(6)&(7)(C) was re-interviewed by law enforcement officers at (b)(6)&(7)(C) home. (b)(6)&(7)(C) maintained throughout that (b)(6)&(7)(C) did not search for or access child pornography. (b)(6)&(7)(C) consented to a search of (b)(6)&(7)(C) computer and a live preview revealed suspicious content involving teenage boys. When asked about the Internet content that (b)(6)&(7)(C) viewed, (b)(6)&(7)(C) explained that (b)(6)&(7)(C)

looked for images of "boys and boys," "boys and men," and "boys and girls," but was not looking for child pornography. (Exhibit 14)

19. On March 10, 2014, DCIS submitted digital evidence to the National Center for Missing Persons and Exploited Children for CVIP analysis. (Exhibit 15)

20. On July 24, 2014, DCIS prepared a second Media Analysis Report that detailed findings and the CVIP results, TA#77941. The suspicious videos submitted after the second interview were not identified in the Child Recognition and Identification System (CRIS). (Exhibit 16)

IDENTITY OF SUBJECTS

		IDENTIFYING DATA
Name	:	(b)(6)&(7)(C)
Alias	:	
Social Security Number	:	
Date/Place of Birth	:	
Race	:	
Sex	:	
Height	:	
Weight	:	
Hair	:	
Eyes	:	
Residence (last known)	:	
Driver's License Number	:	
Issuing State	:	
Education	:	

EVIDENCE

A. Documents

- Pictures, videos and artifacts found during the course of the investigation
- NCMEC reporting
- PayPal business records
- Yahoo!, Inc. business records

B. Witnesses

- DCIS SA (b)(6)&(7)(C) can testify to the statements made to (b)(6)&(7)(C) by (b)(6)&(7)(C)
- HSI SA (b)(6)&(7)(C) can testify to the second statement of (b)(6)&(7)(C)
- DCIS SA (b)(6)&(7)(C) can testify to the media analysis conducted
- A representative from eBay/PayPal can testify about their records
- A representative from Yahoo! Inc. can testify about their records
- A representative from National Center for the Exploitation of Missing Children can testify to the analysis their organization conducted in support of this investigation

STATUS OF INVESTIGATION

The case is currently being considered for prosecution by the U.S. Attorney's Office, District of Maine ("USAO-MA"). This investigation has been coordinated with Homeland Security Investigations, Bangor, ME, the Hancock County Sheriff's Department, and the Maine State Police, Internet Crimes Against Children Unit, Vassalboro, ME.

PROSECUTIVE CONSIDERATIONS

There are no considerations to date.

EXHIBITS

EXHIBIT NO.	DESCRIPTION
1.	DCIS Form 1, May 25, 2011, Case Initiation
2.	DCIS ROI, September 17, 2012, Case Transfer
3.	DCIS Form 1, October 4, 2012, Law Enforcement Coordination with US Postal Inspection Service
4.	DCIS Form 1, December 3, 2012, Surveillance (b)(6)&(7)(C) on December 1, 2013

5. DCIS Form 1, February 26, 2013, Yahoo!, Inc., Electronic Records Preservation

6. DCIS Form 1, March 8, 2013, Interview of (b)(6)&(7)(C) on March 7, 2013

7. US DOJ Memorandum, Preservation Request, Compliance Team Facebook

8. DCIS Form 1, May 29, 2013, Media Analysis Report

9. DCIS Form 1, April 17, 2013, Lead Request to the National Center for the Exploitation of Missing Children

10. TA#71938, June 14, 2013, ECD Technical Assistance Report, National Center for the Exploitation of Missing Children

11. DCIS Form 1, July 12, 2013, TA#70812, ECD Technical Assistance Report, National Center for the Exploitation of Missing Children

12. DCIS Form 1, (b)(6)&(7)(C) Search Warrant Execution

13. DCIS Form 1, September 10, 2013, Yahoo! search warrant return

14. DCIS Form 1, November 26, 2013, Interview of (b)(6)&(7)(C) on November 22, 2013

15. DCIS Form 1, March 10, 2014, Lead Request to the National Center for the Exploitation of Missing Children

16. DCIS Form 1, July 24, 2014, Media Analysis Report

(b)(6)&(7)(C)

Prepared by: (b)(6)&(7)(C) East Coast Cyber Division

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
RALEIGH RESIDENT AGENCY
3200 BEECHLEAF COURT, SUITE 810
RALEIGH, NC 27604

REPORT OF INVESTIGATION

201101744T-15-JUN-2011-20RL- (b)(7)(E) **November 14, 2014**

(b)(6)&(7)(C)

DISTRIBUTION
Southeast Field Office
Regional Desk Officer

NARRATIVE

1. This investigation was initiated based on information derived from Defense Criminal Investigative Service (DCIS) Project: Operation Flicker (CCN: 200701199X). As background, in 2007, U.S. Immigration and Customs Enforcement (ICE) conducted a national investigation that identified over 5,000 U.S. individuals who subscribed to known child pornography websites. DCIS Project Flicker was initiated in May 2007 to identify any Department of Defense (DoD) affiliated individuals and provide investigative assistance as needed to ICE. The DCIS, ICE, the Military Criminal Investigative Organizations (MCIOs), and other Federal, State, and Local law enforcement agencies investigated many of these subjects; however, several leads were either not examined or not fully investigated. In late 2010, DCIS Headquarters (HQ) rechecked all U.S. buyer names identified in the original ICE investigation. (b)(6)&(7)(C) Charlotte, NC, was identified by DCIS-HQ as a DoD affiliated individual who may be in need of further investigative activity.

2. In approximately August 2006 through June 2007, (b)(6)&(7)(C) subscribed to an Internet site believed to be connected to child pornography. (b)(6)&(7)(C) utilized the email address (b)(6)&(7)(C) and on two occasions (b)(6)&(7)(C) paid $77.33to access the Internet site to view child pornography.

3. According to the Reenlistment Eligibility Data Display (REDD) database, (b)(6)&(7)(C) was Active Duty in the United States Army from (b)(6)&(7)(C) (b)(6)&(7)(C) was further listed as Reserve Status in the United States Army from (b)(6)&(7)(C) (b)(6)&(7)(C) No further DoD activities were noted. An inquiry through the DoD Employee Interactive Data System (DEIDS) returned no results for (b)(6)&(7)(C)

4. On November 1, 2011, the Reporting Agent (RA) met with Special Agent (SA) (b)(6)&(7)(C) Homeland Security Investigations (HSI), Charlotte Field Division. The RA and SA (b)(6)&(7)(C) contacted (b)(6)&(7)(C) at (b)(6)&(7)(C) home located at (b)(6)&(7)(C) Charlotte NC. (b)(6)&(7)(C) allowed agents into (b)(6)&(7)(C) home and admitted that (b)(6)&(7)(C) was a frequent viewer of child pornography. (b)(6)&(7)(C) consented to (b)(6)&(7)(C) performing a search of (b)(6)&(7)(C) computer.

5. After conducting a preview of (b)(6)&(7)(C) home computer, HIS SA (b)(6)&(7)(C) obtained enough information to apply for and receive a Federal search warrant for (b)(6)&(7)(C) desktop computer, laptop computer, iPhone and floppy diskette which were identified by (b)(6)&(7)(C) to possibly contain child pornography. This warrant was issued on (b)(6)&(7)(C) , in the Western District of North Carolina in front of the Honorable David C. Kessler. On (b)(6)&(7)(C) the warrant was executed by HIS.

6. An analysis of (b)(6)&(7)(C) computer image was performed and revealed pictures believed to be child pornography (cp). Images were sent to the National Center for Missing and Exploited Children (NCMIC) for analysis and to confirm the identity of any known victims.

7. Additionally, as a result of the interview with (b)(6)&(7)(C) by agents in November 2011, another individual, (b)(6)&(7)(C) was implicated as a criminal co-conspirator involved with child pornography. (b)(6)&(7)(C) was identified as traveling from the state of Washington to North Carolina to visit with (b)(6)&(7)(C) at (b)(6)&(7)(C) residence where (b)(6)&(7)(C) two children reside. This information was coordinated with the Olympia Police Department. As a result, (b)(6)&(7)(C) was investigated and arrested on state charges of possession of depictions of minor engaged in sexually explicit conduct.

8. On September 4, 2012, in the Superior Court of Washington for Thurston County, (b)(6)&(7)(C) (b)(6)&(7)(C) pled guilty to six counts of felony sex offenses. The six counts included two counts of

Possession of Depictions of Minors Engaged in Sexually Explicit Conduct, two counts of Second Degree Child Molestation, and two counts of Voyeurism. (b)(6)&(7)(C) was subsequently sentenced to 116 months in a Washington state prison followed by supervised release. (b)(6)&(7)(C) was also required to join the Offender Registry.

9. During the course of the investigation, case findings were coordinated with the U.S. Attorney's Office in the Western District of North Carolina. Assistant United States Attorney (AUSA) (b)(6)&(7)(C) was assigned to the matter and ultimately determined that the case should be prosecuted through the State of North Carolina District Attorney's Office. The matter was referred and coordinated through Assistant District Attorney (b)(6)&(7)(C)

10. On (b)(6)&(7)(C) was indicted on three counts of 3rd Degree Exploitation of a Minor, an H class felony in the State of North Carolina. On (b)(6)&(7)(C) was arrested by the Mecklenburg Sheriff's Office pursuant to the indictment. At a subsequent initial appearance, (b)(6)&(7)(C) was released with a secure bond of $25,000.

11. On April 29, 2014, (b)(6)&(7)(C) entered a guilty plea to one count of 3rd degree Exploitation of a minor in the State Court of North Carolina. (b)(6)&(7)(C) was subsequently sentenced to 30 months of probation and required to register for the 30 years sex registry.

12. In November 2014 a query was made in the Joint Personnel Adjudication System (JPAS) for (b)(6)&(7)(C) for any clearance information. The query had negative results for active or former clearances.

13. All possible criminal and administrative action has been taken and no fraud vulnerabilities were identified during this investigation. With the completion of all investigative activities, this investigation is closed with the submission of this report.

IDENTITY OF SUBJECT

IDENTIFYING DATA

Name	:	(b)(6)&(7)(C)
Alias	:	
Social Security Number	:	
Date/Place of Birth	:	
Race	:	
Sex	:	
Height	:	
Weight	:	
Hair	:	Unknown
Eyes	:	Unknown
Residence	:	(b)(6)&(7)(C)
Employment/Occupation	:	Unknown
Telephone	:	Unknown

IDENTITY OF SUBJECT

IDENTIFYING DATA

Name	:	(b)(6)&(7)(C)
Alias	:	
Social Security Number	:	
Date/Place of Birth	:	
Race	:	
Sex	:	
Height	:	Unknown
Weight	:	Unknown
Hair	:	Unknown
Eyes	:	Unknown
Residence	:	(b)(6)&(7)(C)
Employment/Occupation	:	Unknown
Telephone	:	Unknown

Prepared by: SA (b)(6)&(7)(C) Raleigh Resident Agency

(b)(6)&(7)(C)

DEPARTMENT OF DEFENSE
OFFICE OF INSPECTOR GENERAL
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
NEW HAVEN RESIDENT AGENCY
ONE CENTURY TOWER
265 CHURCH STREET, SUITE 404
NEW HAVEN, CONNECTICUT 06510-7013

REPORT OF INVESTIGATION

2014000759-03-FEB-2014-10NH-(b)(7)(E)

December 9, 2014

(b)(6)&(7)(C)

Distribution

DCIS Northeast Field Office (10FO)
DCIS HQ Regional Operations (03RO)

2014000759-03-FEB-2014-10NH- (b)(7)(E) December 9, 2014

Narrative:

1. This case was initiated based on information received from the U.S. Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations, (HSI), South Burlington, VT, who identified the titled subject as an individual who has subscribed to known child pornography websites.

2. On (b)(6)&(7)(C) HSI and Vermont State Police executed a U.S. District Court search warrant on the residence of (b)(6)&(7)(C) Colchester, VT. During the execution of the search warrant, known child pornography was identified on several computers and devices at (b)(6)&(7)(C) residence which are owned or controlled by (b)(6)&(7)(C) One of the devices identified by law enforcement Agents was a portable hard drive identified as: Maxtor one touch external hard drive; (b)(6)&(7)(C) The aforementioned device had a green sticker affixed to it stating that it is "unclassified U.S. Army property".

3. During a subsequent interview of (b)(6)&(7)(C) acknowledged that (b)(6)&(7)(C) maintained pornographic images on all the computer devices identified in the residence; but, denied that the aforementioned external hard drive was U.S. Army property. An onsite preliminary scan of the external hard drive labeled "U.S. Army Property" determined that it has known child pornography images on it.

4. Investigative efforts determined that (b)(6)&(7)(C) was employed as (b)(6)&(7)(C) by (b)(6), (b)(7)(C) and (b)(6), (b)(7)(C) held several U.S. Army contracts for software maintenance which (b)(6)&(7)(C) managed. (b)(6)&(7)(C) did not have a security clearance; but, was issued a contractor's Common Access Card (CAC) relative (b)(6)&(7)(C) contractor responsibilities. Following (b)(6)&(7)(C) arrest and termination of employment, (b)(6)&(7)(C) CAC was returned to the DoD.

5. An analysis of U.S Department of Defense (DoD) indices determined that (b)(6)&(7)(C) was not a current member of the U.S. Military; but, had served with the Vermont National Guard and the U.S. Army Reserves, where (b)(6)&(7)(C)

6. It was determined that (b)(6)&(7)(C) was not a subject/target of Project: Operation Flicker.

7. Investigative efforts were unable to determine the origin of the external hard drive seized from (b)(6)&(7)(C) residence which was marked as "unclassified U.S. Army property".

8. Computer forensics personnel from the Vermont State Police determined that the computer evidence seized was indicative of behavior to support charges for possession of child pornography.

9. On (b)(6)&(7)(C) a Grand Jury in the District of Vermont indicted (b)(6)&(7)(C) on 1 count of USC 2252 (a)(4)(B), Possession of Child Pornography.

10. On July 14, 2014, (b)(6)&(7)(C) appeared before U.S. District Court Chief Judge Christina Reiss, District of Vermont, Burlington, VT and pled guilty to 1 count of Possession of Child Pornography.

11. On November 21, 2014, (b)(6)&(7)(C) appeared before U.S. District Court Chief Judge Reiss and was sentenced to 13 months incarceration; 60 months supervised release upon the completion of (b)(6)&(7)(C) incarceration and a $100.00 special assessment.

12. This investigation is closed. All reportable actions have been previously distributed and appropriately annotated in the official file as well as the Case Reporting Investigative Management System.

2014000759-03-FEB-2014-10NH-(b)(7)(E) December 9, 2014

IDENTITY OF SUBJECT

IDENTIFYING DATA

Name:
DPOB:
SSN:
Address:

Height:
Weight:
Position:
Spouse:
Residence Telephone:
Cellular Telephone:

(b)(6)&(7)(C)

Prepared by: (b)(6)&(7)(C) New Haven RA

(b)(6)&(7)(C)

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
INDIANAPOLIS RESIDENT AGENCY
501 PENNSYLVANIA PARKWAY, SUITE 225
INDIANAPOLIS, IN 46280-1377

(Investigations)

REPORT OF INVESTIGATION

201102273B-01-SEP-2011-40IN- (b)(7)(E) **June 17, 2014**

(b)(6)&(7)(C)

DISTR: HSI, Indianapolis, IN (b)(6)&(7)(C)

NARRATIVE

1. This investigation was initiated by the DCIS Denver Resident Agency on August 31, 2011 based on information derived from DCIS Project: Operation Flicker (UID *200701199X*). The DCIS Project, in turn, followed a nation-wide investigation initiated in April 2006 by Homeland Security Investigations (HSI) that identified over 5,000 U.S. individuals who subscribed to known child pornography websites. DCIS Project Flicker was initiated in May 2007 to identify any DoD-affiliated individuals from among the 5,000 individuals identified in HSI Operation Flicker, and to provide investigative assistance as needed to HSI and to the Military Criminal Investigative Organizations.

2. In June 2011, DCIS Headquarters received several referrals from the U.S. Army Criminal Investigations Command (USACIDC) concerning Operation Flicker subjects for whom USACIDC determined it did not have investigatory jurisdiction over. Included with the referrals was one concerning (b)(6)&(7)(C) who was then residing in (b)(6)&(7)(C) and who, according to an inquiry of the Joint Personnel Adjudication System, had a DoD affiliation at the time of the referral.

3. The (b)(6)&(7)(C) referral was forwarded to the DCIS Denver Resident Agency, which initiated this investigation on August 31, 2011.

4. On March 8, 2012, a DoD Inspector General (IG) subpoena was served on eBay/PayPal regarding (b)(6)&(7)(C) accounts. Review of the information received from eBay/PayPal by the Denver Resident Agency initially revealed no links related to known child pornography sites.

5. On December 3, 2012, this investigation was transferred to the DCIS Indianapolis Resident Agency from the DCIS Denver Resident Agency when the DCIS Denver Resident Agency determined that (b)(6)&(7)(C) had moved to Indiana.

6. On December 12, 2012, the reporting agent conducted an inquiry of the Defense Employee Identification Data System (DEIDS) and Reenlistment Eligibility Data Display (REDD) databases, which revealed that (b)(6)&(7)(C) had been a contractor for the U.S. Army from May 20, 2011 through December 14, 2011. According to a records check previously conducted by the Defense Manpower Data Center (DMDC), Seaside, CA, (b)(6)&(7)(C) was also an Army contractor from (b)(6), (b)(7)(C)

7. On December 12, 2012, the reporting agent and SA (b)(6), (b)(7)(C) HSI, Indianapolis, IN, unsuccessfully attempted to interview (b)(6)&(7)(C) at (b)(6)&(7)(C) (b)(6)&(7)(C) IN, which was unoccupied. However; during this attempted knock-and-talk, the reporting agent and SA (b)(6)&(7)(C) observed a handwritten note taped to the front door addressed to the United Parcel Service (UPS) which requested that any packages be left in a second, large mailbox located on the porch. This note was signed by (b)(6)&(7)(C) and two other occupants of the residence.

8. The reporting agent conducted surveillance of (b)(6)&(7)(C) residence on December 13, 2012, December 28, 2012 and January 7, 2013 and observed that the residence appeared to be unoccupied on every occasion.

9. On February 15, 2013, the reporting agent contacted SA (b)(6), (b)(7)(C) DCIS Denver Resident Agency, and obtained the HSI Master Flicker Item ID Listing. The reporting agent reviewed the Master Flicker Item ID Listing and cross-referenced it with the documents previously received from PayPal in response to the IG Subpoena. This was done in order to determine if illegal material was among the items that (b)(6)&(7)(C) ordered, since HSI reported that the vendor used by (b)(6)&(7)(C) was known by HSI to sell both illegal child exploitation material and legal adult pornography.

10. The reporting agent's review confirmed that (b)(6)&(7)(C) credit card was used to purchase illegal child exploitation products between October 16, 2006 and June 12, 2007.

11. The reporting agent's review of the spreadsheet provided with the Operation Flicker referral revealed that (b)(6)&(7)(C) was a resident of Blountville, TN at the time (b)(6)&(7)(C) subscribed to the known child pornography websites.

12. The reporting agent received change of address information from the U.S. Postal Service Office of Inspector General (USPS-OIG), Indianapolis, IN, for (b)(6)&(7)(C) A review of this information revealed that on November 1, 2012, (b)(6)&(7)(C) had previously, submitted a change of address form and listed (b)(6)&(7)(C) new address as (b)(6)&(7)(C) The reporting agent conducted surveillance of this residence, and observed (b)(6)&(7)(C) truck parked at the residence on one occasion.

13. On June 28, 2013, SA (b)(6), (b)(7)(C) and Officer (b)(6)&(7)(C) Fishers Police Department, Fishers, IN unsuccessfully attempted to interview (b)(6)&(7)(C) at (b)(6)&(7)(C) IN residence. Upon departing, SA (b)(6), (b)(7)(C) left a business card at the residence with a note that requested (b)(6)&(7)(C) contact (b)(6)&(7)(C) at (b)(6)&(7)(C) earliest convenience. No response was received.

14. Between June 28 and July 30, 2013, the reporting agent conducted repeated surveillance of the (b)(6)&(7)(C) residence, in both morning and evening hours, which revealed no sign that (b)(6)&(7)(C) continued to occupy the residence.

15. On July 30, 2013, the reporting agent requested an address check from the USPS-OIG to determine if (b)(6)&(7)(C) was still receiving mail at the (b)(6)&(7)(C) address. USPS-OIG review of the USPS Change-of-Address Reporting System (COARS) database revealed that (b)(6)&(7)(C) put in a second change of address on March 11, 2013, which indicated that (b)(6)&(7)(C) new address was (b)(6)&(7)(C) (b)(6)&(7)(C) CO (b)(6), (b)(7)(C)

16. On August 5, 2013, the reporting agent sent a Lead Request to the DCIS Denver Resident Agency which requested that the DCIS Denver Resident Agency locate and interview (b)(6)&(7)(C) with the understanding that the case would be transferred back to the Denver Resident Agency in the event that evidence was developed that (b)(6)&(7)(C) possessed child pornography in Colorado.

17. On August 8, 2013, the DCIS Denver Resident Agency determined that the address reported for (b)(6)&(7)(C) in (b)(6)&(7)(C) CO was for an Extended Stay America Hotel; that (b)(6)&(7)(C) had checked out of the hotel; and that (b)(6)&(7)(C) provided a forwarding address in Indiana.

18. Between August 12 and 17, 2013, the reporting agent attempted to locate (b)(6)&(7)(C) by conducting surveillance at additional addresses reported to be associated with (b)(6)&(7)(C) however, (b)(6)&(7)(C) was not located.

19. On August 14, 2013, the reporting agent conducted another inquiry of DEIDS concerning (b)(6)&(7)(C) and determined that (b)(6)&(7)(C) had been issued a new Common Access Card (CAC) on or about July 17, 2013. The reporting agent requested additional information concerning this CAC; however, no information was located concerning the DoD contractor for whom (b)(6)&(7)(C) allegedly was then employed.

20. On September 27, 2013, the reporting agent contacted the ID Card Branch at the Defense Finance and Accounting Service (DFAS), Indianapolis, IN and determined that (b)(6)&(7)(C) had been re-hired as a DoD contractor and was currently (b)(6)&(7)(C) Subsequently, the reporting agent sent a Lead Request to the DCIS (b)(6)&(7)(C) Post of Duty to interview (b)(6)&(7)(C)

21. On October 23, 2013, (b)(6)&(7)(C) interviewed (b)(6)&(7)(C) (b)(6)&(7)(C) did not admit to possessing child pornography, but gave permission for SA (b)(6), (b)(7)(C) to seize two thumb drives and an external hard drive, which SA (b)(6), (b)(7)(C) seized into evidence and shipped to the reporting agent for forensic review. Although (b)(6)&(7)(C) denied purchasing child pornography, (b)(6)&(7)(C) admitted that the (b)(6)&(7)(C) email address from the Flicker spreadsheet was (b)(6)&(7)(C) also confirmed that the Visa Debit and Discover credit cards used to purchase the items in the Flicker undercover operation were (b)(6)&(7)(C) and (b)(6)&(7)(C) confirmed that the P.O. Box and phone numbers used to purchase the items in the Flicker undercover operation were (b)(6)&(7)(C) Furthermore, (b)(6)&(7)(C) admitted to purchasing pornography (though not child pornography) while utilizing PayPal and with the above mentioned credit cards (b)(6)&(7)(C) also reported that (b)(6)&(7)(C) never reported the theft of either card and stated that (b)(6)&(7)(C) was never the victim of identity theft.

22. During the interview with SA (b)(6), (b)(7)(C) expressed an urgent desire to immediately quit his job with the DoD contractor and immediately return to the U.S. According to SA (b)(6), (b)(7)(C) (b)(6)&(7)(C) planned to depart (b)(6)&(7)(C) and either return to the U.S. or take an alternate assignment in (b)(6), (b)(7)(C) SA (b)(6), (b)(7)(C) and the reporting agent attempted to coordinate an interview with (b)(6)&(7)(C) at his port of entry to the U.S. or in (b)(6)&(7)(C) but these efforts were unsuccessful.

23. On November 4, 2013, the reporting agent received the two thumb drives and external hard drive that SA (b)(6), (b)(7)(C) received from (b)(6)&(7)(C) and entered the items into the Evidence Custody System of the Indianapolis Resident Agency. Later on November 4, 2013, the reporting agent delivered the drives to SA (b)(6), (b)(7)(C) for forensic review in order to obtain a forensic review of the drives to determine if they contained child exploitation materials.

24. SA(b)(6), (b)(7)(C) forensic review of the two thumb drives and external hard drive received from(b)(6), (b)(7)(C) by SA(b)(6), (b)(7)(C) yielded no evidence of child exploitation materials.

25. On December 23, 2013, SA(b)(6), (b)(7)(C) and the reporting agent again unsuccessfully attempted to conduct a knock-and-talk interview of(b)(6)&(7)(C) at the residence located at (b)(6)&(7)(C) (b)(6)&(7)(C) IN, which was confirmed to be(b)(6)&(7)(C) current residence during the interview with(b)(6)&(7)(C) conducted by SA (b)(6), (b)(7)(C) A review of the Consolidated Lead Evaluation and Reporting (CLEAR) database by the reporting agent previously confirmed the property was owned by (b)(6)&(7)(C)

26. Between January and April 2014, the reporting agent conducted numerous surveillances of the residences located at (b)(6)&(7)(C) IN, and at (b)(6)&(7)(C) (b)(6)&(7)(C) IN in an attempt to locate(b)(6)&(7)(C) for a follow-on interview. Although(b)(6)&(7)(C) truck was never observed to be parked at either residence, on two occasions in April 2014, the reporting agent observed a (b)(6)&(7)(C) matching(b)(6)&(7)(C) appearance outside or in the general area of the residence located at (b)(6)&(7)(C)

27. On May 29, 2014, the reporting agent and SA(b)(6), (b)(7)(C) made an unsuccessful attempt to interview(b)(6)&(7)(C) at the residence located at (b)(6)&(7)(C) IN. Upon departing, the reporting agent left a business card at the residence with a note which requested that(b)(6)&(7)(C) contact the reporting agent at(b)(6)&(7)(C) earliest convenience so that the reporting agent could return the hard drive and thumb drives that(b)(6)&(7)(C) had previously provided to SA(b)(6), (b)(7)(C)

28. On May 29, 2014, at 1:10 p.m., the reporting agent received a voicemail from phone number (b)(6)&(7)(C) A review of the voicemail revealed that it was left by (b)(6)&(7)(C) who identified (b)(6)&(7)(C) In the voicemail, (b)(6)&(7)(C) stated that(b)(6)&(7)(C) was temporarily staying at the (b)(6)&(7)(C) residence, which belonged to (b)(6)&(7)(C) (b)(6)&(7)(C), and that(b)(6)&(7)(C) found the note left by the reporting agent for (b)(6)&(7)(C) stated that(b)(6)&(7)(C) had not spoken with (b)(6)&(7)(C) in almost six months but believed that (b)(6)&(7)(C) knew where(b)(6)&(7)(C) was located.

29. On May 29, 2014, at 1:34 p.m. the reporting agent received a voicemail from phone number (b)(6)&(7)(C) This number was previously provided by(b)(6)&(7)(C) to SA(b)(6), (b)(7)(C) as (b)(6)&(7)(C) own phone number; a Google search of this number revealed it was associated with a cell phone that originated in Kingsport, TN (b)(6)&(7)(C) Blountville, TN, 24 miles from Kingsport, TN, at the time(b)(6)&(7)(C) subscribed to the known child pornography websites). A review of the voicemail revealed that it was left by (b)(6)&(7)(C) who identified(b)(6)&(7)(C) as (b)(6)&(7)(C) and the owner of the residence at (b)(6)&(7)(C) In the voicemail, (b)(6)&(7)(C) stated that(b)(6)&(7)(C) did not reside with(b)(6)&(7)(C) but(b)(6)&(7)(C) did receive mail at the address, and(b)(6)&(7)(C) offered to accept the hard drives on(b)(6)&(7)(C) behalf.

30. In two conversations with the reporting agent on the morning of May 30, 2014, (b)(6)&(7)(C) reported that(b)(6)&(7)(C) was (b)(6)&(7)(C) after returning from (b)(6)&(7)(C) and acted "paranoid" and would not want contact with the reporting agent. According to (b)(6)&(7)(C) had left(b)(6)&(7)(C) home and was living on the road, possibly in a camper attached to(b)(6)&(7)(C) pickup truck.(b)(6)&(7)(C) was

aware of the investigation and stated that (b)(6)&(7)(C) was full of remorse for what (b)(6)&(7)(C) had done and no longer used a computer or the internet. (b)(6)&(7)(C) said that (b)(6)&(7)(C) would return the hard drives to (b)(6)&(7)(C) if the reporting agent turned them over to (b)(6)&(7)(C) The reporting agent informed (b)(6)&(7)(C) that (b)(6)&(7)(C) would need to provide authorization in writing, in order to release the drives to another person's custody. (b)(6)&(7)(C) proposed that (b)(6)&(7)(C) could send the reporting agent a fax "from wherever (b)(6)&(7)(C) is" to authorize the release of the drives to (b)(6)&(7)(C) custody. (b)(6)&(7)(C) believed that (b)(6)&(7)(C) would be in touch with (b)(6)&(7)(C) again in the next few days. However, as of this report, no contact had been received from (b)(6)&(7)(C) In that the drives were determined to be of no evidentiary value, disposition thereof will be handled in accordance with Chapter 18, DCIS Special Agent Manual, "*Evidence Custody System.*"

31. In that the potential offenses identified in the Operation Flicker referral occurred in Blountville, TN, which was outside the area of responsibility of the Indianapolis Resident Agency and since no evidence was obtained which indicated (b)(6)&(7)(C) committed an offense within the state of Indiana at any time, there was no proper venue for prosecution of the matter in the state or federal courts in Indiana. Even so, on June 2, 2014, the reporting agent coordinated with AUSA (b)(6)&(7)(C) U.S. Attorney's Office for the Southern District of Indiana (USAO-SDIN), Indianapolis, IN, concerning the (b)(6)&(7)(C) matter. AUSA (b)(6)&(7)(C) confirmed that the USAO-SDIN would decline to prosecute the matter.

32. No further criminal, civil or administrative actions are contemplated and this matter is closed. There were no management control deficiencies identified during the course of the investigation. A copy of this Report of Investigation is provided to HSI, Indianapolis, IN, for information and follow-on action as deemed appropriate by that agency.

IDENTITY OF SUBJECT

IDENTIFYING DATA

Name	:	(b)(6)&(7)(C)
Alias	:	
Social Security Number	:	
Date/Place of Birth	:	
Race	:	
Sex	:	
Height	:	
Weight	:	
Hair	:	
Eyes	:	
Residence	:	
Employment/Occupation	:	
Telephone Number	:	
Driver's License Number and Issuing State	:	
Education	:	

(b)(6)&(7)(C)

Prepared by (b)(6)&(7)(C) Indianapolis Resident Agency

DEPARTMENT OF DEFENSE
OFFICE OF INSPECTOR GENERAL
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
BOSTON RESIDENT AGENCY
JFK FEDERAL BUILDING
55 NEW SUDBURY STREET, SUITE 1325
BOSTON, MA 02203-0131

REPORT OF INVESTIGATION

201100896K-15-FEB-2011-10BN-(b)(7)(E) June 13, 2012

(b)(6)&(7)(C)

DISTRIBUTION
Northeast Field Office
U.S. Attorney's Office, District of Massachusetts

TABLE OF CONTENTS

SYNOPSIS

The Defense Criminal Investigative Service (DCIS) initiated an investigation based on information provided by U.S. Immigration and Customs Enforcement (ICE) that (b)(6)&(7)(C) (b)(6)&(7)(C) had allegedly subscribed to known child pornography web sites. (b)(6)&(7)(C) was identified by DCIS Headquarters (HQ) as an individual affiliated with the U.S. Department of Defense (DoD) because of (b)(6)&(7)(C) work for a DoD contractor. On April 13, 2011 (b)(6)&(7)(C) was interviewed by DCIS agents at (b)(6)&(7)(C) residence in Oxford, MA, and during the interview (b)(6)&(7)(C) admitted to accessing the member restricted websites, which (b)(6)&(7)(C) described as "nudist sites" that contained pictures of children. On April 13, 2011, and again on April 15, 2011, (b)(6)&(7)(C) consented to the search of (b)(6)&(7)(C) residence and allowed the examination of digital media in (b)(6)&(7)(C) possession. The review of digital media has revealed pictures and videos consistent with the depiction of child pornography/sexual exploitation of children. The National Center for the Exploitation of Missing Children (NCMEC), conducted analysis in support of this investigation and from the pictures and videos submitted, identified nineteen (19) series with known sexual exploitation victims.

The case is currently being considered for prosecution by the U.S. Attorney's Office, District of Massachusetts (USAO-MA). Certain investigative techniques used in this investigation are not reportable in this document and will be provided under separate cover.

STATUTES

Title 18, United States Code, Section 2252 makes it illegal for someone to knowingly transport, receive or possess visual depictions that affect interstate commerce of minors engaged in sexually explicit conduct. Title 18 USC Section 2256 (1) defines a "minor" as someone who is under the age of 18 years old. "Sexually explicit conduct" in Section 2256 (2) (A) includes actual or simulated sexual intercourse, bestiality, masturbation, sadistic or masochistic abuse, or lascivious exhibition of the genitals.

BACKGROUND

In 2006 and 2007, special agents assigned to ICE's Child Exploitation Center conducted a national investigation that identified over 5,000 U.S. individuals who subscribed to a known child pornography website known as "Home Collection." The ICE investigation further identified in excess of 200 commercial child exploitation websites. It was learned that individuals accessed the member restricted websites by purchasing access through financial entities on the internet such as PayPal. DCIS accessed information obtained during the ICE investigation to determine whether any individuals identified were affiliated with the DoD. DCIS subsequently identified (b)(6)&(7)(C) as a "DoD affiliated individual," who from (b)(6)&(7)(C) (b)(6)&(7)(C) was employed by (b)(6), (b)(7)(C) in Connecticut, a government contractor that provided services to the DoD. (b)(6)&(7)(C) also had applied for a security clearance and, among other positions, worked for (b)(6), (b)(7)(C) with mainframe computers. (b)(6)&(7)(C) was separated from service with (b)(6), (b)(7)(C) on (b)(6)&(7)(C)

NARRATIVE

Location, Identification, and Interview of (b)(6)&(7)(C)

1. The DCIS investigation involving (b)(6)&(7)(C) was initiated February 15, 2011. At the time it was believed that (b)(6)&(7)(C) lived in Norwich, Connecticut, given (b)(6)&(7)(C) prior employment with CSC. It was later determined that on or about June 1, 2009, after retiring from (b)(6)&(7)(C) resided in Oxford, Massachusetts. *Exhibit 1* is the Report of Investigation (ROI), dated April 14, 2011, prepared in conjunction with the transfer of the investigation from the DCIS New Haven Resident Agency (RA) to the DCIS Boston RA, and, is hereby incorporated by reference.

2. On April 13, 2011, DCIS agents interviewed (b)(6)&(7)(C) and confirmed that (b)(6)&(7)(C) was employed by (b)(6), (b)(7)(C) from (b)(6)&(7)(C) *Exhibit 2* is the report pertaining to the initial contact and interview of (b)(6)&(7)(C) at (b)(6)&(7)(C) Oxford, MA. (b)(6)&(7)(C) now sells items that (b)(6)&(7)(C) finds on eBay and uses PayPal as a way to make internet purchases. (b)(6)&(7)(C) also enjoys building, updating, and repairing computers. (b)(6)&(7)(C) lives alone and was in exclusive control of the computers located in (b)(6)&(7)(C) residence. (b)(6)&(7)(C) primary email address was (b)(6)&(7)(C) and this was the email address (b)(6)&(7)(C) used to access PayPal services. When (b)(6)&(7)(C) lived in Norwich, Connecticut, (b)(6)&(7)(C) used a different email, possibly (b)(6)&(7)(C) Agents presented (b)(6)&(7)(C) with PayPal transaction history records. *Exhibit 3* lists the eBay/PayPal records related to (b)(6)&(7)(C) purchases of access to the member restricted websites that forms the basis for investigation. Indicated within the transaction history were records that between 2006 and 2007, (b)(6)&(7)(C) PayPal account was associated with the purchase of subscriptions from websites hosting contraband content. (b)(6)&(7)(C) did not immediately recall visiting the "Angel Collection" or "Home Collection," but after (b)(6)&(7)(C) reviewed the eBay/PayPal records (b)(6)&(7)(C) said that (b)(6)&(7)(C) paid to access "nudist sites" where (b)(6)&(7)(C) viewed "bare ass kids."

3. (b)(6)&(7)(C) said that subscriptions to these "nudist sites" were paid through PayPal and that upon subscribing (b)(6)&(7)(C) would receive a username and password. (b)(6)&(7)(C) explained how (b)(6)&(7)(C) was able to view thumbnail pictures on the website and then select and download files containing the pictures (b)(6)&(7)(C) was interested in viewing on (b)(6)&(7)(C) computer. Some of the pictures, (b)(6)&(7)(C) said, included children who appeared to be between the ages of six and fifteen. (b)(6)&(7)(C) made a point to say that the pictures (b)(6)&(7)(C) downloaded and viewed on (b)(6)&(7)(C) computer were not of boys, but were of female children, not engaged in sexual acts. (b)(6)&(7)(C) said that the member restricted website also had pictures of older girls with men. (b)(6)&(7)(C) said that in order to view the pictures (b)(6)&(7)(C) downloaded the files and saved them to a folder on (b)(6)&(7)(C) computer, and that after (b)(6)&(7)(C) viewed the pictures (b)(6)&(7)(C) deleted the files. (b)(6)&(7)(C) denied storing or collecting, transferring or distributing child pornography. (b)(6)&(7)(C) said that the last time (b)(6)&(7)(C) viewed the member restricted websites was about three years ago and that the pictures were boring to (b)(6)&(7)(C) because they were of "nude kids not in sexual acts." (b)(6)&(7)(C) identified the ACER desktop computer, adjacent to a Hewlett Packard desktop computer in (b)(6)&(7)(C) living room, as the computer used at the time (b)(6)&(7)(C) accessed the member restricted websites. (b)(6)&(7)(C) said this computer was no longer used by (b)(6)&(7)(C)

Collection of Evidence

4. On April 13, 2011, (b)(6)&(7)(C) provided agents with written consent (*Exhibit 4*) to image and search computer media, which consisted of (a) a HP Pavilion a210e, (b)(6)&(7)(C) desktop computer, (living room), as well as to remove and search the (b) a desktop Acer Aspire M1100, (b)(6)&(7)(C) (living room), (c) an ASUS Tower computer, motherboard s/n (b)(6)&(7)(C) (bedroom), and (d) a Western Digital Passport USB drive, s/n (b)(6)&(7)(C) (bedroom). *Exhibit 5* details the items seized on April 13, 2011. Agents further observed additional devices in the residence with potential digital media. For example, there was a computer beneath (b)(6)&(7)(C) kitchen table, which (b)(6)&(7)(C) said belonged to someone else. Also, a hand-held video camera with memory card was observed in the proximity of the Hewlett Packard desktop. While signing the consent to search, (b)(6)&(7)(C) offered a comment that (b)(6)&(7)(C) might as well consent because "you (referring to the DCIS Agents) would come back with a search warrant anyway."

Re-Interview of (b)(6)&(7)(C)

5. On April 15, 2011, agents re-contacted (b)(6)&(7)(C) at (b)(6)&(7)(C) residence. *Exhibit 6* is a report detailing additional information provided by (b)(6)&(7)(C) When questioned, (b)(6)&(7)(C) said that (b)(6)&(7)(C) was aware that there were text files on (b)(6)&(7)(C) HP Computer that contained internet links to child pornography, but explained that (b)(6)&(7)(C) had only recently acquired the files. (b)(6)&(7)(C) also said that (b)(6)&(7)(C) thought the passwords to the websites listed in the text files were likely embedded with the links. (b)(6)&(7)(C) said that (b)(6)&(7)(C) wanted (b)(6)&(7)(C) cooperation "noted" and offered to assist by identifying child pornography on the internet. Before departing the residence, (b)(6)&(7)(C) mentioned that (b)(6)&(7)(C) was seeking unspecified treatment from the Veterans Administration. (b)(6)&(7)(C) served in the U.S. Army and was a veteran of the Vietnam War. Photographs were taken inside the residence at the conclusion of the search. One photograph taken in the living room was of a box that contained dollhouse furniture. The dollhouse furniture, (b)(6)&(7)(C) said, were items that (b)(6)&(7)(C) intended to sell on eBay.

Collection of Evidence

6. *Exhibit 7* is a report related to the consent search conducted on April 15th. (b)(6)&(7)(C) remained cooperative and provided written consent, *Exhibit 8*, to continue to search. *Exhibit 9* is a copy of the items seized on April 15th from (b)(6)&(7)(C) residence, which included (a) a San Disk thumb drive, model Cruzer, (b) a HP Pavilion n5420 laptop, (c) a desktop Dell Dimension 3000, (b)(6)&(7)(C) (d) a desktop AST Premmia Tower, (b)(6)&(7)(C) (e) a desktop Dell Optiplex GX110, service tag 90KTM01, (f) a desktop HP Pavilion 552x, (b)(6)&(7)(C) and (g) a desktop HP Pavilion a210e, (b)(6)&(7)(C)

Examination of Digital Evidence

7. *Exhibit 10* is the Media Analysis Report that describes the forensic review of digital computer media and the identification of over 19,000 digital pictures (26,000 including duplicates) and approximately two dozen videos consistent with the depiction of child pornography/sexual exploitation of children. The pictures found were of human female children in nude or semi-nude state. The female children were portrayed in ways that lasciviously

exposed their genitalia. Hardcore pictures were also located that depict the sexual assault of children. Pictures that depicted bestiality were also observed. Hardcore videos that contain child pornography were located. One hardcore video depicted a female child performing fellatio on an adult male while bound with rope. Other hardcore videos depicted the sexual assault of female children by male adults. Videos were also found that depicted nude or semi-nude female children in costumes, or displaying genitalia lasciviously. Two text files were located that contained apparent URL links to websites either hosting or linking to suspected child pornography. Recent internet history revealed instances where suspect URL links in the text file had been accessed. Although not contraband, a homemade video was located that depicted a female child playing in a wooded area. Another homemade video, taken by the driver of the vehicle, focuses on a young boy standing along the side of the road, with the video ending near (b)(6)&(7)(C) residence. Still another video that was located is of a man and woman pushing a stroller in front of (b)(6)&(7)(C) residence. Also observed were numerous sadomasochistic anime images depicting sexually explicit scenarios, such as the rape of a female child by an adult male.

NCMEC Coordination

8. On May 27, 2011, Technical Assistance (TA) Report No. 56376, *Exhibit 11*, was received from NCMEC. Analysis of pictures and videos was conducted and NCMEC identified eighteen (18) series with known sexual exploitation victims: (b)(7)(E) (b)(7)(E) (b)(7)(E) NCMEC's CyberTipLine did not have any information related to (b)(6)&(7)(C)

9. On June 27, 2011, TA Report No. 56445, *Exhibit 12*, was received from NCMEC. Analysis of two text files that contained links to websites, emails, and digital artifacts identified on (b)(6)&(7)(C) computer was conducted. NCMEC found that a number of the web links in the text files, in addition to web links in one email, had been identified in CyberTipline reporting.

10. On February 17, 2012, TA Report No. #61766, *Exhibit 13*, was received from NCMEC. NCMEC was asked to query CyberTipline records for information based on certain URLs found within the Recent Internet History located on one of (b)(6)&(7)(C) computers. NCMEC was able to identify several URLs in CyberTipline reporting. Recent access to the links was on March 2, 2011, April 5, 2011, and April 12, 2011.

11. On May 8, 2012, TA Report No. #61989, *Exhibit 14*, was received from NCMEC. NCMEC was asked to review videos suspected to contain child pornography. Their review identified 5 series with known victims: (b)(7)(E) This was the first instance where the series (b)(7)(E) was identified on the digital media provided by (b)(6)&(7)(C) increasing the total number of series identified to 19.

Law Enforcement Coordination

12. Detective (b)(6)&(7)(C) of the Nottinghamshire Police, United Kingdom (UK), was contacted about the (b)(6)&(7)(C) series. Detective (b)(6)&(7)(C) confirmed that the pictures obtained from (b)(6)&(7)(C) are those of a known victim in the (b)(7)(E) series. *Exhibit 15* is an email from Detective (b)(6)&(7)(C) along with a copy of the victim's birth certificate, affidavit that identifies the picture found on

(b)(6)&(7)(C) computer, and further explains the police's investigation into the abuse, sentencing of the offender, and impact the abuse had on the victim.

13. Detective (b)(6)&(7)(C) UK, Child Exploitation and Online Protection Center (CEOP), was contacted about the (b)(7)(E) Detective (b)(6)&(7)(C) confirmed by email, *Exhibit 16*, that the pictures found were of known child abuse victims and further provided information regarding the arrest and sentencing of the offender in both cases.

14. Detective Inspector (b)(6)&(7)(C) Bundeskriminalamt, (BKA), German Federal Police, was contacted about the (b)(7)(E) Detective Inspector (b)(6)&(7)(C) confirmed in an email, *Exhibit 17*, that the pictures found were known child abuse victims in the (b)(7)(E) and that the victims were under the age of 14 at the time the pictures were made.

15. Attempts to contact the Polish Police and Belgium Federal Police, regarding the (b)(7)(E) (b)(7)(E) respectively, were unsuccessful.

16. During the April 15, 2011 consent search, a credit card statement was observed with an entry referencing inet-cash.de (Inet) along with a foreign transaction fee. Inet was located in Germany that provides web-based payment systems. BKA Detective Inspector (b)(6)&(7)(C) was able to confirm with Inet certain information about (b)(6)&(7)(C) transactions with Inet. The email address and Internet Protocols (IP) linked to certain transactions were, in fact, conducted by (b)(6)&(7)(C) on Inet's website. Inet captured information that (b)(6)&(7)(C) was using Mozilla (Firefox) as a web browser launched from the IPs of Charter Communications: 71.83.49.101 and 68.116.181.147. Detective (b)(6)&(7)(C) was told that Inet carefully filters data from "Usnet" so that no pornographic material ever reaches Inet's website. Detective Inspector (b)(6)&(7)(C) provided an email, which is translated as *Exhibit 18*, regarding Inet.

IDENTITY OF SUBJECTS

IDENTIFYING DATA

Name	:	(b)(6)&(7)(C)
Social Security Number	:	
Date of Birth	:	
Place of Birth	:	
Race	:	
Sex	:	
Residence	:	
Employment/Occupation	:	
Telephone Number	:	
Education	:	

LAW ENFORCEMENT RECORDS

Certain law enforcement database queries were conducted that are not reportable in this document.

EVIDENCE

A. DOCUMENTS
(See Narrative)

B. WITNESSES
(See Narrative)

STATUS OF INVESTIGATION
The investigation has been coordinated with the USAO-MA.

PROSECUTORIAL CONSIDERATIONS
There are no considerations to date.

EXHIBITS

Exhibit No.	Description
1.	Report of Investigation
2.	Interview of (b)(6)&(7)(C) Form 1
3.	eBay/PayPal Transactional Data
4.	Written Consent to Search
5.	Evidence Custody Document, Form 14
6.	Interview of (b)(6)&(7)(C) Form 1
7.	Consent Search of (b)(6)&(7)(C) Residence, Form 1
8.	Written Consent to Search
9.	Evidence Custody Document, Form 14
10.	Media Analysis Report, Form 1
11.	NCMEC Technical Assistance Report No. 56376
12.	NCMEC Technical Assistance Report No. 56445
13.	NCMEC Technical Assistance Report No. 61766
14.	NCMEC Technical Assistance Report No. 61989
15.	Email and attachments from Nottinghamshire Police, UK
16.	Email from Child Exploitation and Online Protection, UK
17.	Email from the German Federal Police
18.	Email from the German Federal Police

Prepared by (b)(6)&(7)(C) Boston RA APPR: (b)(6)&(7)(C)

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
TULSA RESIDENT AGENCY
1603 S. 101ST EAST AVENUE, STE 131
TULSA, OK 74128

REPORT OF INVESTIGATION

201101704F-07-JUN-2011-30TL- (b)(7)(E) **June 10, 2014**

(b)(6)&(7)(C)

DISTRIBUTION:
AFCAF
San Antonio Police Department

NARRATIVE

1. This case was initiated based on information derived from Defense Criminal Investigative Service (DCIS) Project: Operation Flicker (UID: 200701199X). In 2007, the Bureau of Immigration and Customs Enforcement (ICE), now known as the Department of Homeland Security/Homeland Security Investigations (HSI), conducted a national investigation that identified over 5,000 U.S. individuals who subscribed to known child pornography websites. The DCIS project was initiated in May 2007 to identify any Department of Defense (DoD) affiliated individuals on the subscriber list, and to provide investigative assistance as needed to ICE.

2. The DCIS, ICE, the Military Criminal Investigative Organizations, and other federal, state, and local law enforcement agencies investigated many of these subjects; however, several leads were either not examined or not fully investigated. In late 2010, DCIS Headquarters rechecked all U.S. buyer names identified in the original ICE investigation. (b)(6)&(7)(C) was identified as a DoD-affiliated individual who had not previously been investigated under Project Flicker and was identified based on the existence of a record in the Joint Personnel Adjudication System (JPAS); however, (b)(6)&(7)(C) DoD affiliation at the time the investigation was initiated was unknown.

3. A review of (b)(6)&(7)(C) JPAS record showed that (b)(6)&(7)(C) received a favorable eligibility determination by the Air Force Central Adjudication Facility (AFCAF) on January 24, 2011, but did not have a clearance. Inquiries of other DoD databases indicated that (b)(6)&(7)(C) was a DoD Contractor from (b)(6)&(7)(C), and previously served in the U.S. Marine Corps (USMC) from (b)(6)&(7)(C)

4. (b)(6)&(7)(C)

(b)(6)&(7)(C)

5. The subscriber information provided by ICE reflected that on October 31, 2006, (b)(6)&(7)(C) purchased a subscription to "HL Package," a known child pornography website, through PayPal using (b)(6)&(7)(C) personal email address, (b)(6)&(7)(C) Database queries were conducted indicating that (b)(6)&(7)(C) resided at (b)(6)&(7)(C) Oklahoma City, OK 73119 and moved to Oklahoma from Texas in August 2008.

6. On December 8, 2011, SA (b)(6)&(7)(C) DCIS, Tulsa Resident Agency (RA), contacted (b)(6)&(7)(C) Oklahoma Employee Securities Commission (OKESO), Oklahoma City, OK, to inquire about (b)(6)&(7)(C) employment history, to which (b)(6)&(7)(C) stated that the OKESO employment history information is derived from the Internal Revenue Service via social security number, and therefore requires a subpoena for disclosure. (b)(6)&(7)(C) further stated that the records would only provide the name of the employer, employer's address, and salary, but would not identify the location of the employment or the position held by the employee. (b)(6)&(7)(C) added that the records are purged after four years, and therefore the earliest records available date back to the last quarter of 2007. Unfortunately, the information provided by Project Flicker identified October 2006 as the approximate date of the alleged criminal

activity and therefore falls outside of the date range for which employment history can be gathered. Further investigation determined that (b)(6)&(7)(C) did not have a DoD affiliation at the time of (b)(6)&(7)(C) alleged subscription to the child pornography site in October 2006.

7. On December 27, 2011, SA (b)(6)&(7)(C) interviewed (b)(6)&(7)(C) via telephone about (b)(6)&(7)(C) employment history under the ruse that (b)(6)&(7)(C) DoD clearance needed to be updated. (b)(6)&(7)(C) stated that (b)(6)&(7)(C) currently worked for (b)(6), (b)(7)(C) in Oklahoma City, OK, as a (b)(6)&(7)(C) Prior to (b)(6)&(7)(C) employment with (b)(6), (b)(7)(C) (b)(6)&(7)(C) worked for several DoD contractors including (b)(6), (b)(7)(C) and (b)(6), (b)(7)(C) in Oklahoma City, OK, from (b)(6)&(7)(C) (b)(6)&(7)(C)

8. On February 9, 2012, SA (b)(6)&(7)(C) interviewed (b)(6)&(7)(C) via telephone about the allegation that (b)(6)&(7)(C) subscribed to a known child pornography website in October of 2006. (b)(6)&(7)(C) denied that (b)(6)&(7)(C) ever subscribed to such a website. (b)(6)&(7)(C) explained that (b)(6)&(7)(C) debit and credit cards were stolen in October 2006 and may have been used to purchase the subscription; however, (b)(6)&(7)(C) was unable to provide any documentation to support the claim. (b)(6)&(7)(C) indicated that (b)(6)&(7)(C) was currently employed by (b)(6), (b)(7)(C) but had recently moved to (b)(6)&(7)(C) San Antonio, TX. (b)(6)&(7)(C) stated that (b)(6)&(7)(C) did not currently have a security clearance.

9. On March 16, 2012, SA (b)(6)&(7)(C) presented the case to Assistant U.S. Attorney (b)(6)&(7)(C) U.S. Attorney's Office, Western District of Oklahoma, Oklahoma City, OK, who verbally declined to prosecute (b)(6)&(7)(C) based on insufficient evidence.

10. On April 6, 2012, SA (b)(6)&(7)(C) DCIS, San Antonio Post of Duty, telephonically contacted (b)(6)&(7)(C) and requested an interview to which (b)(6)&(7)(C) agreed to meet at the DCIS office on April 10, 2012. On April 9, 2012, SA (b)(6)&(7)(C) received a telephone call from Legal Assistant (b)(6)&(7)(C) who advised that (b)(6)&(7)(C) was represented by (b)(6)&(7)(C) and wouldn't be available for the interview. On April 25, 2012, (b)(6)&(7)(C) provided a letter to SA (b)(6)&(7)(C) confirming (b)(6)&(7)(C) representation.

11. On April 25, May 1, May 4, and May 7, 2012, SA (b)(6)&(7)(C) left messages at the Law Office of (b)(6)&(7)(C) requesting to speak with (b)(6)&(7)(C) to schedule an interview with (b)(6)&(7)(C) however, SA (b)(6)&(7)(C) never received a response.

12. In September of 2012, upon SA (b)(6)&(7)(C) investigative responsibility for the case was transferred to SA (b)(6)&(7)(C) DCIS, Tulsa RA. After reviewing the case file, SA (b)(6)&(7)(C) placed numerous phone calls to (b)(6)&(7)(C) to schedule an interview with (b)(6)&(7)(C) The initial information provided by (b)(6)&(7)(C) office was that they were unable to locate (b)(6)&(7)(C) After numerous, unsuccessful attempts to reach (b)(6)&(7)(C) between November 2012 and April 2013, SA (b)(6)&(7)(C) contacted (b)(6)&(7)(C) who confirmed that (b)(6)&(7)(C) was still (b)(6)&(7)(C) attorney and that (b)(6)&(7)(C) had spoken with (b)(6)&(7)(C) recently.

13. On May 15, 2013, SA (b)(6)&(7)(C) spoke with (b)(6)&(7)(C) who stated that (b)(6)&(7)(C) would contact (b)(6)&(7)(C) to schedule an interview. In July 2013, after (b)(6)&(7)(C) failed to respond to SA (b)(6)&(7)(C) (b)(6)&(7)(C) DCIS, Southwest Field Office, sent an official request to (b)(6)&(7)(C) requesting that (b)(6)&(7)(C) contact SA (b)(6)&(7)(C) to schedule an interview with (b)(6)&(7)(C) On August 8, 2013, (b)(6)&(7)(C) called and scheduled an interview with (b)(6)&(7)(C) for September 16, 2013, which was subsequently rescheduled for October 21, 2013.

14. On August 19, 2013, in accordance with the investigative plan for Operation Flicker cases, a DoD Inspector General subpoena was issued to PayPal for records of payments made by (b)(6)&(7)(C) which failed to reveal any additional information not previously known to the investigation.

15. On October 21, 2013, SA (b)(6)&(7)(C) interviewed (b)(6)&(7)(C) in the presence of (b)(6), (b)(7)(C) at the Tulsa RA. During the interview, (b)(6)&(7)(C) stated that (b)(6)&(7)(C) never held a security clearance during the course of any work on any DoD contracts and only held a clearance during (b)(6)&(7)(C) service in the USMC. (b)(6)&(7)(C) further explained that (b)(6)&(7)(C) never had access to any DoD databases and that (b)(6)&(7)(C) computer access was restricted to the specific task to which (b)(6)&(7)(C) was assigned.

16. During the interview, (b)(6)&(7)(C) provided copies of (b)(6)&(7)(C) bank statements in response to the purported theft of (b)(6)&(7)(C) debit card in 2006. (b)(6)&(7)(C) highlighted the alleged fraudulent PayPal charge for the child pornography website, but could not show any credits issued to the account as a result of the compromise. (b)(6)&(7)(C) stated that (b)(6)&(7)(C) did not file a police report about the fraudulent debit card transaction, but contacted (b)(6)&(7)(C) bank about the compromise to which a new debit card was issued. (b)(6)&(7)(C) stated that (b)(6)&(7)(C) would work with (b)(6)&(7)(C) to recover any additional evidence of the fraudulent charge and forward the information to SA (b)(6)&(7)(C)

17. On November 21, 2013, (b)(6)&(7)(C) left a voicemail for SA (b)(6)&(7)(C) stating that the bank records supporting (b)(6)&(7)(C) account of a debit card compromise were sent to the DCIS Tulsa RA via certified mail, however the records never arrived.

18. On December 3, 2013, SA (b)(6)&(7)(C) called (b)(6)&(7)(C) to inquire about the records without response. From December 2013 to February 2013, SA (b)(6)&(7)(C) continued to leave messages with (b)(6)&(7)(C) in an attempt to locate the records.

19. On March 10, 2014, SA (b)(6)&(7)(C) called (b)(6)&(7)(C) office and spoke with (b)(6)&(7)(C) who advised that the records had been returned to their office as undeliverable due to a missing office suite number, to which (b)(6)&(7)(C) agreed to resend the letter.

20. On March 12, 2014, SA (b)(6)&(7)(C) received the records from (b)(6)&(7)(C) office. The records included a printout from (b)(6)&(7)(C) account at Northstar Bank of Texas, indicating that a new debit card was issued on December 18, 2006, supporting (b)(6)&(7)(C) claim that (b)(6)&(7)(C) requested a new debit card; however, the records did not contain any file notes indicating fraud as the reason for the replacement. Furthermore, the printout did not contain any information to support that the charges were ever reversed due to fraud.

21. In March 2014, April 2014, and May 2014, SA (b)(6)&(7)(C) called (b)(6)&(7)(C) office numerous times seeking additional information to support (b)(6)&(7)(C) claim of the fraudulent use of

(b)(6)&(7)(C) debit card and to inquire if (b)(6)&(7)(C) would consent to a search of (b)(6)&(7)(C) computer. SA (b)(6)&(7)(C) never heard from (b)(6)&(7)(C)

22. All requests for information have been ignored and all investigative efforts have been exhausted. This case was previously declined for prosecution based on insufficient evidence and it is highly unlikely that any further evidence or probable cause will be developed to necessitate further investigation. No administrative action will occur. This case is now closed.

IDENTITY OF SUBJECTS

IDENTIFYING DATA

Name	(b)(6)&(7)(C)
Alias	
Social Security Number	
Date/Place of Birth	
Race	
Sex	
Height	
Weight	
Hair	
Eyes	
Residence	
Employment/Occupation (current)	
Telephone Number	
Driver's License Number	
And Issuing State	
Education	: Unknown

Prepared by SA (b)(6)&(7)(C), Tulsa RA APPR: (b)(6)&(7)(C)

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
WASHINGTON, DC RESIDENT AGENCY
4800 MARK CENTER DRIVE, SUITE 10D25-04
ALEXANDRIA, VA 22350-1500

(Investigations)

REPORT OF INVESTIGATION

DFAS (NO. 2008-DICIB-0016)

200801296F-08-MAY-2008-60DC- (b)(7)(E) **April 4, 2014**

(b)(6)&(7)(C)

DISTRIBUTION

DFAS – SA (b)(6)&(7)(C) (DFAS Internal Review Columbus, OH)
FBI – SA (b)(6)&(7)(C) Baltimore, Maryland)

NARRATIVE

1. As background, on May 8, 2008, the DCIS Arlington Resident Agency (RA) initiated a joint investigation with the FBI into an alleged scheme to steal DoD payments intended for contractors. The investigation revealed that unauthorized users accessed and modified DoD contractors' Department of Defense Central Contractor's Registry (CCR) information causing the diversion of Defense Finance and Accounting Service (DFAS) payments intended for DoD contractors to unauthorized financial accounts. The victimized DoD contractors' payment notifications were sent to unauthorized DFAS MyInvoice accounts. The case was accepted for prosecution by Assistant United States Attorney (AUSA) (b)(6)&(7)(C) Eastern District of Virginia (EDVA) for unauthorized access of DoD computer systems and AUSA (b)(6)&(7)(C) District of Minnesota for Bank Fraud, Aggravated Identity Theft, and Money Laundering. There was assistance from numerous other AUSAs and Trial Attorneys throughout the U.S, as well.

2. On April 10, 2008, the DCIS, Arlington Resident Agency (RA), was notified by (b)(6)&(7)(C) (b)(6)&(7)(C) Defense Logistics Agency (DLA), Office of Investigations (OI), Battle Creek, Michigan concerning allegations that an unauthorized user(s) accessed Abacus Technology Corporation's (Abacus) CCR information and revised its remittance and point of contact (POC) information. The revisions caused the diversion of six DFAS payments totaling $727,119.52 to an unauthorized CitiBank NA (Citibank) correspondent bank account. The e-mail address revisions diverted DFAS e-mail correspondence from authorized Abacus employee contacts to unauthorized e-mail accounts.

3. On April 24, 2008, SA (b)(6)&(7)(C) FBI, New Mexico, contacted (b)(6)&(7)(C) Computer Crimes Coordinator (CCC), to de-conflict a similar matter involving the New Mexico Institute of Mining Technology (NMIMT), Socorro, NM. SAs (b)(6)&(7)(C) compared the incidents and decided to pursue the matters jointly.

4. Initially SA (b)(6)&(7)(C) presented the Abacus matter to Trial Attorney (TA) (b)(6)&(7)(C) (b)(6)&(7)(C) on April 29, 2008, and (b)(6)&(7)(C) accepted the case for prosecution. SA (b)(6)&(7)(C) FBI, Cyber Crime Investigations, Baltimore, MD was asked to join the investigation. Following additional instances of attempted diversions, in July 2008, TA (b)(6)&(7)(C) transferred the investigation to AUSA (b)(6)&(7)(C)

5. While investigating the Abacus diversion it was learned that (b)(6)&(7)(C) Abacus, was responsible for monitoring the receipt of DFAS payments. When (b)(6)&(7)(C) noticed in MyInvoice that DFAS payments were not received in the Abacus bank account, (b)(6)&(7)(C) contacted DFAS and Wide Area Work Flow to inquire.

6. The DFAS MyInvoice web-based application was used by DoD contractors and Government employees to obtain invoice and payment status via e-mail notifications. The MyInvoice registration did not include a vetting process, so any user was able to create a MyInvoice account for any contractor. Contractors were not notified of the MyInvoice accounts that received their payment notifications. The DFAS payment notification sent via e-mail included cage code, duns number, contract number, invoice number, invoice amount, and payment date.

7. SAs (b)(6)&(7)(C) and (b)(6)&(7)(C) interviewed numerous Abacus employees, to include (b)(6)&(7)(C) (b)(6)&(7)(C) (b)(6)&(7)(C) It was learned in the interviews that DFAS had at least three payment systems and DFAS used the remittance information in the CCR to make payments. The CCR Change History report captured each instance Abacus' CCR information was accessed and revised. (b)(6)&(7)(C) who managed the CCR information, confirmed (b)(6)&(7)(C) did not make the changes that caused the diversions. Abacus subsequently changed its Trading Partner Identification Number (TPIN), and there were no further diversions.

8. DFAS performed a review of Abacus' MyInvoice account and discovered an unauthorized account registered with e-mail address (b)(6)&(7)(C) which also received Abacus' payment notifications.

9. On May 28, 2008, SA (b)(6)&(7)(C) interviewed (b)(6)&(7)(C) Citibank. (b)(6)&(7)(C) stated the CitiBank account was the main clearing account for all wire transfers to Kenya. The diversions failed because the destination account information was required. Transactions without the destination account information were reversed and the funds sent back to the bank initiating the ACH. DFAS successfully recovered Abacus' diverted payments.

10. Investigation of the NMIMT diversion revealed DFAS payments were diverted to two accounts at Fidelity, Umb Bank, NA (Fidelity). The accounts were created using stolen identities. The accounts were created and accessed via the Internet. Fidelity immediately "froze" the accounts so no additional DoD monies were lost.

11. On May 20, 2008, SA (b)(6)&(7)(C) notified SA (b)(6)&(7)(C) that (b)(6)&(7)(C) (b)(6)&(7)(C) headquartered in Hampton, VA, contacted CCR security on May 19, 2008, and reported their CCR e-mail addresses and remittance information were changed. (b)(6)&(7)(C) who monitored DFAS payments, anticipated DFAS payments into (b)(6)&(7)(C) Bank of America business account. When the payments were not deposited as expected, (b)(6)&(7)(C) checked (b)(6)&(7)(C) CCR information. (b)(6)&(7)(C) noticed (b)(6)&(7)(C) CCR information was revised. (b)(6)&(7)(C) made the corrections and contacted CCR Security and DFAS. The remittance revision caused the diversion of their DFAS payments to an unauthorized account with Guaranty Bank, MN. (b)(6)&(7)(C) stated (b)(6)&(7)(C) had inadvertently published its TPIN on the company's website.

12. DFAS notified Guaranty Bank, of the diverted DFAS payments intended for (b)(6)&(7)(C)

13. Investigation of (b)(6)&(7)(C) diversion revealed the Guaranty Bank account was in the name of (b)(6)&(7)(C) business MaliHvac Services. According to (b)(6)&(7)(C) Security, Guaranty Bank, the transactions on the account were considered "normal" activity until September 4, 2007, when all transactions originated from Nairobi, Kenya. Including ATM withdrawals in Nairobi, Kenya, a total of $3,002.74 was debited from the account. Guaranty Bank reversed all of the deposits so there was no loss of DoD funds.

14. On June 2, 2008, SAs (b)(6)&(7)(C) interviewed (b)(6)&(7)(C) (b)(6)&(7)(C) at (b)(6)&(7)(C) residence in Minneapolis, MN. According to (b)(6)&(7)(C) and (b)(6)&(7)(C) lived together for nearly nine months until (b)(6)&(7)(C) moved out in March 2007. (b)(6)&(7)(C) had several financial statements mailed to (b)(6)&(7)(C) residence. (b)(6)&(7)(C) stated (b)(6)&(7)(C) created a business named MaliHvac Services for fraudulent purposes but (b)(6)&(7)(C) threw out the statements. On

or around May 29, 2008, (b)(6)&(7)(C) received a box of checks from Fidelity Investment bearing the name of (b)(6)&(7)(C) When (b)(6)&(7)(C) moved out, (b)(6)&(7)(C) claimed to (b)(6)&(7)(C) life would change drastically in four to five months. (b)(6)&(7)(C) recalled (b)(6)&(7)(C) also banked with TCF Bank and had received an (b)(6)&(7)(C) last heard from (b)(6)&(7)(C) on May 18, 2008, when (b)(6)&(7)(C) called from (b)(6)&(7)(C)

15. On May 29, 2008, (b)(6)&(7)(C) notified SA (b)(6)&(7)(C) via e-mail that the CCR data for Applied Resources, Incorporated (ARI), Arlington, VA, was revised twice and the DFAS payments were diverted to unauthorized bank accounts.

16. Investigation of the ARI diversion revealed ARI's remittance information was revised on two separate instances to two unauthorized accounts. One account was at JP Morgan Chase Bank and the other Wells Fargo Bank, IN. Both banks rejected the DFAS payments since the name in the transfer did not match the names on the accounts. Both of the accounts were owned by one person.

17. On July 8, 2009, SAs (b)(6)&(7)(C) and (b)(6)&(7)(C) DCIS Richmond Post of Duty (POD) interviewed the owner of the JP Morgan Chase Bank and the Wells Fargo Bank accounts and learned that the accounts were controlled and managed by the owner's relatives in Kenya. The accounts were closed in 2008 when the banks notified the owner of fraudulent activities.

18. On June 10, 2008, (b)(6)&(7)(C) notified SA (b)(6)&(7)(C) via e-mail that the CCR data for University of Notre Dame (UND), Notre Dame, IN, was revised and DFAS payments were diverted to an unknown account.

19. Investigation into the UND diversion revealed that (b)(6)&(7)(C) Maryland Procurement Office (MPO), Fort Meade, MD, contacted (b)(6)&(7)(C) Research and Sponsored Programs Accounting, UND, to report the UND bank account information obtained from the CCR was invalid and requested a valid bank account for payment. (b)(6)&(7)(C) advised MPO sent a payment to the UND bank account identified in the CCR and it was returned by the bank as not valid.

20. The MPO payment intended for UND was sent to the JP Morgan Chase account. The payment was rejected, and the funds returned to MPO.

21. The investigation revealed UND's CCR information was accessed three times by an unauthorized user. On the second attempt, the remittance information was revised to a Fidelity account used in the NMIMT incident. Fidelity rejected one payment and the other was successfully deposited. Fidelity denied online access and financial transactions to the account, and the funds were returned to DFAS.

22. On the third attempt to divert UND's funds, the banking information was changed to a TCF Bank account in Minneapolis, MN. Between June 5 and June 12, 2008, a total of $209,862 intended for UND was deposited into the TCF Bank account and withdrawn by unknown subject(s). TCF Bank did not archive video footage of the person(s) who accessed the account.

23. The investigation of the UND incident revealed Wright State University's (WSU), Dayton, OH, DFAS payments totaling $126,245 were successfully deposited into the TCF Bank account.

24. On June 18, 2008, (b)(6)&(7)(C) notified SA (b)(6)&(7)(C) the University of West Florida (UWF), Pensacola, FL, reported its CCR data was revised and DFAS payments were diverted to an unauthorized financial account. (b)(6)&(7)(C) was contacted by (b)(6)&(7)(C) UWF, who reported the incident. According to (b)(6)&(7)(C) UWF had a contract with the National Park Service (NPS). The Contracting Officer (CO), NPS, obtained UWF's remittance information from the CCR. The CO noticed discrepancies between the CCR information and information recently included in a grant proposal and contacted (b)(6)&(7)(C) for clarification, alerting (b)(6)&(7)(C) to the unauthorized revisions.

25. The investigation of UWF revealed the remittance information was revised twice. The account information was changed once to an account at Fidelity and changed a second time to an account at Eastern Florida Financial Credit Union (EFFCU), Miramar, FL. Fidelity denied online access and financial transactions on the account. One UWF DFAS payment for less than $2,000 was successfully deposited into the EFFCU account. EFFCU did not have video footage of the subject(s) who accessed the account because the account had been inactive for some time. Once EFFCU was notified of the fraudulent activity the bank froze the account.

26. While investigating the UWF incident, SA (b)(6)&(7)(C) DCIS Pensacola POD, learned the University of Kansas Center for Research (UKCR), Lawrence, KS, and the Research Foundation for the State University of New York (RFSUNY), Albany, NY, had DFAS payments diverted as well. A total of $132, 234 was successfully deposited into the same EFFCU bank account. DFAS payments diverted to the EFFCU account intended for RFSUNY were rejected, while UKCR DFAS payments were successfully deposited. RFSUNY DFAS payments were also unsuccessfully diverted to a Fidelity account.

27. On July 30, 2008, John Carroll University (JCU), University Heights, OH was identified as a victim of the scheme. JCU's DFAS payments were unsuccessfully diverted to a Fidelity account.

28. Fidelity Investment conducted an investigation of the accounts that were used to receive diverted DFAS payments. Fidelity Investment concluded there was a relationship between the fraudulent accounts. Fidelity Investment identified a total of ten fraudulent accounts created online between January 15, 2008, and May 19, 2008. All of the accounts were accessed from the same computer that accessed the (b)(6)&(7)(C) account. When users accessed their online accounts, Fidelity saved a "cookie" or file on their computer. In addition, the IP Addresses used to access the ten Fidelity bank accounts were associated with an Internet Service Provider in Nairobi, Kenya.

29. On December 23, 2008, SA (b)(6)&(7)(C) was contacted by SA (b)(6)&(7)(C) FBI, Canton, OH, to de-conflict a CCR intrusion which diverted DFAS payments intended for Midwest Industrial Supply, Inc. (MIS), Canton, OH. MIS's DFAS payment of $138,452 was diverted to a Bank of America account located in Georgia. SA (b)(6)&(7)(C) presented the matter to the United States' Attorney's Office, Northern District of Ohio and it was declined for prosecution.

30. From April 10, 2008, through December 23, 2008, the scheme affected eleven DoD contractors and the conspirators attempted to divert a total of $5.1 million in DFAS payments. The total loss to DoD was $606,793.

31. The investigative effort identified the use of "profiles" to open the fraudulent accounts. When Kenyans left the U.S., they would sell their personal identifying information, or "profile," to conspirators of this scheme to steal DoD monies. The profiles were then used to open fraudulent accounts for receipt of stolen funds from DFAS.

32. In July 2011, the case was presented to the International Organized Crime Intelligence and Operations Center (IOC-2), Fairfax, VA. Since the last CCR diversion occurred in December 2008, IOC-2 was unable to assist. AUSA(b)(6)&(7)(C) and AUSA(b)(6)&(7)(C) declined prosecution of this matter due to the lack of direct evidence such as photo or video, and lack of new activity since December 2008. Investigative sources suggested the subjects identified as having significant knowledge or responsible for the scheme were not in the U.S. for questioning.

33. DCIS will not pursue further investigative actions. Subsequent to the diversions, DFAS developed new security measures for CCR access and monitoring the creation of MyInvoice accounts. Additionally, the CCR posted TPIN awareness messages on its website.

There were no other fraud vulnerabilities identified during the course of this investigation.

(b)(6)&(7)(C)

Prepared by: SA (b)(6)&(7)(C) Washington, DC RA APPR: (b)(6)&(7)(C)

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
WASHINGTON, DC RESIDENT AGENCY
4800 MARK CENTER DRIVE, SUITE 10D25-04
ALEXANDRIA, VA 22350-1500

REPORT OF INVESTIGATION

2011050089-22-JUL-2011-60DC- (b)(7)(E) **May 12, 2014**

(b)(6)&(7)(C)

DISTRIBUTION: DCIS HQ (b)(6)&(7)(C)

NARRATIVE

1. This case was initiated based on information derived from Defense Criminal Investigative Service (DCIS) Project: Operation Flicker (Case Control Number 200701199X). As background, in 2007, Immigration and Customs Enforcement (ICE) conducted a national investigation that identified over 5,000 U.S. individuals who subscribed to known child pornography websites. DCIS Project Flicker was initiated in May of 2007 to identify and Department of Defense (DoD) affiliated individuals, and provide investigative assistance as needed to ICE. DCIS, ICE, the Military Criminal Investigative Organizations (MCIOs), and other Federal, State, and Local law enforcement agencies investigated many of these subjects, however, several leads were either not examined or not fully investigated. In late 2010, DCIS Headquarters rechecked all U.S. buyer names identified in the original ICE investigation.

2. (b)(6)&(7)(C) U.S. Air Force (USAF) was identified as a DoD affiliated individual that had not previously been investigated under the Project Flicker. According to reenlistment Eligibility Data Display (REDD) report, (b)(6)&(7)(C) enlisted in the USAF (b)(6)&(7)(C) was identified as a subject after a review of (b)(6)&(7)(C) PayPal account revealed purchases made on December 28, 2006, and January 25, 2007, to an unspecified website that was suspected of containing child pornography.

3. On August 17, 2011, SA (b)(6)&(7)(C) DCIS Arlington RA received from (b)(6)&(7)(C) (b)(6)&(7)(C), eBay/PayPal Incorporated (eBay/PayPal), records related to eBay/PayPal accounts associated with (b)(6)&(7)(C) or the e-mail address (b)(6)&(7)(C) in response to an Inspector General (IG) Subpoena address to eBay/PayPal, served on August 12, 2011.

4. A review of the records identified two transactions associated with (b)(6)&(7)(C) one on December 28, 2006, in the amount of $79.95 to "Belfast LTD," and one on January 25, 2007, in the amount of $79.95 to "Lencomps Ltd." The records showed two transactions associated with (b)(6)&(7)(C) one on October 11, 2006, in the amount of $27.74 to "MyDom Computers and Services," and one on January 3, 2011, in the amount of $34.99 to "FileServe Ltd." No other transactions were identified.

5. On December 16, 2011, SA (b)(6)&(7)(C) and SA (b)(6)&(7)(C) DCIS Arlington RA, interviewed (b)(6)&(7)(C) regarding the allegations. (b)(6)&(7)(C) denied subscribing to any child pornography websites.

6. On December 21, 2011, SA (b)(6)&(7)(C) and SA (b)(6)&(7)(C) DCIS Arlington RA, re-interviewed (b)(6)&(7)(C) per (b)(6)&(7)(C) request. (b)(6)&(7)(C) admitted lying in previous interview. (b)(6)&(7)(C) further admitted (b)(6)&(7)(C) subscribed to a website (NFI) providing child pornography, but claimed to log into the website only once before cancelling (b)(6)&(7)(C) account. (b)(6)&(7)(C) gave consent for SA (b)(6)&(7)(C) to image and search (b)(6)&(7)(C) HP Pavilion laptop, Toshiba laptop, Western Digital My Passport external hard drive, and additional external hard drive.

7. On December 21, 2011, SA (b)(6)&(7)(C) submitted a lead request for computer forensics analysis on (b)(6)&(7)(C) two laptops and two external hard drives.

8. On January 9, 2012, SA (b)(6)&(7)(C) and SA (b)(6)&(7)(C), U.S. Army Criminal Investigation Division (USACIDC), interviewed (b)(6)&(7)(C) regarding the allegations. (b)(6)&(7)(C) admitted (b)(6)&(7)(C) previously had in (b)(6)&(7)(C) possession a third computer, an HP desktop, which (b)(6)&(7)(C) used to download images and movies of young girls from a website called "LS Magazine," which contained images and videos of females 6 years-old to approximately 17 or 18 years-old. (b)(6)&(7)(C) stated after DCIS interviewed (b)(6)&(7)(C) the first time, (b)(6)&(7)(C) "destroyed" the computer.

9. In April 2012, SA (b)(6)&(7)(C) reviewed the imaged computer media that was provided by (b)(6)&(7)(C) Images shown on the media were documented and submitted to the National Center for Missing and Exploited Children (NCMEC) for expert analysis.

10. On October 18, 2012, SA (b)(6)&(7)(C) received the expert analysis returned from NCMEC. NCMEC reviewed the submitted picture and video files in an effort to positively identify any known child victims that were identified by law enforcement in past investigations. NCMEC found that one video file did appear to contain a child victim who had been identified by law enforcement and provided a 'Child Identification Report'.

11. On February 22, 2013, SA (b)(6)&(7)(C) presented the case for prosecution to AUSA (b)(6)&(7)(C) (b)(6)&(7)(C) EDVA, and AUSA (b)(6)&(7)(C) EDVA. AUSAs (b)(6)&(7)(C) accepted the case for prosecution.

12. On June 21, 2013, (b)(6)&(7)(C) surrendered a Toshiba hard drive, a My Passport External hard drive, and a Toshiba laptop computer to SA (b)(6)&(7)(C)

13. On July 10, 2013, (b)(6)&(7)(C) surrendered (b)(6)&(7)(C) Hewlett Packard (HP) Pavilion laptop computer to SA (b)(6)&(7)(C)

14. On September 3, 2013, SA (b)(6)&(7)(C) AUSA (b)(6)&(7)(C) and defense attorney (b)(6)&(7)(C) met and reviewed the pertinent evidence.

15. On January 15, 2014, (b)(6)&(7)(C) pled guilty in U.S. District Court, Eastern District of Virginia (EDVA), Alexandria Division, to one count of a criminal Information that was filed that same day charging (b)(6)&(7)(C) with a violation of 18 U.S.C. § 2252 (a)(4), Possession of Child Pornography (Exhibit 1).

16. On May 2, 2014, (b)(6)&(7)(C) was sentenced to 15 months imprisonment, 5 years of supervised release with special conditions, and a $100.00 criminal assessment penalty. Sentencing was ordered by the Honorable Judge Liam O'Grady in U.S. District Court, Eastern District of Virginia (EDVA), Alexandria Division (Exhibit 2).

17. With the completion of the sentencing action, all investigative effort is completed and this investigation is now closed.

18. There were no fraud vulnerabilities identified during the course of this investigation.

IDENTITY OF SUBJECTS

	IDENTIFYING DATA
Name Alias Social Security Number Date/Place of Birth	(b)(6)&(7)(C)
Race	: UNK
Sex	(b)(6)&(7)(C)
Height	: UNK
Weight	: UNK
Hair	: UNK
Eyes	: UNK
Residence	(b)(6)&(7)(C)
Employment/Occupation	
Telephone Number	: UNK
Driver's License Number/Issuing State	: UNK

EXHIBITS

EXHIBIT NO.	DESCRIPTION
1	Plea Agreement, filed January 15, 2014, Criminal No. 1:13-CR-498, U.S. District Court, Eastern District of Virginia.
2	Judgment in a Criminal Case, filed May 2, 2014, Criminal No. 1:13-CR-498, U.S. District Court, Eastern District of Virginia.

(b)(6)&(7)(C) (b)(6)&(7)(C)

Prepared by: Special Agent (b)(6)&(7)(C) Washington, DC Resident Agency APPR: (b)(6)&(7)(C)