

This document is made available through the declassification efforts  
and research of John Greenewald, Jr., creator of:

# The Black Vault



The Black Vault is the largest online Freedom of Information Act (FOIA)  
document clearinghouse in the world. The research efforts here are  
responsible for the declassification of hundreds of thousands of pages  
released by the U.S. Government & Military.

**Discover the Truth** at: <http://www.theblackvault.com>



(Investigations)

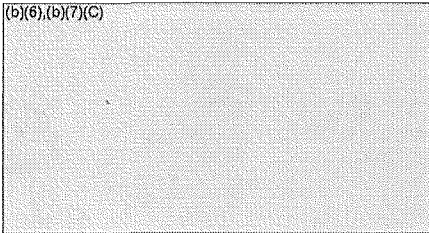
INSPECTOR GENERAL  
DEPARTMENT OF DEFENSE  
DEFENSE CRIMINAL INVESTIGATIVE SERVICE  
SYRACUSE POST OF DUTY  
441 S. SALINA ST, STE 602  
SYRACUSE, NY 13202-2400

REPORT OF INVESTIGATION

200701516W-25-JUL-2007-10SY-W1/E

20-NOVEMBER-2009

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



DISTRIBUTION

Headquarters, Investigative Operations Directorate  
Northeast Field Office  
Pittsburgh Resident Agency

C-1

CLASSIFICATION:

~~FOR OFFICIAL USE ONLY~~

WARNING

~~This document is the property of the Department of Defense Inspector General and is loaned to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without the specific prior authorization of the Deputy Inspector General for Investigations.~~

NARRATIVE

1. On July 11, 2007, the reporting agent received a lead referral from Special Agent (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) DCIS Mid-Atlantic Field Office regarding the Immigration and Customs Enforcement (ICE) initiated Operation Flicker. Operation Flicker is a nationwide investigation that has identified over 5,000 individuals that have subscribed to predicated child pornography websites. SA (b)(6),(b)(7)(C) sent a list of individuals in New York State that are employed by the Department of Defense/U.S. Military, that have subscribed to websites that contain child pornographic images or other material that exploit children via the internet.
2. In April 2006, the ICE/Cyber Crimes Center/Child Exploitation Section (ICE/C3/CES) initiated an investigation into a criminal organization operating a commercial child pornography website known as "Home Collection." The investigation has revealed that the same organization is operating numerous commercial child pornography websites. In addition, the organization utilizes various Pay Pal accounts to process the payments for access to the member restricted areas of these websites. The investigation is being worked jointly with ICE/C3/CES, ICE/RAC/Birmingham, the U.S. Postal Inspection Service, the U.S. Department of Justice/Child Exploitation and Obscenity Section, and the USAO for the Northern District of Alabama. ICE has designated this operation as PROJECT FLICKER.
3. ICE/C3/CES has conducted over 60 undercover transactions at the advertising websites associated with this investigation. The investigation has identified that a specific criminal organization is operating approximately 18 different commercial child pornography advertising websites which provide access to approximately 18 child pornography member restricted websites.
4. Among the 5,000 names ICE identified under Project Flicker, several individuals used their .mil e-mail address, Fleet Post Office (FPO), or Army Post Office (APO) military zip codes. SA (b)(6),(b)(7)(C) advised the U.S. Attorney's Office and ICE that the DCIS will assist in identifying any additional Department of Defense (DoD) affiliated individuals and provide any investigative assistance.
5. SA (b)(6),(b)(7)(C) conducted queried DoD databases to identify individuals that may be in possession of child pornographic material or access, and has forwarded the results of his queries to the respective DCIS office for consideration for possible DCIS case initiations. SA (b)(6),(b)(7)(C) attached a spreadsheet for subjects of Operation Flicker in the state of New York that have a DoD affiliation. One subject identified on the spreadsheet includes an individual identified as (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) (b)(6),(b)(7)(C)
6. The reporting agent queried the Defense Employee Interactive Data Systems (DEIDS), and obtained the following information regarding (b)(6),(b)(7)(C) (b)(6),(b)(7)(C)

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

7. The reporting agent also queried the Re-Enlistment Eligibility Data Display (REDD) database for (b)(6),(b)(7)(C) and obtained the following information: (b)(6),(b)(7)(C)
- (b)(6),(b)(7)(C)
- (b)(6),(b)(7)(C)
8. The reporting agent contacted Special Agent (b)(6),(b)(7)(C) ICE Alexandria Bay, NY regarding Operation Flicker. SA (b)(6),(b)(7)(C) subsequently forwarded the reporting agent a spreadsheet that identifies all New York subjects of Operation Flicker, and pertinent information regarding subscriber information related to the child exploitation websites. SA (b)(6),(b)(7)(C) advised that he would be reviewing the list of subjects for possible investigation. The reporting agent advised that the DCIS would review the list, and initiate an investigation of DoD related personnel in the Syracuse Post of Duty area of responsibility. SA (b)(6),(b)(7)(C) advised that another ICE agent would be assigned to specific investigation, but he would assist in the computer forensics part of the cases.
9. Upon review of the spreadsheet sent by SA (b)(6),(b)(7)(C) the reporting agent determined that (b)(6),(b)(7)(C) made one payment utilizing PayPal to the restricted access websites. The transaction occurred on January 30, 2007 for \$79.95. The "trans.Item Title" was either listed as an invoice number: Invoice # 41041. (Agent Note: this is the subject line identifier which indicates which member restricted site a specific customer purchased. In the Project Flicker Overview report, it stated that in November 2006, the criminal organization omitted the subject line identifiers, and began using Invoice numbers. The ICE agent stated that the Pay Pal accounts still identify the specific member restricted sites an individual purchased). The reporting agent will review the spreadsheet, and will report the details under a separate Form 1.
10. On November 16, 2007, the reporting agent, SA (b)(6),(b)(7)(C) ICE SA (b)(6),(b)(7)(C) and ICE SA (b)(6),(b)(7)(C) conducted a consent search at the residence of (b)(6),(b)(7)(C) The reporting agent and SA (b)(6),(b)(7)(C) interviewed (b)(6),(b)(7)(C) The interview report was written by SA (b)(6),(b)(7)(C)
11. SA (b)(6),(b)(7)(C) and SA (b)(6),(b)(7)(C) conducted a preliminary computer forensic review of two desktop computers and one laptop computer. During the initial review of the computers, the agents discovered numerous child pornographic materials on one of the computers believed to be utilized by (b)(6),(b)(7)(C) The computer that contained the child pornographic material was seized by SA (b)(6),(b)(7)(C) and ICE will maintain custody of the computer. The review/analysis of the computer will be conducted by SA (b)(6),(b)(7)(C) after a search warrant is issued by the U.S. District Court, Northern District of New York. During the next reporting period, it is anticipated that the search warrant will be issued for the complete examination of the seized computer.
12. The reporting agent and SA (b)(6),(b)(7)(C) have been in contact with Assistant United States Attorney (AUSA) (b)(6),(b)(7)(C) Northern District of New York, Syracuse, NY for consideration of criminal prosecution of (b)(6),(b)(7)(C) in violation of Certain Activities Related to the Sexual Exploitation of Minors, Title 18 USC § 2252.

13. In February 2008, the reporting agent obtained a copy of (b)(6),(b)(7)(C) military service records from the National Archives and Records Administration in St. Louis, MO. The records indicated that (b)(6),(b)(7)(C)

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

14. On January 15, 2008, an application and affidavit for a Search Warrant was ordered by the (b)(6),(b)(7)(C) Northern District of New York for "one desktop computer, central processing unit, black and grey in color, identified and marked as a Dell Dimension, bearing serial number H3XQQ31." The search warrant was based upon the consent search that was conducted on November 16, 2007 for a computer belonging to (b)(6),(b)(7)(C) that was determine to contain child pornographic images. The search warrant authorized the agents to conduct a thorough forensic examination of the computer to attempt to substantiate the allegations regarding violations by (b)(6),(b)(7)(C) of the Exploitation of minors under Title 18 United States Code § 2252.

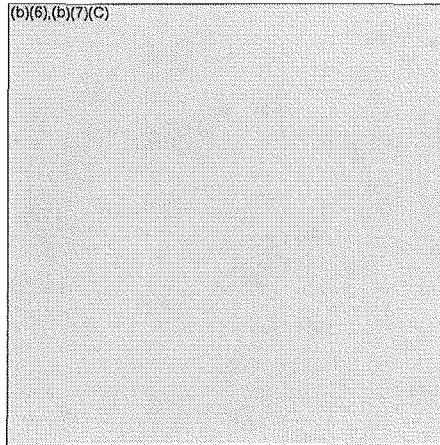
15. From a period of February 2009 to November 2009, the reporting agent attempted to determine from SA (b)(6),(b)(7)(C) the status of the review of the forensic evidence. SA (b)(6),(b)(7)(C) advised that the computer forensic was conducted and evidence was obtained that was related to child pornographic material. SA (b)(6),(b)(7)(C) advised the reporting agent that he was requested by AUSA (b)(6),(b)(7)(C) to determine if (b)(6),(b)(7)(C) was still engaged in pornographic material.

16. On 22 October 2009, the reporting agent contacted AUSA (b)(6),(b)(7)(C) to determine the status of the potential for prosecution of (b)(6),(b)(7)(C) AUSA (b)(6),(b)(7)(C) advised the she has not received a forensic report from SA (b)(6),(b)(7)(C) AUSA (b)(6),(b)(7)(C) further advised that she is planning to close her case due to lack of information/evidence on the case. AUSA (b)(6),(b)(7)(C) stated that she may consider re-opening the case on (b)(6),(b)(7)(C) if the agents were able to provide evidence that (b)(6),(b)(7)(C) violated United States laws as codified under Exploitation of minors under Title 18 United States Code § 2252.

17. This investigation is closed based upon the lack of participation by the Immigration and Customs Enforcement to present the forensic evidence obtained during the course of the investigation to the U.S. Attorney's Office. This case may be re-opened if ICE presents this case for prosecution, and the U.S. Attorney's Office accepts this case for prosecution.

**IDENTITY OF SUBJECTS**

Name :  
Alias :  
Social Security Number :  
Date of Birth :  
Sex :  
Race :  
Height :  
Weight :  
Eyes :  
Hair :  
Residence :





(Investigations)

INSPECTOR GENERAL  
DEPARTMENT OF DEFENSE  
DEFENSE CRIMINAL INVESTIGATIVE SERVICE  
ARLINGTON RESIDENT AGENCY  
201 12TH STREET, SUITE 712  
ARLINGTON, VA 22202-5408

REPORT OF INVESTIGATION

200701274Z-14-JUN-2007-60DC-W1/F

April 9, 2009

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

DISTRIBUTION:

Defense Criminal Investigative Service Headquarters, National Security Program (03NS)  
Immigration and Customs Enforcement, SAC Washington, D.C. (SA <sup>(b)(6),(b)(7)(C)</sup>)

CLASSIFICATION:

~~FOR OFFICIAL USE ONLY~~

WARNING

This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without the specific prior authorization of the Deputy Inspector General for Investigations.

April 9, 2009

**NARRATIVE:**

1. On May 29, 2007, the DCIS Arlington Resident Agency (RA), initiated Project: Operation Flicker (CCN: 200701199X) based on information provided by Assistant U.S. Attorney (AUSA) Gerald Smagala, U.S. Attorney's Office (USAO), Eastern District of Virginia (EDVA), Alexandria Division. AUSA Smagala advised that the ICE was conducting a national investigation that identified over 5,000 individuals who subscribed to predicated child pornography websites. AUSA Smagala specifically requested DCIS assistance relative to any identifying DoD personnel.
2. SA Victor (b)(6) DCIS Arlington RA, utilized information contained within the DoD Employee Interactive Data System and the Joint Personnel Adjudication Systems to identify DoD affiliated individuals. Among those identified was (b)(6), an employee of Oracle Corporation who supported a contract for the National Security Agency. A query of JPAS revealed that (b)(6),(b)(7)(C) held a top secret clearance.
3. AUSA Smagala advised that (b)(6),(b)(7)(C) was previously identified in another ICE operation that collected subscriber information to predicated child pornography sites. In 2003, under Operation Falcon, ICE executed a search warrant in Florida of a credit card processing company called Regpay. Among the items seized during the warrant were subscriber records. (b)(6),(b)(7)(C) was 1 of 400 targets in Virginia who purchased subscriptions to various child pornography websites. (b)(6),(b)(7)(C) had approximately 21 purchases, making him the largest buyer in Virginia. In addition, two other people at (b)(6),(b)(7)(C) residence purchased approximately 11 additional subscriptions. A review of (b)(6),(b)(7)(C) credit card records revealed multiple purchases to child pornography websites. Federal search warrants were unattainable due to the staleness of the information gathered from Operation Falcon. (b)(6),(b)(7)(C) was never interviewed. However, under Operation Flicker, (b)(6),(b)(7)(C) was identified as making approximately four purchases.
4. On June 21, 2007, agents executed a search warrant on (b)(6),(b)(7)(C) residence located at (b)(6),(b)(7)(C) (b)(6),(b)(7)(C)
5. During a non-custodial interview of (b)(6),(b)(7)(C) he stated that he worked for (b)(6),(b)(7)(C) and he had been doing computer work for several years to include website consulting for (b)(6),(b)(7)(C)
6. (b)(6),(b)(7)(C) said that it was fair to say that he had an interest in child pornography for about 3 years prior to his interview. (b)(6),(b)(7)(C) said that he spent about \$50 to \$60 monthly on the various sexually explicit sites. (b)(6),(b)(7)(C) said that after each session on the computer (porn sites) he wiped the Internet history off the system. (b)(6),(b)(7)(C) said that there would be a mixture of pornography on the computer; there will be adult porn, child porn, and sexual activity with animals. (b)(6),(b)(7)(C) said that his wife had no knowledge of his pornography interests.

**WARNING**

This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without the specific prior authorization of the Deputy Inspector General for Investigations.



April 9, 2009

7. On June 20, 2007, SA (b)(6),(b)(7)(C) met with (b)(6),(b)(7)(C) representatives at their office located at (b)(6),(b)(7)(C). (b)(6),(b)(7)(C) representatives agreed to the release of both computers to SA (b)(6),(b)(7)(C) for forensic analysis. The (b)(6),(b)(7)(C) human resources manager advised that she was suspending all of (b)(6),(b)(7)(C) access to (b)(6),(b)(7)(C) and was putting (b)(6),(b)(7)(C) on administrative leave with pay.

9. On June 21, 2007, SA (b)(6),(b)(7)(C) received an email containing (b)(6),(b)(7)(C) parking records, related to (b)(6),(b)(7)(C) access to (b)(6),(b)(7)(C) offices on June 19, 2007, the date of the search warrant. According to the (b)(6),(b)(7)(C) parking records, (b)(6),(b)(7)(C) entered (b)(6),(b)(7)(C) parking garage on June 19, 2007 at 10:00:47 a.m. and exited at 11:06:00 a.m. It appeared that (b)(6),(b)(7)(C) travelled to his office at (b)(6),(b)(7)(C) after the search warrant on his residence, tampered with his (b)(6),(b)(7)(C) issued computers, and left his office.

10. On July 25, 2007, an additional search warrant was obtained for (b)(6),(b)(7)(C) issued desktop computer.

11. A forensic examination of (b)(6),(b)(7)(C) computers revealed images of child pornography.

12. On March 27, 2008, (b)(6),(b)(7)(C) was indicted in the U.S. District Court, Eastern District of Virginia, on two counts of attempted receipt of child pornography and possession of child pornography, a violation of Title 18, U.S. Code, Sections 2252A(a)(2) and 2252A(a)(5)(B).

13. SA (b)(6),(b)(7)(C) advised that (b)(6),(b)(7)(C) fled the U.S. and was believed to be in Libya. On March 28, 2008, an arrest warrant was issued for (b)(6),(b)(7)(C).

14. On September 10, 2008, Interpol Washington issued red notice for (b)(6),(b)(7)(C) arrest, reference number (b)(6),(b)(7)(C) of 2 September 2008.

15. Until (b)(6),(b)(7)(C) is arrested and extradited to the U.S., no further criminal, civil or administrative activity by the DCIS will occur. This case is closed as "finished."

## WARNING

This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without the specific prior authorization of the Deputy Inspector General for Investigations.

**IDENTITY OF SUBJECTS**

Name : (b)(6),(b)(7)(C)

Social Security Number : (b)(6),(b)(7)(C)

Date/Place of Birth : (b)(6),(b)(7)(C)

Race : (b)(6),(b)(7)(C)

Sex : (b)(6),(b)(7)(C)

Height : (b)(6),(b)(7)(C)

Weight : (b)(6),(b)(7)(C)

Hair : (b)(6),(b)(7)(C)

Eyes : (b)(6),(b)(7)(C)

Residence : (b)(6),(b)(7)(C)

Employment/Occupation : (b)(6),(b)(7)(C)

Telephone Number : (b)(6),(b)(7)(C)

Driver's License Number : (b)(6),(b)(7)(C)

and Issuing State : (b)(6),(b)(7)(C)

Passport Number : (b)(6),(b)(7)(C)

Education : (b)(6),(b)(7)(C)

Prepared by Special Agent (b)(6),(b)(7)(C) Arlington Resident Agency

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



Investigations)

**INSPECTOR GENERAL  
DEPARTMENT OF DEFENSE  
DEFENSE CRIMINAL INVESTIGATIVE SERVICE  
NEW HAVEN RESIDENT AGENCY  
265 CHURCH STREET  
SUITE 404  
NEW HAVEN, CT 06510**

**REPORT OF INVESTIGATION**

200701333L-25-JUN-2007-10HF-W1

21-NOVEMBER-2008

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



**Distribution**

DCIS Headquarters  
Northeast Field Office

**Table of Contents**

	<b><u>Section</u></b>
Narrative	A
Identity of Subjects	B

Narrative

1. This case was initiated upon referral of the Defense Contract Management Agency (DCMA), Hartford, CT. On March 14, 2007, (b)(6),(b)(7)(C) DCMA Hartford, requested DCIS assistance in evaluating possible child pornography images contained on the hard drive of a government owned computer assigned to (b)(6),(b)(7)(C), DCMA Hamilton Sundstrand.
2. In January 2007, DCMA received a complaint indicating that (b)(6),(b)(7)(C) was using his government computer to play games. DCMA Information Technology personnel remotely accessed (b)(6),(b)(7)(C) government computer and found evidence that he was accessing internet gaming websites and pornographic websites. On January 26, 2007, DCMA seized (b)(6),(b)(7)(C) government computer hard drive for analysis. During a subsequent analysis of the hard drive, DCMA forensic examiners identified images that they thought could constitute child pornography.
3. On March 14, 2007, (b)(6),(b)(7)(C) DCMA Hartford, requested DCIS assistance in reviewing the contents of (b)(6),(b)(7)(C) hard drive for evidence of child pornography. DCIS forensic examiners analyzed the hard drive, and identified approximately 40 images suspected of being child pornography. Each of these images was a so called "thumbnail" image, indicating that the image was reviewed on line, but was not downloaded. The images were run against the National Child Victim Identification Program (NCVIP), and none of the images was positively identified as a known child victim.
4. On May 18, 2007, the reporting agent met with Assistant United States Attorney (AUSA) (b)(6),(b)(7)(C) to review the "suspect" images contained on (b)(6),(b)(7)(C) hard drive. After reviewing the images, AUSA (b)(6),(b)(7)(C) indicated that while he believed the thumbnail images themselves did not constitute sufficient evidence to merit prosecution, any final decision regarding prosecution would have to be made by the Chief of the Criminal Division. Peter Jongbloed, Chief, Criminal Division, US Attorney's Office for the District of Connecticut, was briefed by the reporting agent and requested that DCIS interview (b)(6),(b)(7)(C) prior to any final decision on the disposition of the case.
5. On June 21, 2007, the reporting agent interviewed (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) admitted to playing on line games on his work computer for an average of three hours a day during his work day. He also admitted to accessing pornographic websites on his work computer during the work day, but denied ever downloading pornography on his work computer, and

denied ever intending to view or possess child pornography. (b)(6),(b)(7)(C) indicated that he also accessed pornography from his home computer, and over several years had downloaded approximately 5000 pornographic images on to a memory stick that he maintained at his home. When asked whether this memory stick contained images that would constitute child pornography, (b)(6),(b)(7)(C) stated that some of the images might "raise some eyebrows" and might be "questionable."

6. On June 22, 2007, (b)(6),(b)(7)(C) voluntarily relinquished the memory stick and agreed to allow DCIS to search the memory stick for evidence of child pornography. Given the volume of forensic analysis already accomplished, and the amount required to complete this inquiry, the decision to open an investigation was made on June 25, 2007.
7. The 2701 files contained on the memory stick were run against the National Child Victim Identification Program (NCVIP), and none of the images was positively identified as a known child victim. A number of suspect images were identified that possibly depicted minors engaged in sexual posing and sexual acts. Analysis of the images indicated that the individuals were not pre-teen in age, but pubescent and developed females, some of whom might be teenagers.
8. On October 11, 2007, the US Attorney's Office declined prosecution of (b)(6),(b)(7)(C) for possession of child pornography. The declination was based upon an inability to determine the age or identity of the individuals depicted in the files. (b)(6),(b)(7)(C) statement that he did not intend to possess child pornography, (b)(6),(b)(7)(C) cooperation in the investigation, and the number and nature of the vast majority of the images which were not child pornography.
9. On July 8, 2008, (b)(6),(b)(7)(C) completed a thirty day suspension imposed upon him by the Defense Contract Management Agency (DCMA). (b)(6),(b)(7)(C) suspension resulted from admissions he made to the reporting agent during an interview relating to his extensive misuse of government time and resources. DCMA (b)(6),(b)(7)(C) stated that she was attempting to recoup approximately \$20,000.00 from (b)(6),(b)(7)(C) through the Defense Finance and Accounting Service (DFAS). This amount represents the dollar value of the time (b)(6),(b)(7)(C) spent computer gaming during the workday.
10. On November 17, 2008, DCMA (b)(6),(b)(7)(C) advised that she was unsuccessful in recouping funds from (b)(6),(b)(7)(C) through DFAS.
11. This case is closed. There were no management control deficiencies identified during the course of this investigation.

SIFICATION:

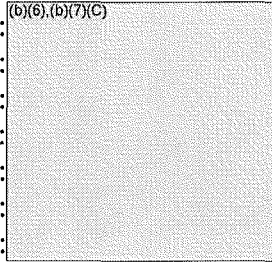
**FOR OFFICIAL USE ONLY**

**WARNING**

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without the specific prior authorization of the Deputy Inspector General for Investigations.~~

**Identity of Subject**

Name  
DoB  
SSN  
Alias  
Race  
Sex  
Employment/Occupation



Prepared by SA (b)(6), (b)(7)(C) New Haven RA

APR: (b)(6), (b)(7)(C)



(Investigations)

INSPECTOR GENERAL  
DEPARTMENT OF DEFENSE  
DEFENSE CRIMINAL INVESTIGATIVE SERVICE  
VALENCIA RESIDENT AGENCY  
25350 MAGIC MOUNTAIN PARKWAY  
SUITE 200  
VALENCIA, CA 91355

REPORT OF INVESTIGATION

200701558M-31-JUL-2007-50VN-W1

August 14, 2009

DOD-RELATED CHILD PORNOGRAPHERS – NORTHERN LOS ANGELES

DISTRIBUTION

Western Field Office  
ICE – Camarillo  
ICE – Bakersfield

CLASSIFICATION:

~~FOR OFFICIAL USE ONLY~~

WARNING

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without the specific prior authorization of the Deputy Inspector General for Investigations.~~



**NARRATIVE**

1. This investigation was initiated based upon a referral from SA (b)(6),(b)(7)(C) DCIS Arlington Resident Agency, identifying thirteen persons with ties to the Department of Defense who reside in the DCIS Valencia Resident Agency area of responsibility and were suspected of involvement in child pornography. SA (b)(6),(b)(7)(C) initially received the information from Assistant United States Attorney (AUSA) Gerald Smagala, United States Attorney's Office (USAO), Eastern District of Virginia. The persons identified are active and retired military members, DoD civilians and DoD contractor employees, several of whom have Top Secret or higher clearances.

2. In April 2006, the ICE/Cyber Crimes Center/Child Exploitation Section (ICE/C3/CES) initiated an investigation into a criminal organization operating a commercial child pornography website known as "Home Collection." The investigation revealed that the organization operated numerous commercial child pornography websites. In addition, the organization utilized various PayPal accounts to process the payments for access to the member restricted websites. The investigation was worked jointly with ICE/C3/CES, ICE/RAC/Birmingham, the U.S. Postal Inspection Service, the U.S. Department of Justice/Child Exploitation and Obscenity Section, and the USAO for the Northern District of Alabama. ICE designated this operation 'Project Flicker'.

3. ICE/C3/CES conducted over 60 undercover transactions with the advertising websites associated with this investigation. The investigation determined that a specific criminal organization operated approximately 18 commercial child pornography portal websites which provided access to approximately 18 child pornography member-restricted websites, using a specific payment website known as "iWest." The investigation identified that the criminal organization (1) used various PayPal accounts to facilitate the customer payments; (2) used specific subject identifiers within the PayPal accounts to identify purchases into the various member restricted websites; and (3) used specific administrative e-mail accounts that were used to distribute access to the member-restricted websites.

4. Project Flicker data was sorted to identify individuals who used their personal e-mail addresses, .mil e-mail addresses, Fleet Post Office or Army Post Office military zip codes to register for the PayPal service to gain access the child pornography websites. The thirteen suspects identified in the 50VN AOR were titled as subjects based upon the initial evidence that was provided to the DCIS by ICE. Because the subjects are DoD employees who possess security clearances, ICE listed them as a Tier 1 priority. This investigation was coordinated with ICE Supervisory Special Agent (b)(6),(b)(7)(C) Child Exploitation Unit, Long Beach, CA. ICE Senior Special Agent (b)(6),(b)(7)(C) of ICE Long Beach, Special Agent (b)(6),(b)(7)(C) of ICE Bakersfield, and Special Agent (b)(6),(b)(7)(C) of ICE Camarillo were assigned as case agents.

5. (b)(6),(b)(7)(C) is the husband of (b)(6),(b)(7)(C) a Navy E-5. (b)(6),(b)(7)(C) was interviewed by SA (b)(6),(b)(7)(C) about his alleged purchases of child pornography. At the conclusion of the interview,

SA <sup>(b)(6),(b)(7)(C)</sup> determined that <sup>(b)(6),(b)(7)(D)</sup> purchase was accidental and not indicative of criminal behavior. SA <sup>(b)(6),(b)(7)(C)</sup> interview was reviewed by the AUSA's office in Fresno, CA and prosecution against <sup>(b)(6),(b)(7)(C)</sup> was declined.

6. <sup>(b)(6),(b)(7)(C)</sup> a civilian contractor at Edwards Air Force Base, CA, purchased two subscriptions to two different websites featuring child pornography on two separate occasions, for a duration of one month on each subscription. When ICE agents executed the search warrant at <sup>(b)(6),(b)(7)(C)</sup> home on February 28, 2008, <sup>(b)(6),(b)(7)(C)</sup> was present and was interviewed by SA <sup>(b)(6),(b)(7)(C)</sup> and SA <sup>(b)(6),(b)(7)(C)</sup>. During the interview <sup>(b)(6),(b)(7)(C)</sup> stated that the computer he used to access the websites was located at the residence, and that he relied on disclaimers posted on the websites stating that the material was legal. <sup>(b)(6),(b)(7)(C)</sup> further stated that he never downloaded or saved any images or movies from the websites to his computer. The search of <sup>(b)(6),(b)(7)(C)</sup> residence revealed no child pornography at the residence or on his computer. Due to lack of evidence, ICE closed their investigation on <sup>(b)(6),(b)(7)(C)</sup> (Exhibit 1).

7. Christopher Oswald, a telephone maintenance worker at Naval Air Station, Pt Mugu CA, was arrested on August 6, 2008, based on evidence discovered at his home during a California State search warrant executed by members of the Ventura County Sheriff's Office High Tech Task Force, ICE Camarillo, and DCIS. He was convicted on two counts of possession of child pornography under CA Penal Code 311.11(a) and sentenced to 16 months incarceration, in addition to registration with the National Sex Offender Registry. Oswald was also administratively separated from his employment as a telephone installer on May 16, 2009 (Exhibits 2, 4, 5, 6).

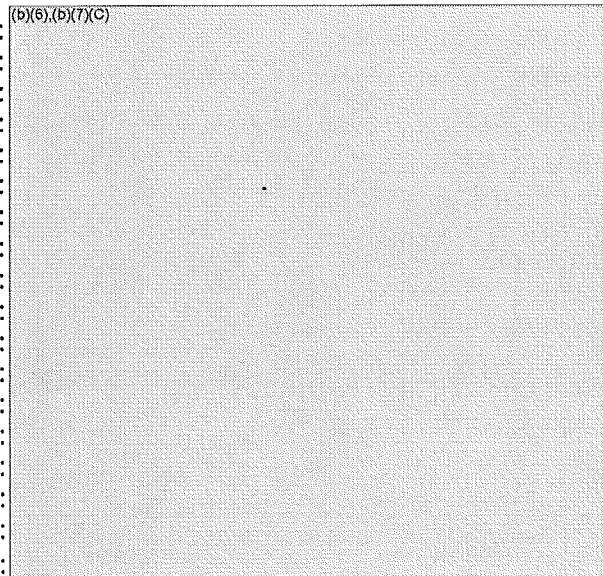
8. <sup>(b)(6),(b)(7)(C)</sup> Naval Air Warfare Center, China Lake CA, was being investigated by the Ridgecrest Police Department after <sup>(b)(6),(b)(7)(C)</sup> turned over his personal computer to a computer repair store for a hard drive swap. The repair technician discovered thousands of possible child pornography images and notified the police. <sup>(b)(6),(b)(7)(C)</sup> admitted to possessing the images and agreed to a search of his home. Before Deputy District Attorney <sup>(b)(6),(b)(7)(C)</sup> could formally charge him, <sup>(b)(6),(b)(7)(C)</sup> died on July 6, 2009 of chronic obstructive pulmonary disease (Exhibits 3, 7).

9. For the remaining nine individuals, it was determined that the probable cause for search warrants was stale and that current, relevant evidence was not available. It was also determined that a portion of the original basis for the referral was unsubstantiated. The referral indicated that the subjects used their .mil accounts to register for and/or conduct the illegal purchase of child pornography. The use of a .mil account, in conjunction with the subjects' military service connections, was considered sufficient nexus to initiate an investigation, but subsequent investigation of these thirteen suspects revealed no .mil accounts were used.

10. With all relevant criminal activity addressed, this investigation is closed. No further judicial or administrative activity will occur. There were no management control deficiencies identified during the course of this investigation.

**IDENTITY OF SUBJECTS**

Name  
Alias  
Social Security Number  
Date of Birth  
Place of Birth  
Race  
Sex  
Height/Weight  
Hair  
Eyes  
Residence  
Employment  
Occupation  
Telephone Number Home  
Telephone Number Bus  
Drivers License Number/Issuing State  
Dependents  
Identifying Characteristics

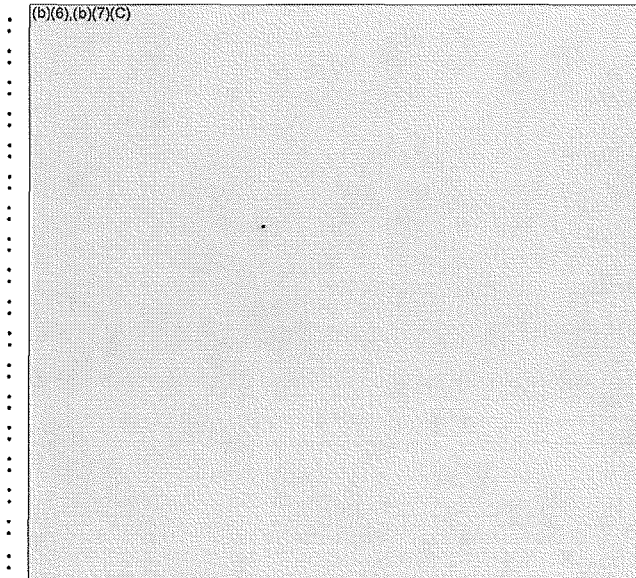


**IDENTITY OF SUBJECTS**

Name	:	Christopher Lester Oswald
Alias	:	Chris Oswald
Social Security Number	:	(b)(6),(b)(7)(C)
Date of Birth	:	
Place of Birth	:	
Race	:	
Sex	:	
Height/Weight	:	
Hair	:	
Eyes	:	
Residence	:	
Employment	:	Unemployed
Occupation	:	Telecommunications Repair
Telephone Number Home	:	(b)(6),(b)(7)(C)
Telephone Number Bus	:	
Drivers License Number/Issuing State	:	
Dependents	:	
Identifying Characteristics	:	

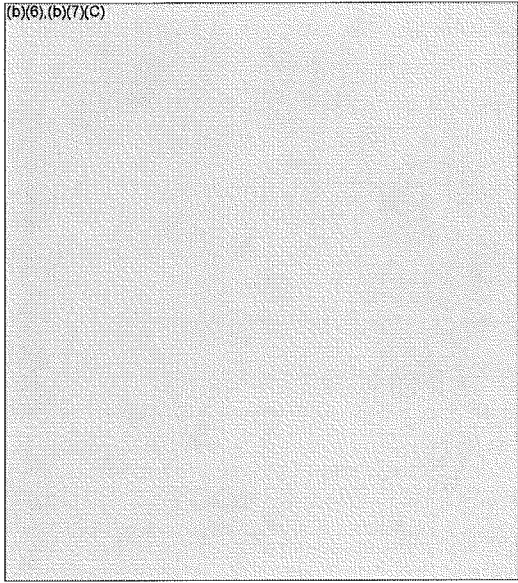
**IDENTITY OF SUBJECTS**

Name  
Alias  
Social Security Number  
Date of Birth  
Place of Birth  
Race  
Sex  
Height/Weight  
Hair  
Eyes  
Residence  
Employment  
Occupation  
Telephone Number Home  
Telephone Number Bus  
Drivers License Number/Issuing State  
Dependents  
Identifying Characteristics



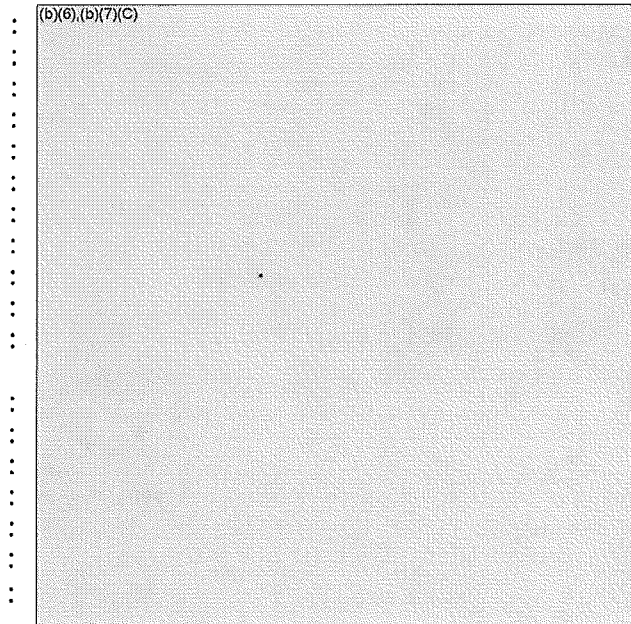
**IDENTITY OF SUBJECTS**

Name  
Alias  
Social Security Number  
Date of Birth  
Place of Birth  
Race  
Sex  
Height/Weight  
Hair  
Eyes  
Residence  
Employment  
Occupation  
Telephone Number Home  
Telephone Number Bus  
Drivers License Number/Issuing State  
Dependents  
Identifying Characteristics



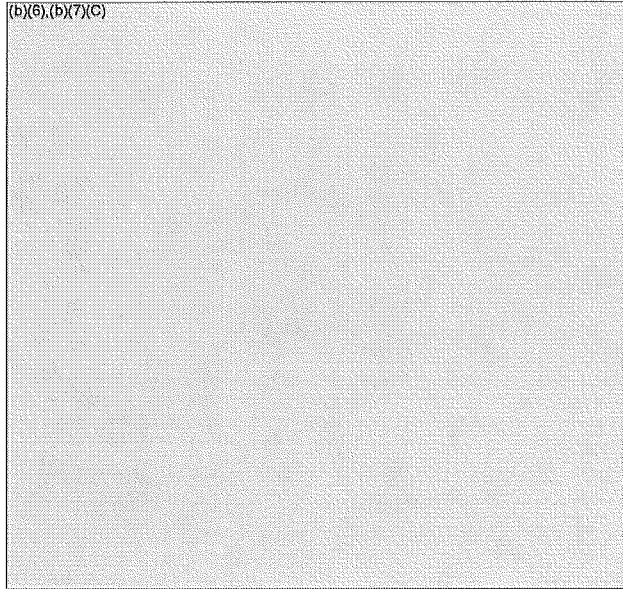
**IDENTITY OF SUBJECTS**

Name  
Alias  
Social Security Number  
Date of Birth  
Place of Birth  
Race  
Sex  
Height/Weight  
Hair  
Eyes  
Residence  
  
Employment  
Occupation  
Telephone Number Home  
Telephone Number Bus  
Drivers License Number/Issuing State  
Dependents  
Identifying Characteristics



**IDENTITY OF SUBJECTS**

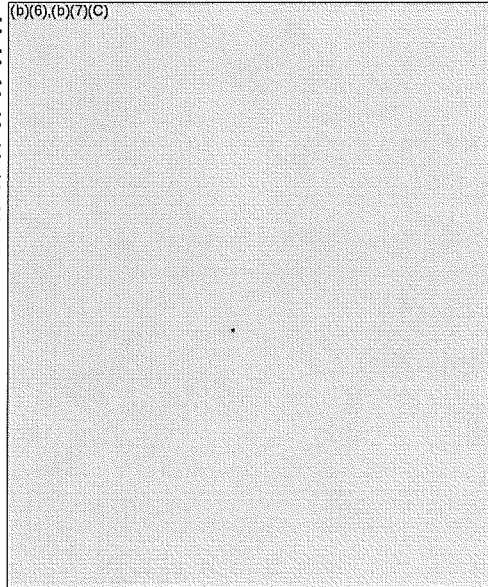
Name  
Alias  
Social Security Number  
Date of Birth  
Place of Birth  
Race  
Sex  
Height/Weight  
Hair  
Eyes  
Residence  
Employment  
Occupation  
Telephone Number Home  
Telephone Number Bus  
Drivers License Number/Issuing State  
Dependents  
Identifying Characteristics





**IDENTITY OF SUBJECTS**

Name  
Alias  
Social Security Number  
Date of Birth  
Place of Birth  
Race  
Sex  
Height/Weight  
Hair  
Eyes  
Residence  
Employment  
Occupation  
Telephone Number Home  
Telephone Number Bus  
Drivers License Number/Issuing State  
Dependents  
Identifying Characteristics





(Investigations)

**DEPARTMENT OF DEFENSE  
INSPECTOR GENERAL  
DEFENSE CRIMINAL INVESTIGATIVE SERVICE  
ARLINGTON RESIDENT AGENCY  
201 12<sup>TH</sup> STREET SOUTH, SUITE 712  
ARLINGTON, VIRGINIA 22202-5408**

**REPORT OF INVESTIGATION**

**200701571Z-01-AUG-2007-60DC-W1/F**

**November 24, 2009**

**FITZPATRICK, LELAND CHACE**

**DISTRIBUTION:**

**DCIS Headquarters, National Security Program (03NS)**

CLASSIFICATION:

**FOR OFFICIAL USE ONLY  
LAW ENFORCEMENT SENSITIVE**

**WARNING**

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without specific prior authorization of the Deputy Inspector General for Investigations.~~

**NARRATIVE:**

1. This case was initiated based on information derived from Defense Criminal Investigative Service (DCIS) Project: Operation Flicker (Case Control Number 200701199X).

2. As background, the DCIS Arlington Resident Agency, initiated Project: Operation Flicker based on information provided by Assistant U.S. Attorney (AUSA) Gerald Smagala, U.S. Attorney's Office, Eastern District of Virginia (EDVA), Alexandria Division. AUSA Smagala advised that the Immigration and Customs Enforcement was conducting a national investigation that identified over 5,000 individuals who subscribed to predicated child pornography websites. AUSA Smagala specifically requested DCIS assist in identifying DoD affiliated individuals and provide investigative assistance.

3. Leland Chace Fitzpatrick was identified as (b)(6),(b)(7)(C)  
(b)(6),(b)(7)(C)  
(b)(6),(b)(7)(C)

4. On August 2, 2007, agents executed a search warrant on Fitzpatrick's residence located at (b)(6),(b)(7)(C) Subsequent to the execution of the search warrant, agents conducted a non-custodial interview of Fitzpatrick. (b)(6),(b)(7)(C)  
(b)(6),(b)(7)(C)

5. A forensic examination of an external hard drive seized from Fitzpatrick's residence during the course of the search warrant, contained 93 documents, 8,400 pictures, and 200 movies that were evidence of the receipt of child pornography.

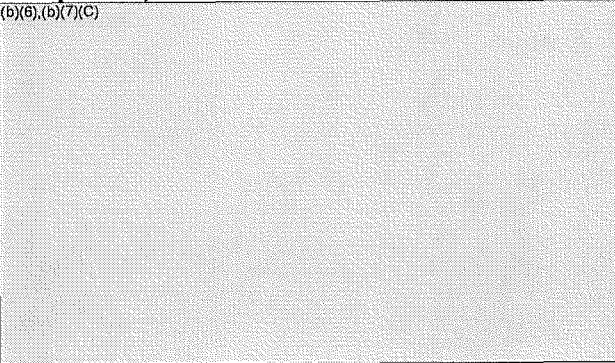
6. On September 24, 2008, Fitzpatrick was arrested based on a criminal complaint issued on September 16, 2008 by the U.S. District Court, EDVA.

7. On November 12, 2008, Fitzpatrick was indicted on one count of Title 18, U.S. Code, Sections 2252A(a)(2), receipt of child pornography, 2252A(a)(5)(B), possession of child pornography.

8. On February 9, 2009, Fitzpatrick pled guilty to Title 18, U.S. Code, Section 2252A(a)(2), receipt of child pornography. The count of Title 18, U.S. Code Section 2252A(a)(5)(B), possession of child pornography was dismissed.

9. On May 1, 2009, Fitzpatrick was sentenced to 60 months imprisonment, 60 months supervised release, and ordered to pay a \$100 special assessment fee.

**IDENTIFY OF SUBJECTS:**

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

**WARNING**

This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without specific prior authorization of the Deputy Inspector General for Investigations.

**EXHIBITS:**

None.

Prepared by Special Agent (b)(6),(b)(7)(C) Arlington Resident Agency      APPR: (b)(6),(b)(7)(C)

C-1

CLASSIFICATION:

~~FOR OFFICIAL USE ONLY~~  
~~LAW ENFORCEMENT SENSITIVE~~

**WARNING**

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without specific prior authorization of the Deputy Inspector General for Investigations.~~



(Investigations)

INSPECTOR GENERAL  
DEPARTMENT OF DEFENSE  
DEFENSE CRIMINAL INVESTIGATIVE SERVICE  
DAYTON RESIDENT AGENCY  
3055 KETTERING BLVD, #205  
DAYTON, OH 45439

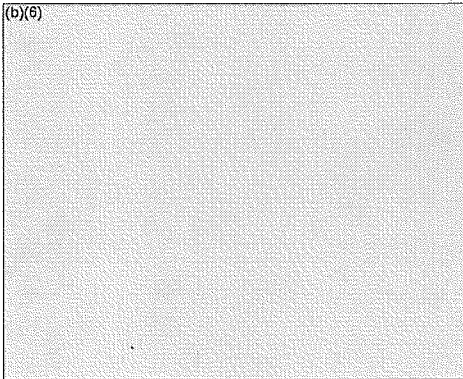
REPORT OF INVESTIGATION

200701765V-10-SEP-2007-40DY-W1/Z

31-OCTOBER-2008

**PROJECT FLICKER – SDOH (Western Division) – WDKY – EDKY**

(b)(6)



Distribution  
DCIS Headquarters  
Central Field Office

CLASSIFICATION:

~~FOR OFFICIAL USE ONLY~~

**WARNING**

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without the specific prior authorization of the Deputy Inspector General for Investigations.~~

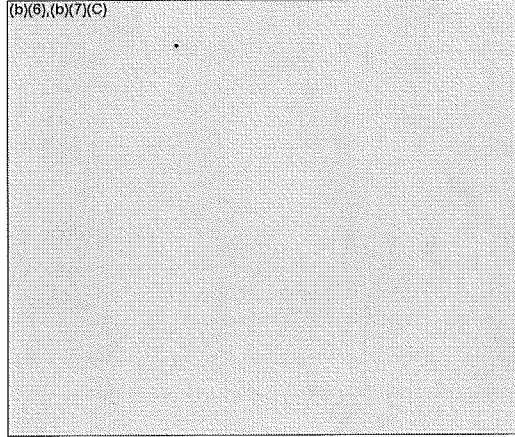
NARRATIVE

1. This project was initiated based upon information and a request from the DCIS Mid-Atlantic Field Office regarding information received from Project Flicker, an Immigration and Customs Enforcement (ICE) national undercover investigation into commercial child pornography websites.
2. Project Flicker identified over 5,000 individuals who subscribed to the commercial child pornography websites that were targeted by ICE. The names and identifying data on the individuals who subscribed to the commercial child pornography websites were checked against the Department of Defense (DoD) databases to identify those individuals who were associated with the DoD and subscribing to child pornography.
3. Child pornography is illegal and subscribers of commercial child pornography that are associated with the DoD put the DoD, the military and national security at risk by compromising computer systems, military installations and security clearances to name a few. Additionally, it puts the DoD at risk of blackmail, bribery, and threats, especially since these individuals typically have access to military installations.
4. This investigation developed sufficient information for three (3) Federal Search Warrants (subjects (b)(6), (b)(7)(C)), one (1) criminal charge (b)(6), (b)(7)(C) and one (1) arrest (b)(6), (b)(7)(C)
5. As dictated by DCIS Headquarters, this project is canceled. Additionally, a conclusion about Management Control Deficiencies could not be made.

**IDENTITY OF SUBJECTS**

Name:  
Social Security Number:  
Date/Place of Birth:  
Race:  
Sex:  
Height:  
Weight:  
Residence:

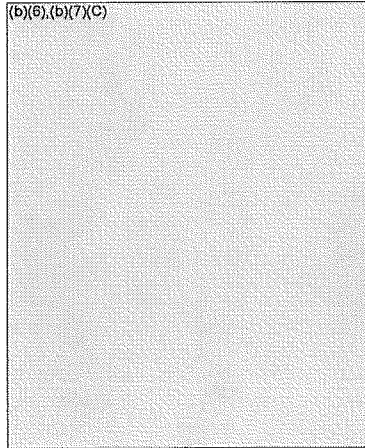
Home Phone Number:  
Driver's License Number:  
Employment/Occupation:





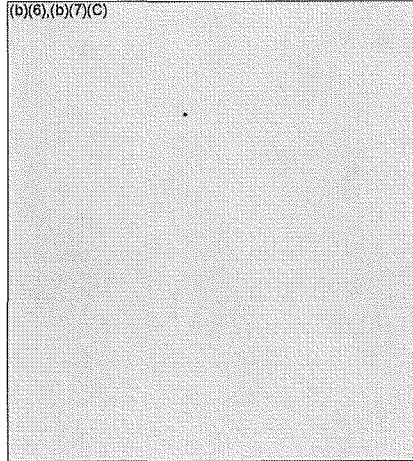
**IDENTITY OF SUBJECTS**

Name:  
Social Security Number:  
Date/Place of Birth:  
Race:  
Sex:  
Height:  
Weight:  
Residence:  
  
Home Phone Number:  
Driver's License Number:  
Employment/Occupation:



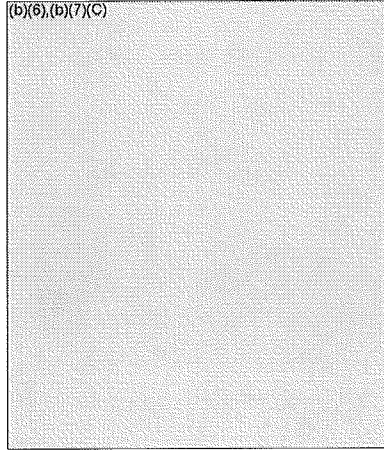
**IDENTITY OF SUBJECTS**

Name:  
Social Security Number:  
Date/Place of Birth:  
Race:  
Sex:  
Height:  
Weight:  
Residence:  
  
Home Phone Number:  
Driver's License Number:  
Employment/Occupation:



**IDENTITY OF SUBJECTS**

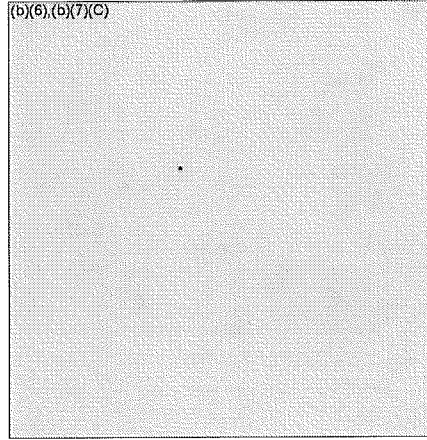
Name:  
Social Security Number:  
Date/Place of Birth:  
Race:  
Sex:  
Height:  
Weight:  
Residence:  
  
Home Phone Number:  
Driver's License Number:  
Employment/Occupation:



**IDENTITY OF SUBJECTS**

Name:  
Social Security Number:  
Date/Place of Birth:  
Race:  
Sex:  
Height:  
Weight:  
Residence:

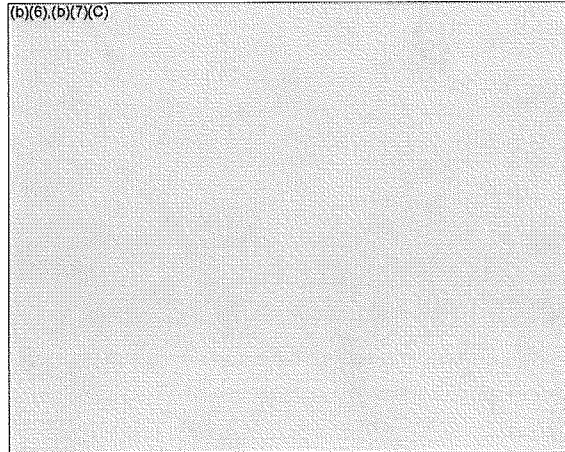
Home Phone Number:  
Driver's License Number:  
Employment/Occupation:



**IDENTITY OF SUBJECTS**

Name:  
Social Security Number:  
Date/Place of Birth:  
Race:  
Sex:  
Height:  
Weight:  
Residence:

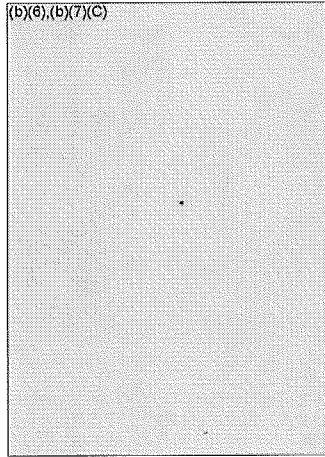
Home Phone Number:  
Driver's License Number:  
Employment/Occupation:



**IDENTITY OF SUBJECTS**

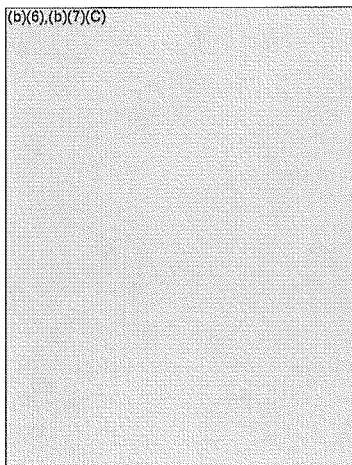
Name:  
Social Security Number:  
Date/Place of Birth:  
Race:  
Sex:  
Height:  
Weight:  
Residence:

Home Phone Number:  
Driver's License Number:  
Employment/Occupation:



**IDENTITY OF SUBJECTS**

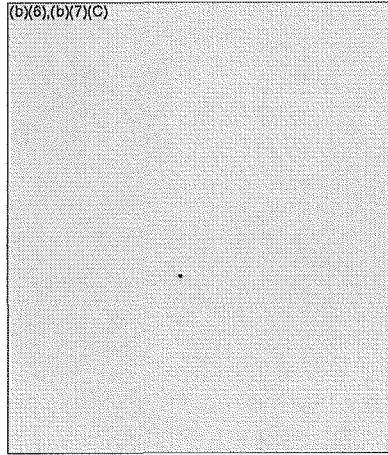
Name:  
Social Security Number:  
Date/Place of Birth:  
Race:  
Sex:  
Height:  
Weight:  
Residence:  
  
Home Phone Number:  
Driver's License Number:  
Employment/Occupation:



**IDENTITY OF SUBJECTS**

Name:  
Social Security Number:  
Date/Place of Birth:  
Race:  
Sex:  
Height:  
Weight:  
Residence:

Home Phone Number:  
Driver's License Number:  
Employment/Occupation:

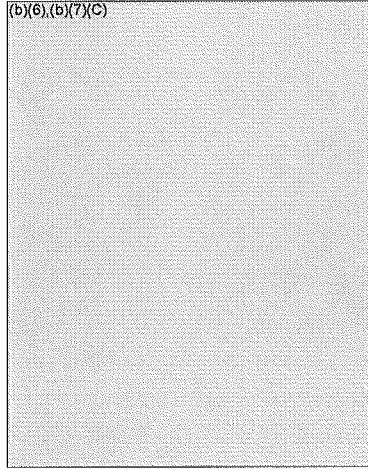




**IDENTITY OF SUBJECTS**

Name:  
Social Security Number:  
Date/Place of Birth:  
Race:  
Sex:  
Height:  
Weight:  
Residence:

Home Phone Number:  
Driver's License Number:  
Employment/Occupation:



Prepared by SA (b)(6),(b)(7)(C) Dayton RA

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

CLASSIFICATION:

~~FOR OFFICIAL USE ONLY~~

WARNING



(Investigations)

INSPECTOR GENERAL  
DEPARTMENT OF DEFENSE  
DEFENSE CRIMINAL INVESTIGATIVE SERVICE  
NORFOLK RESIDENT AGENCY  
200 GRANBY ST, STE 412  
NORFOLK, VA 23510-1811

REPORT OF INVESTIGATION

200701862T-19-SEP-2007-60NF-W1/F

February 10, 2009

STOKES, CHRISTOPHER MICHAEL

DISTRIBUTION

DCIS Headquarters (03NS)  
Mid-Atlantic Field Office (60FO)

CLASSIFICATION:

~~FOR OFFICIAL USE ONLY~~

WARNING

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without the specific prior authorization of the Deputy Inspector General for Investigations.~~

**NARRATIVE**

1. This case was initiated based on information derived from Operation Flicker (UID: 200701199X). On May 29, 2007, DCIS initiated Operation Flicker based on a request and information provided by Assistant United States Attorney (AUSA) Gerald Smagala, United States Attorneys Office (USAO), Eastern District of Virginia (EDVA), Alexandria, VA. AUSA Smagala advised that the U.S. Immigration and Customs Enforcement (ICE) was conducting a national investigation that identified over 5,000 individuals who allegedly subscribed to predicated child pornography websites. AUSA Smagala specifically requested that DCIS assist in identifying DoD affiliated individuals among those subscribers. Utilizing the information developed by ICE, Christopher Stokes, a U.S. Government employee (GS-11) at the National Defense University, Norfolk, VA, was identified as a subject who reportedly made two purchases from at least one of the predicated child pornography websites. During the course of the investigation, it was confirmed that Stokes resided at (b)(6),(b)(7)(C)

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

2. Evidence collected during the course of this investigation revealed that on October 11, 2006 and again on December 29, 2006, Stokes (b)(6),(b)(7)(C)

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

3. On October 11, 2007, DCIS executed a federal search warrant at Stokes' residence with the assistance of ICE and the Norfolk Police Department. During the execution of the warrant, numerous items were seized including a computer, hard drive, and numerous compact disks (CDs). Stokes was present during the execution of the search warrant and consented to an interview. During the interview, Stokes provided a written statement and consented to a search of his personal vehicle located in the parking lot of the apartment complex. During the interview, (b)(6),(b)(7)(C)

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

4. (b)(6),(b)(7)(C) Computer Forensic Analyst, USAO, EDVA, Newport News, VA, performed a forensic analysis of various computer related equipment seized during the execution of the search warrant. In addition, Special Agent (b)(6),(b)(7)(C) ICE, Norfolk Office, also examined two CDs, which were seized during the execution of the search warrant, confirming that they contained images of child pornography.

5. On April 11, 2008, AUSA (b)(6),(b)(7)(C) Norfolk Division, Criminal Section, filed a Criminal Information with the U.S. District Court, EDVA, Norfolk, VA, which charged Stokes with Possession of Material Containing Child Pornography (Title 18, U.S. Code, Section

2252(a)(5)(B)) and Criminal Forfeiture (Title 18, U.S. Code, Section 2253).

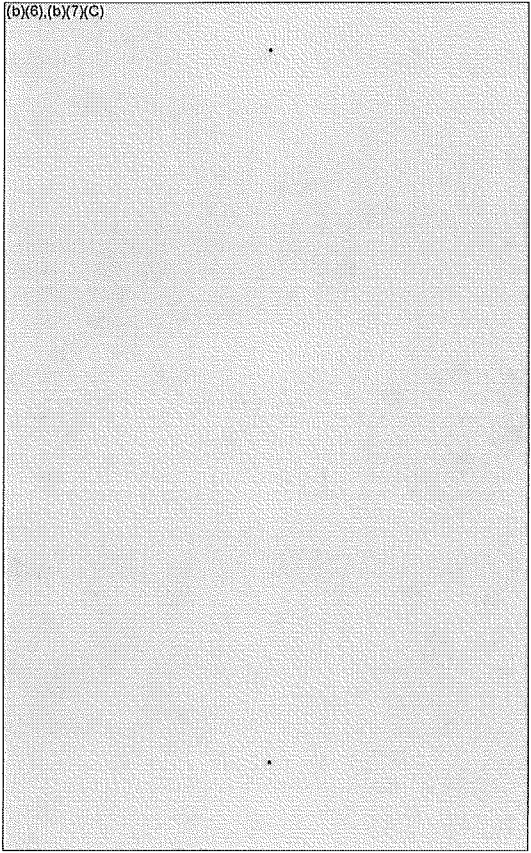
6. On May 20, 2008, Stokes pled guilty in U.S. District Court, EDVA, Norfolk to the single count Criminal Information filed on April 11, 2008, charging him with Possession of Material Containing Child Pornography. As part of his guilty plea, Stokes agreed to forfeit assorted computer equipment and digital media which contained and facilitated the viewing of child pornography.
7. On October 24, 2008, pursuant to his guilty plea, Stokes was sentenced by Senior United States District Judge Henry Coke Morgan, Jr. in U.S. District Court, EDVA, Norfolk to 60 months confinement and lifetime supervised release. In addition, Stokes was ordered to immediately pay \$12,500 in fines, as a \$100 Special Assessment had already been paid to the court. Additional rules were established concerning Stokes' supervised release, which are to be monitored by his Probation Officer upon his release from confinement. Stokes was allowed to remain on bond pending notification of his assignment to a federal penitentiary.
8. On January 12, 2009, the Final Order of Forfeiture was signed by Senior United States District Judge Henry Coke Morgan, Jr., and filed in the U.S. District Court, EDVA, Norfolk.
9. All investigative and judicial actions have been completed. No fraud vulnerabilities were uncovered during the course of this investigation.
10. This investigation is now closed as finished.

**IDENTITY OF SUBJECTS**

**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 :

**Christopher Michael Stokes**



Prepared by Special Agent (b)(6),(b)(7)(C) Norfolk RA

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



(Investigations)

DEPARTMENT OF DEFENSE  
INSPECTOR GENERAL  
DEFENSE CRIMINAL INVESTIGATIVE SERVICE  
ARLINGTON RESIDENT AGENCY  
201 12<sup>TH</sup> STREET SOUTH, SUITE 712  
ARLINGTON, VIRGINIA 22202-5408

**REPORT OF INVESTIGATION**

200701653I-16-AUG-2007-60DC-W1/A

November 30, 2009

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

**DISTRIBUTION:**

DCIS Headquarters, National Security Program (03NS)

CLASSIFICATION:

~~FOR OFFICIAL USE ONLY~~  
~~LAW ENFORCEMENT SENSITIVE~~

**WARNING**

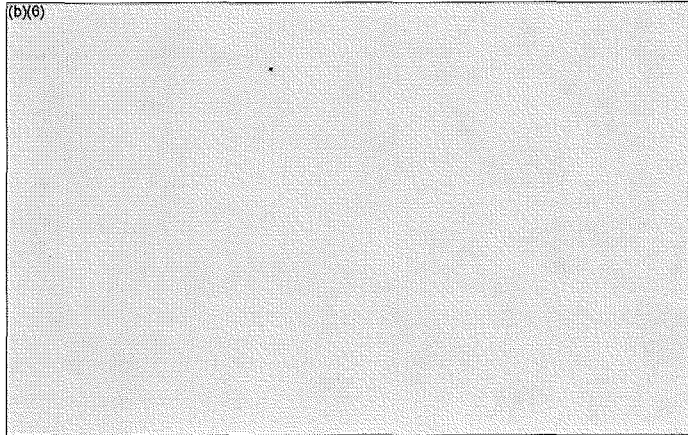
~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without specific prior authorization of the Deputy Inspector General for Investigations.~~

**NARRATIVE:**

1. This case was initiated based on information derived from Defense Criminal Investigative Service (DCIS) Project: Operation Flicker (Case Control Number 200701199X).
2. As background, the DCIS Arlington Resident Agency, initiated Project: Operation Flicker based on information provided by Assistant U.S. Attorney (AUSA) Gerald Smagala, U.S. Attorney's Office, Eastern District of Virginia (EDVA), Alexandria Division. AUSA Smagala advised that the Immigration and Customs Enforcement (ICE) was conducting a national investigation that identified over 5,000 individuals who subscribed to predicated child pornography websites. AUSA Smagala specifically requested DCIS assist in identifying DoD affiliated individuals and provide investigative assistance.
3. (b)(6),(b)(7)(C) was identified as an employee of Audio Video Systems, Incorporated, a DoD contractor.
4. On August 15, 2007, agents executed a search warrant on (b)(6),(b)(7)(C) residence located at (b)(6),(b)(7)(C). Subsequent to the execution of the search warrant, agents conducted a non-custodial interview of (b)(6),(b)(7)(C). (b)(6),(b)(7)(C) admitted to subscribing to approximately five websites that offered child pornography images. (b)(6),(b)(7)(C) stated he was looking for images of high school age girls. (b)(6),(b)(7)(C) admitted to viewing pornographic images of individuals under age 18. (b)(6),(b)(7)(C) stated he knew it was wrong.
5. Due to a lack of resources, this case will be closed. ICE, as the lead investigative agency, will be responsible for the final adjudication of this matter. No management control deficiencies were identified during this investigation.

**IDENTIFY OF SUBJECTS:**

Name	:	
Alias	:	
Social Security Number	:	
Date/Place of Birth	:	
Race	:	
Sex	:	
Height	:	
Weight	:	
Hair	:	
Eyes	:	
Residence	:	
Employment/Occupation	:	Unknown
Telephone Number	:	Unknown
Driver's License Number	:	Unknown
and Issuing State	:	Unknown
Education	:	Unknown



**WARNING**

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without specific prior authorization of the Deputy Inspector General for Investigations.~~



**EXHIBITS:**

None.

Prepared by Special Agent (b)(6),(b)(7)(C) Arlington Resident Agency APPR: (b)(6),(b)(7)(C)

C-1

CLASSIFICATION:

**~~FOR OFFICIAL USE ONLY~~**  
**~~LAW ENFORCEMENT SENSITIVE~~**

**WARNING**

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without specific prior authorization of the Deputy Inspector General for Investigations.~~



(Investigations)

**DEPARTMENT OF DEFENSE  
OFFICE OF INSPECTOR GENERAL  
DEFENSE CRIMINAL INVESTIGATIVE SERVICE  
ARLINGTON RESIDENT AGENCY  
201 12<sup>th</sup> STREET SOUTH, SUITE 712  
ARLINGTON, VIRGINIA 22202-5408**

**REPORT OF INVESTIGATION**

**200701665U-17-AUG-2007-60DC-W1/D**

**December 30, 2008**

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

**DISTRIBUTION:**

**DCIS Headquarters, National Security Program (03NS)  
Immigration and Customs Enforcement, SAC Washington, DC (Attn: (b)(6), (b)(7)(C))**

CLASSIFICATION:

**~~FOR OFFICIAL USE ONLY~~  
~~LAW ENFORCEMENT SENSITIVE~~**

**WARNING**

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without specific prior authorization of the Deputy Inspector General for Investigations.~~

**NARRATIVE:**

1. This case was initiated based on information derived from DCIS Project: Operation Flicker (Case Control Number 200701199X). The project identified (b)(6),(b)(7)(C) former U.S. Navy reservist (E-05), as an individual who downloaded child pornography.
2. As background, Immigration and Customs Enforcement (ICE) initiated an investigation into a criminal organization operating a commercial child pornography website known as "Home Collection." The investigation revealed "Home Collection" was operating numerous commercial child pornography websites. In addition, the organization utilized various PayPal accounts to process the payments for access to the member-restricted websites. Assistant United States Attorney (AUSA) Gerald Smagala, Eastern District of Virginia, requested DCIS assist in identifying individuals affiliated with the DoD and provide investigative assistance. In response, the DCIS Arlington Resident Agency (RA) initiated Operation Flicker.
3. The criminal organization utilized a specific and identifiable payment website known as "iWest." The information developed during the course of the investigation identified that the organization (1) used various PayPal accounts to facilitate the customer payments; (2) used specific subject identifiers within the PayPal accounts to identify purchases of subscriptions to various member restricted websites; and (3) used specific administrative e-mail accounts that were used to distribute access to the member restricted websites.
4. SA (b)(6),(b)(7)(C) DCIS Arlington RA, utilized information contained within the DoD Employee Interactive Data System and the Joint Personnel Adjudication Systems (JPAS) to identify DoD personnel and contract employees who joined the member restricted sites. Among those identified was (b)(6),(b)(7)(C)
5. On August 29, 2007, DCIS and ICE executed a search warrant at (b)(6),(b)(7)(C) based on evidence (b)(6),(b)(7)(C) resided there. Upon entry, it was determined (b)(6),(b)(7)(C) no longer resided there. The occupants related (b)(6),(b)(7)(C) continued to receive mail at that address. It was later determined (b)(6),(b)(7)(C) new address was (b)(6),(b)(7)(C)
6. On August 29, 2007, SA (b)(6),(b)(7)(C) interviewed (b)(6),(b)(7)(C) owner of the property at (b)(6),(b)(7)(C) rented a room at (b)(6),(b)(7)(C) Drive for over a year. During his occupancy, (b)(6),(b)(7)(C) had three roommates, (b)(6),(b)(7)(C) moved out of (b)(6),(b)(7)(C) on February 1, 2007. (b)(6),(b)(7)(C) informed (b)(6),(b)(7)(C) he was moving to find cheaper rent. (b)(6),(b)(7)(C) believed (b)(6),(b)(7)(C) was a (b)(6),(b)(7)(C) at Fair Oaks Mall, Fairfax, VA.
7. On August 29, 2007, (b)(6),(b)(7)(C) Information Control Officer, Virginia Employment Commission, provided SA (b)(6),(b)(7)(C) employment data. Quirk informed (b)(6),(b)(7)(C) employed (b)(6),(b)(7)(C) SA (b)(6),(b)(7)(C) contacted (b)(6),(b)(7)(C) in Fair Oaks Mall and

was informed (b)(6),(b)(7)(C) no longer worked there. Instead, he was employed at (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) Tyson's Corner Center Mall, McLean, VA.

8. On November 30, 2007 SAs (b)(6),(b)(7)(C) DCIS Arlington RA, interviewed (b)(6),(b)(7)(C) The interview took place in the (b)(6),(b)(7)(C) in Tyson's Corner Center Mall. During the interview (b)(6),(b)(7)(C) gave SAs (b)(6),(b)(7)(C) consent to search his personally owned computer for forensic analysis. (b)(6),(b)(7)(C) guided SAs (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) to his residence at (b)(6),(b)(7)(C)

Once at his residence, (b)(6),(b)(7)(C) informed SAs (b)(6),(b)(7)(C) he paid \$50 to access the child pornography website Desired Angles. (b)(6),(b)(7)(C) informed the nude children on the website were definitely underage. After (b)(6),(b)(7)(C) visited the website once and viewed the child pornography, he decided it was not what he expected and did not access it again. (b)(6),(b)(7)(C) did not download the child pornography. Furthermore, (b)(6),(b)(7)(C) stated his computer might contain images of underage girls wearing clothes.

9. On April 30, 2008, SA Thomas provided one compact disc (CD) containing images SA (b)(6),(b)(7)(C) found on (b)(6),(b)(7)(C) computer to Inspector (b)(6),(b)(7)(C) United States Postal Inspection Service, National Center for Missing and Exploited Children (NCMEC), 699 Prince Street, Alexandria, VA. SA (b)(6),(b)(7)(C) requested Inspector (b)(6),(b)(7)(C) examine the CD for known child victims.

10. On June 18, 2008, (b)(6),(b)(7)(C) Child Victim Identification Program, NCMEC, analyzed (b)(6),(b)(7)(C) computer and identified several files that appeared to contain images of child victims law enforcement previously identified.

11. On July 23, 2008, SA (b)(6),(b)(7)(C) DCIS Arlington RA, reviewed the images NCMEC identified and concluded all images were found in "free space." On October 20, 2008, SA Carson completed a final media analysis that concluded all images were carved from "free space."

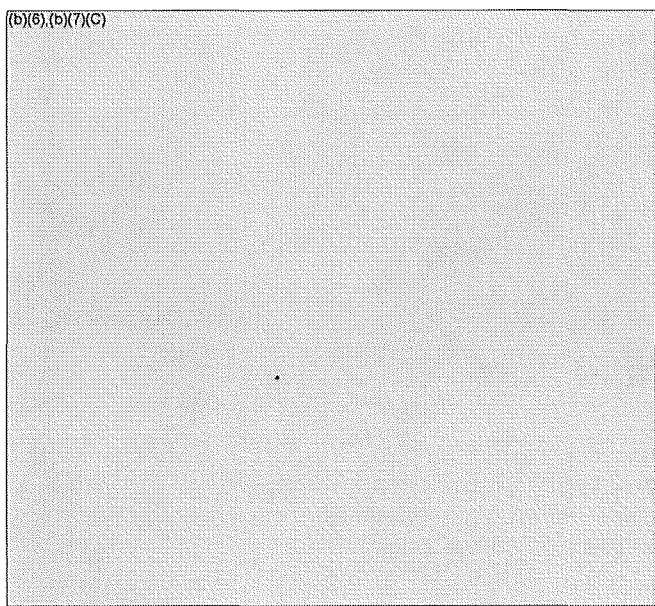
12. On June 28, 2008, SA (b)(6),(b)(7)(C) analyzed (b)(6),(b)(7)(C) Internet search logs and visited each website. Although many websites advertised teen and child models, no websites advertised child pornography.

13. On July 28, 2008, AUSA Smagala declined prosecution on the matter. AUSA Smagala advised he did not intend to prosecute (b)(6),(b)(7)(C) because the images NCMEC identified were in "free space." AUSA Smagala explained items in "free space" do not constitute possession.

14. No judicial or administrative action will occur. No fraud vulnerabilities were identified during this investigation. DCIS will take no further action on this matter. The investigation is closed as "declined."

**IDENTITY OF SUBJECTS:**

Name :  
 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-1

Prepared by Special Agent (b)(6),(b)(7)(C) Arlington Resident Agency APPR: (b)(6),(b)(7)(C)

CLASSIFICATION:

**~~FOR OFFICIAL USE ONLY~~**  
**~~LAW ENFORCEMENT SENSITIVE~~**

**WARNING**

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without specific prior authorization of the Deputy Inspector General for Investigations.~~



(Investigations)

**DEPARTMENT OF DEFENSE  
OFFICE OF INSPECTOR GENERAL  
DEFENSE CRIMINAL INVESTIGATIVE SERVICE  
ARLINGTON RESIDENT AGENCY  
201 12<sup>th</sup> STREET SOUTH, SUITE 712  
ARLINGTON, VIRGINIA 22202-5408**

**REPORT OF INVESTIGATION**

**200901015K-03-MAR-2009-60DC-W1/R**

**December, 09 2009**

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

**DISTRIBUTION:**

**DCIS Headquarters, National Security Program (03NS)**

**B-1**

**CLASSIFICATION:**

**~~FOR OFFICIAL USE ONLY~~  
~~LAW ENFORCEMENT SENSITIVE~~**

**WARNING**

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without specific prior authorization of the Deputy Inspector General for Investigations.~~

**NARRATIVE:**

1. On October 8, 2008, (b)(6),(b)(7)(C) a National Reconnaissance Office (NRO), contract employee with (b)(6),(b)(7)(C) was interviewed by the Personnel Security Division (PSD), NRO, regarding the renewal of his security clearance. During this interview (b)(6),(b)(7)(C) admitted to being addicted to pornography and that he viewed child pornography about twice a week from his home computer. (b)(6),(b)(7)(C) stated he finds child pornography on the internet by using an internet search engine to search for terms such as “underage” or “underage model.” (b)(6),(b)(7)(C) further stated he has joined pay for view web sites depicting children in nude or nearly nude photos and videos.

2. Investigator (INV) (b)(6),(b)(7)(C) NRO, Office of the Inspector General (OIG), reported that the NRO PSD was prompted to address this specific topic of trafficking in child pornography with (b)(6),(b)(7)(C) based upon an allegation made in September 2006 by his then girlfriend, (b)(6),(b)(7)(C) who was also a contract NRO employee, and was residing with (b)(6),(b)(7)(C) at the time, reported she had discovered evidence on his computer that he was in possession of child pornography. (b)(6),(b)(7)(C) confronted (b)(6),(b)(7)(C) and he confessed to knowingly possessing the child pornography. (b)(6),(b)(7)(C) had reported this matter to the Personnel Security Division; however, the decision was made internally to only address the issue at (b)(6),(b)(7)(C) next personnel security update. NRO OIG had only received this information after (b)(6),(b)(7)(C) confession during his PSD interview. INV (b)(6),(b)(7)(C) further received copies of credit card statements from (b)(6),(b)(7)(C) indicating that (b)(6),(b)(7)(C) was possibly using his credit cards to pay for pornographic internet memberships. Legal processes were issued in order to establish probable cause for a search of (b)(6),(b)(7)(C) residence and computer.

3. On June 9, 2009, SA (b)(6),(b)(7)(C) coordinated with Assistant U.S. Attorney Jerry Smagala, U.S. Attorney’s Office, Eastern District of Virginia, Alexandria, VA, who stated no records were available concerning the aforementioned credit cards statements.

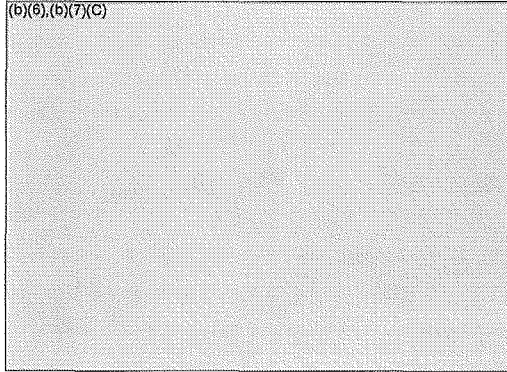
4. On July 22, 2009, SA (b)(6),(b)(7)(C) was contacted by INV (b)(6),(b)(7)(C) who reported (b)(6),(b)(7)(C) had permanently relocated to a NRO facility in New Mexico and was currently residing at (b)(6),(b)(7)(C)

5. As (b)(6),(b)(7)(C) currently worked and resided in New Mexico, the Arlington Resident Agency referred this matter to the DCIS South West Field Office (SWFO). The matter was briefed by Acting Computer Crimes Coordinator (b)(6),(b)(7)(C) to Resident Agent in Charge (b)(6),(b)(7)(C) on August 11, 2009. The matter was referred to the SWFO under Information Report 200902497C-10-SEP-2009-60DC-W1/R.

**IDENTITY OF SUBJECTS**

**IDENTIFYING DATA**

**Name** :  
**Alias** :  
**Social Security Number** :  
**Date/Place of Birth** :  
**Race** :  
**Sex** :  
**Residence** :  
  
**Employment/Occupation** :







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

(Investigations)

REPORT OF INVESTIGATION

200801774O-16-JUL-2008-30TL-Z1/F

April 9, 2009

LEDFORD, KRIS ALLEN

DISTRIBUTION:

B-1

CLASSIFICATION:

~~FOR OFFICIAL USE ONLY~~

WARNING

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without the specific prior authorization of the Deputy Inspector General for Investigations.~~

200801774O-16-JUL-2008-30TL-Z1/F

April 9, 2009

Bureau of Alcohol, Tobacco and Firearms (ATF) – Muskogee, OK

B-2

CLASSIFICATION:

~~FOR OFFICIAL USE ONLY~~

WARNING

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without the specific prior authorization of the Deputy Inspector General for Investigations.~~

2008017740-16-JUL-2008-30TL-Z1/F

April 9, 2009

NARRATIVE

1. On July 10, 2008, the Defense Criminal Investigative Service (DCIS), Tulsa Resident Agency, received a formal request from Assistant United States Attorney (AUSA) (b)(6),(b)(7)(C) Chief, Criminal Division, Eastern District of Oklahoma, to assist in the Federal investigation of Kris A. Ledford. It was alleged that Ledford, a Muskogee police officer, stole firearms from the Muskogee police evidence room, impersonated a Tulsa police officer and stole a police issued bullet proof vest from a co-worker. AUSA Horn requested the DCIS assist in helping determine Ledford's military service record. Ledford's counsel had proclaimed in the local media that Ledford served in the U.S. military as a sniper and was awarded the Purple Heart and Bronze Star along with other commendations and that Ledford suffers from Post Traumatic Stress Disorder (PTSD).

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

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

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

5. On September 2, 2008, the RA obtained a copy Ledford's military personnel file from National Personnel Records Center.

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

**WARNING**

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without the specific prior authorization of the Deputy Inspector General for Investigations.~~

2008017740-16-JUL-2008-30TL-Z1/F

April 9, 2009

6. On September 16, 2008 the reporting agent interviewed (b)(6),(b)(7)(C) who was the former (b)(6),(b)(7)(C) 1<sup>st</sup> Battalion, 36<sup>th</sup> Infantry Regiment. (b)(6),(b)(7)(C) stated he was the (b)(6),(b)(7)(C) 1<sup>st</sup> Battalion, 36<sup>th</sup> Infantry Regiment, during which time Ledford was assigned to the unit. (b)(6),(b)(7)(C) stated he remembered deploying to Bosnia with Ledford being assigned to this unit. (b)(6),(b)(7)(C) stated Ledford did not receive a Bronze Star or Purple Heart for action during the deployment. (b)(6),(b)(7)(C) stated he specifically recalls Ledford due to (b)(6),(b)(7)(C)

7. On October 1, 2008, the RA obtained records from the U.S. Department of Veteran Affairs concerning Kris A. Ledford. (b)(6),(b)(7)(C)

8. On November 12, 2008, Kris Ledford was charged by way of a criminal Information for violating Title 18 United States Code § 922(j) Possession of Stolen Firearm and Title 18 United States Code § 704 Stolen Valor. The information charges that on or about June 4, 2007 to on or about May 29, 2008, Ledford knowingly possessed, concealed, stored, bartered, sold and disposed of nine stolen firearms. The Information also charges that on or about July 23, 2008, Ledford falsely represented himself, verbally and in writing, to have been awarded the Purple Heart and the Bronze Star.

9. On November 19, 2008, Kris Ledford pled guilty in U.S. District Court for the Eastern District of Oklahoma to a one count violation of Title 18 United States Code § 922(j) Possession of Stolen Firearm and to a one count violation of Title 18 United States Code § 704 Stolen Valor.

10. On March 31, 2008, Kris Ledford was sentenced in U.S. District Court for the Eastern District of Oklahoma to 48 months imprisonment and ordered to pay a special assessment of \$100 for one count violation of Title 18 United States Code § 922(j) Possession of Stolen Firearm and sentenced to 12 months imprisonment and ordered to pay a special assessment of \$25 for one count violation of Title 18 United States Code § 704 Stolen Valor.

11. All adjudication has been completed and no further action is anticipated. This investigation is complete and will be closed. There were no fraud vulnerabilities identified during the course of this investigation.

B-4

CLASSIFICATION:

**FOR OFFICIAL USE ONLY****WARNING**

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without the specific prior authorization of the Deputy Inspector General for Investigations.~~

200801774O-16-JUL-2008-30TL-Z1/F

April 9, 2009

IDENTITY OF SUBJECTS

IDENTIFYING DATA:

Name : Kris Allen Ledford  
 Alias : None  
 Social Security Number : (b)(6),(b)(7)(C)  
 Date/Place of Birth :  
 Race :  
 Sex :  
 Residence :  
 Employment/Occupation : Police Officer  
 Muskogee Police Department  
 Telephone Number : (b)(6),(b)(7)(C)  
 Education :

Prepared by: SA (b)(6),(b)(7)(C) Tulsa Resident Agency

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

B-5

CLASSIFICATION:

~~FOR OFFICIAL USE ONLY~~

**WARNING**

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without the specific prior authorization of the Deputy Inspector General for Investigations.~~



(Investigations)

INSPECTOR GENERAL  
DEPARTMENT OF DEFENSE  
DEFENSE CRIMINAL INVESTIGATIVE SERVICE  
BALTIMORE RESIDENT AGENCY  
US APPRAISERS STORES BUILDING, SUITE 208  
103 SOUTH GAY STREET  
BALTIMORE, MD 21202

REPORT OF INVESTIGATION

200800031G-03-OCT-2007-60BT-W1/F

October 21, 2008

DEMOULIN, STANLEY P.  
Odenton, MD

DISTRIBUTION

DCIS Headquarters (03SO)

NSA-OIG (SA<sup>(b)(6),(b)(7)(C)</sup> [REDACTED])

ICE-Baltimore (SA<sup>(b)(6),(b)(7)(C)</sup> [REDACTED])

CLASSIFICATION:

~~FOR OFFICIAL USE ONLY~~

WARNING

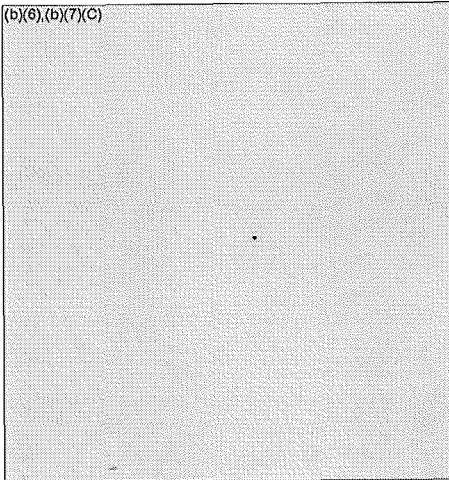
~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without the specific prior authorization of the Deputy Inspector General for Investigations.~~

NARRATIVE

1. This investigation was initiated based upon based on information derived from a DCIS Project, Operation Flicker, Case Control Number 200701199X. As background, on May 29, 2007, DCIS initiated Operation Flicker based on information provided by Assistant United States Attorney (AUSA) Gerald Smagala, United States Attorney's Office, Eastern District of Virginia, Alexandria Division. AUSA Smagala advised that Immigration and Customs Enforcement (ICE) was conducting a national investigation that identified over 5,000 individuals who subscribed to predicated child pornography websites. AUSA Smagala specifically requested that DCIS assist in identifying DoD affiliated individuals and provide investigative assistance. The reporting agent utilized information contained within the DoD Employee Interactive Data System and the Joint Personnel Adjudication Systems (JPAS) to identify DoD affiliated individuals. Among those identified was Stanley P. Demoulin, a (b)(6),(b)(7)(C) DoD contractor employee at the National Security Agency. A query of JPAS revealed that Demoulin (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) Under Operation Flicker, Demoulin made approximately four purchases of alleged pornographic material depicting children. Exhibit 1 is a copy of the DCIS Form 1, "Case Initiation", dated October 3, 2007.
2. On October 17, 2007, a search warrant was executed on DeMoulin's residence in Odenton, MD. Numerous computer-related and other items were seized from the residence. Exhibit 2 is a copy of the DCIS Form 1, "Significant Incident Report/Search Warrant", dated October 22, 2007.
3. Analysis of DeMoulin's computer files indicated evidence of child pornography. After negotiations with DeMoulin and his attorney, on April 15, 2008, DeMoulin agreed to plead guilty to a Criminal Information charging him with Receipt of Child Pornography, Title 18 USC §2252A(a)(2)(A) & Title 18 USC §2256. Exhibit 3 is a copy of the DCIS Form 1, "Plea Agreement", dated May 29, 2008, and Exhibit 4 is a copy of the DCIS Form 1, "Criminal Information", dated May 29, 2008.
4. On July 11, 2008, DeMoulin pleaded guilty in U.S. District Court, Baltimore, MD, to violating one count of Receipt of Child Pornography, Title 18 USC §2252A(a)(2)(A) & Title 18 USC §2256. On August 28, 2008, DeMoulin was sentenced to 63 months in prison, a \$100 assessment, sentenced to lifetime probation, and ordered to register as a sexual offender upon release from prison. Exhibit 5 is a copy of the DCIS Form 1, "Guilty Plea", dated July 11, 2008, and Exhibit 6 is a copy of the DCIS Form 1, "Sentencing", dated August 28, 2008.
5. No fraud vulnerability reports were completed during the course of this investigation. All investigative effort is now complete. This investigation is closed as "finished" with the submission of this report.

IDENTITY OF SUBJECTS

IDENTIFYING DATA

Name	:	Stanley P. DeMoulin
Alias	:	
Social Security Number	:	
Date/Place of Birth	:	
Race	:	
Sex	:	
Height	:	
Weight	:	
Hair	:	
Eyes	:	
Residence	:	
Employment/Occupation	:	
Telephone Number	:	Home: UNKNOWN Office: UNKNOWN [If appropriate] Cell: UNKNOWN
Driver's License Number and Issuing State	:	UNKNOWN
Education	:	UNKNOWN



EXHIBITS

- 1 - DCIS Form 1, "Case Initiation", dated October 3, 2007.
- 2 - DCIS Form 1, "Significant Incident Report/Search Warrant", dated October 22, 2007.
- 3 - DCIS Form 1, "Plea Agreement", dated May 29, 2008.
- 4 - DCIS Form 1, "Criminal Information", dated May 29, 2008.
- 5 - DCIS Form 1, "Guilty Plea", dated July 11, 2008.
- 6 - DCIS Form 1, "Sentencing", dated August 28, 2008.

Prepared by: SA (b)(6),(b)(7)(C) Baltimore Resident Agency

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

C-1

CLASSIFICATION:

~~FOR OFFICIAL USE ONLY~~

**WARNING**

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without the specific prior authorization of the Deputy Inspector General for Investigations.~~



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

(Investigations)

200901117N-18-MAR-2009-30TL-W1/D

January 7, 2010

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

**CASE TERMINATION - CLOSED:** This investigation was initiated pursuant to a formal request from the U.S. Immigration and Custom Enforcement (ICE) to assist in the Federal investigation of (b)(6),(b)(7)(C). It was alleged that (b)(6),(b)(7)(C) a civilian employee with the U.S. Army at Fort Sill, OK, downloaded child pornography. On December 29, 2008, ICE Cyber Crimes Center received notification from Bundeskriminalamt (BKA), the German Federal Criminal Office, concerning the distribution of child pornography via the file sharing system known as Gnutella.

Specifically, the BKA advised that on December 17, 2008, their Computer Crime Unit conducted a search/analysis for child pornography in the Gnutella file-sharing network. Analysis of the logged data streams reflected a file containing child pornography had been received from different sources/suspects. One of the suspects was identified as using the IP address (b)(6),(b)(7)(C) which belongs to AT&T Internet Services. ICE requested the subscriber information from AT&T Internet Services for the user logged in to that IP address on the noted specific date and time. AT&T informed ICE that the user account logged on to IP address (b)(6),(b)(7)(C) on the above listed date and time was subscribed to by (b)(6),(b)(7)(C) with a service address of (b)(6),(b)(7)(C).

An on-line search for (b)(6),(b)(7)(C) in state of Oklahoma conducted by ICE revealed an e-mail address of (b)(6),(b)(7)(C). ICE then contacted the Defense Criminal Investigative Service (DCIS) for assistance in helping determine the further identify of (b)(6),(b)(7)(C). The DCIS Tulsa Resident Agency conducted a Department of Defense Employee Interactive Data System query, which determined (b)(6),(b)(7)(C) to be a GS-7 Army Civilian working for the U.S. Army Medical Command with a home address of (b)(6),(b)(7)(C). This was the same address documented in the AT&T service address. An on-line query of "amedd" listed in the e-mail address provided by ICE revealed it was an abbreviation for Army Medical Department. A Reenlistment Eligibility Data Display query revealed (b)(6),(b)(7)(C).

C-1

CLASSIFICATION:

WARNING

**FOR OFFICIAL USE ONLY**

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without the specific prior authorization of the Deputy Inspector General for Investigations.~~

200901117N-18-MAR-2009-30TL-W1/D

January 7, 2010

On April 23, 2009, ICE and DCIS Criminal Investigative Service executed a search warrant at (b)(6),(b)(7)(C) the personal residence of (b)(6),(b)(7)(C). One computer was seized during the execution of the search warrant. During the forensic examination of the computer, approximately five thumbnail images were discovered from the Thumbs.db file of the media player. These images appeared to be the initial frame of deleted video files, which depicted the sexual abuse of minor children.

On July 13, 2009, ICE Special Agents' (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) both interviewed (b)(6),(b)(7)(C) who waived his rights and provided the following information. (b)(6),(b)(7)(C) was shown the thumbnail images of videos that had been deleted from his computer and was asked if he downloaded the videos. (b)(6),(b)(7)(C) stated that he did and that he used Limewire to download them. (b)(6),(b)(7)(C) did not remember watching them nor did he remember the exact search terms he would have used to find them. (b)(6),(b)(7)(C) was also shown a portion of the video which was downloaded by the BKA. (b)(6),(b)(7)(C) stated that he has seen pictures of the minor female, but he did not recall ever seeing a video of her or downloading one. (b)(6),(b)(7)(C) stated that he usually would download videos and then immediately delete them.

On July 14, 2009, Assistant U.S. Attorney (AUSA) (b)(6),(b)(7)(C) was briefed on the investigative findings and AUSA (b)(6),(b)(7)(C) declined prosecution. Subsequently, the reporting agent provided all investigative findings to Special Agent in Charge (b)(6),(b)(7)(C) of the Fort Lawton U.S. Army Criminal Investigation Command office, who briefed (b)(6),(b)(7)(C) unit commander on the investigative findings.

The final report of investigation prepared by ICE is attached. This investigation is being closed as no further investigative activity is anticipated. There were no fraud vulnerability reports identified during the course of this investigation.

## Attachment:

1. ICE Report of Investigation # OC07QR09OC0006 dated July 14, 2009.

Prepared by: SA (b)(6),(b)(7)(C) Tulsa Resident Agency  
 DISTR: ICE – SA (b)(6),(b)(7)(C)

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

CLASSIFICATION:

~~FOR OFFICIAL USE ONLY~~

## WARNING

This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without the specific prior authorization of the Deputy Inspector General for Investigations.



**INSPECTOR GENERAL  
DEPARTMENT OF DEFENSE  
DEFENSE CRIMINAL INVESTIGATIVE SERVICE  
Mid-Atlantic Field Office – Arlington Resident Agency  
201 12<sup>th</sup> Street South, Suite 712  
Arlington, Virginia 22202-5408**

**REPORT OF INVESTIGATION**

200301205U-11-JUL-2003-60DC-W1/D

February 4, 2005

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

**SPECIAL INTEREST CASE**

**DISTRIBUTION:**

DCIS Headquarters, National Security Program (03NS)

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

CLASSIFICATION:

**OFFICIAL USE ONLY**

**WARNING**

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without the specific authorization of the Deputy Inspector General for Investigations.~~

NARRATIVE:

1. This investigation was initiated based upon information received from (b)(6),(b)(7)(C) Security and Intelligence Directorate, Defense Advanced Research Projects Agency (DARPA), Arlington, VA, concerning possible possession of child pornography by (b)(6),(b)(7)(C) Program Manager, DARPA, Arlington, VA.
2. (b)(6),(b)(7)(C) indicated that on June 23, 2003, during a routine check of (b)(6),(b)(7)(C) work computer for a virus, (b)(6),(b)(7)(C) a contractor from DARPA's Information Technology Division, Arlington, VA, discovered what appeared to be child pornography.
3. On June 24, 2003, (b)(6),(b)(7)(C) who is the (b)(6),(b)(7)(C) was interviewed by Special Agent (SA) (b)(6),(b)(7)(C) Defense Criminal Investigative Service (DCIS), Mid-Atlantic Field Office (MAFO), and advised that on June 23, 2003, he was approached by (b)(6),(b)(7)(C) a network engineer, who stated that he had found a large amount of pornography on (b)(6),(b)(7)(C) computer during the process of reviewing the file system for a virus that had been reported by the network virus scanning software. (b)(6),(b)(7)(C) called (b)(6),(b)(7)(C) immediate supervisor, (b)(6),(b)(7)(C), who came over to examine the images. While (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) were showing the images to (b)(6),(b)(7)(C), they discovered images that appeared to be child pornography. (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) then directed (b)(6),(b)(7)(C) to copy the portions of the file system from (b)(6),(b)(7)(C) hard drive that contained the pornography. (b)(6),(b)(7)(C) provided DCIS with a series of CD-ROMs containing the pornography copied from (b)(6),(b)(7)(C) computer.
4. On July 15, 2003, SA (b)(6),(b)(7)(C) DCIS-MAFO, began an analysis of the images provided by DARPA. Images that contained potential child pornography were identified and provided to the National Center for Missing and Exploited Children (NCMEC) to determine whether the individuals contained in the images could be identified as known victims. Routinely, in order to criminally prosecute child pornography cases through the Federal system, individuals in the images must be identified as known victims.
5. On October 31, 2003, the NCMEC reported that no known victims were found in the images provided for their review.
6. On November 3, 2003, Assistant United States Attorney (AUSA) (b)(6),(b)(7)(C) U.S. Attorney's Office, Eastern District of Virginia, Alexandria, VA, declined to criminally prosecute this matter given that there were no images of known victims.

CLASSIFICATION:

**OFFICIAL USE ONLY****WARNING**

This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without the specific authorization of the Deputy Inspector General for Investigations.

February 4, 2005

7. On December 15, 2003, (b)(6),(b)(7)(C) Criminal Investigator, Computer Crime Unit, Office of the Attorney General, Commonwealth of Virginia, Richmond, VA, was contacted and provided with a copy of the DCIS-MAFO media analysis report. (b)(6),(b)(7)(C) stated that under Virginia statutes (b)(6),(b)(7)(C) could be prosecuted by the Commonwealth under § 18.2-374.1:1, Possession of Child Pornography; which would be a class 5 felony. Virginia statute does not require that the individuals in the images be identified as known victims. (b)(6),(b)(7)(C) stated his office would open an investigation and contact a Commonwealth's Attorney to prosecute this matter.

8. On February 27, 2004, (b)(6),(b)(7)(C) was interviewed by SA (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) confessed to downloading pornography both from his residential and his office computers; however, he denied specifically targeting any child pornography for download (see Exhibit 1). (b)(6),(b)(7)(C) provided a written statement concerning his activity (see Exhibit 2). (b)(6),(b)(7)(C) gave consent for the search of his residential computers and his office notebook.

9. On April 7, 2004, the media received from (b)(6),(b)(7)(C) were provided to the Defense Computer Forensics Lab (DCFL) for analysis.

10. On September 22, 2004, the DCFL completed their analysis of the material received from (b)(6),(b)(7)(C). A review of the report revealed a large amount of pornographic material that might meet the definition of child pornography. A copy of the DCFL report was provided to (b)(6),(b)(7)(C).

11. This Report of Investigation is being provided to DARPA for information purposes and action as deemed appropriate. Should administrative action be taken, it is requested that SA (b)(6),(b)(7)(C) be notified. SA (b)(6),(b)(7)(C) can be contacted at (b)(2) or at the electronic mail address of (b)(6) @dodig.osd.mil.

12. Possible images of child pornography and other pornographic images obtained during the course of this investigation cannot be appended to this report due to their graphic nature and, in regards to the possible images of child pornography, their classification as contraband. Should additional information about the images be needed, please contact SA (b)(6),(b)(7)(C).

13. Based on information obtained to date, the DCIS-MAFO will continue to work with the Commonwealth of Virginia in seeking possible criminal prosecution of (b)(6),(b)(7)(C).

A-2

IDENTITY OF SUBJECTS:

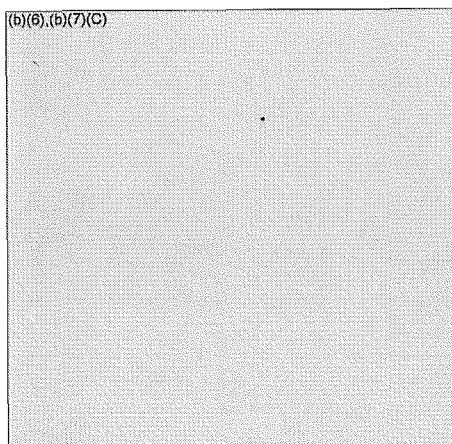
CLASSIFICATION:

**OFFICIAL USE ONLY****WARNING**

This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without the specific authorization of the Deputy Inspector General for Investigations.

IDENTIFYING DATA

Name :  
Social Security Number :  
Date/Place of Birth :  
Race :  
Sex :  
Height :  
Weight :  
Hair :  
Eyes :  
Residence :  
  
Employment/Occupation :



Defense Advanced Research Projects Agency  
Arlington, VA

B-1

EXHIBITS:

CLASSIFICATION:

~~OFFICIAL USE ONLY~~

**WARNING**

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without the specific authorization of the Deputy Inspector General for Investigations.~~

1. DCIS Form 1 - Interview of (b)(6),(b)(7)(C)
2. (b)(6),(b)(7)(C) Written Statement

Prepared by SA (b)(6),(b)(7)(C) Mid-Atlantic Field Office

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

C-1

CLASSIFICATION:

~~OFFICIAL USE ONLY~~

**WARNING**

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without the specific authorization of the Deputy Inspector General for Investigations.~~





(Investigations)

DEPARTMENT OF DEFENSE  
OFFICE OF INSPECTOR GENERAL  
DEFENSE CRIMINAL INVESTIGATIVE SERVICE  
ARLINGTON RESIDENT AGENCY  
201 12<sup>th</sup> STREET SOUTH, SUITE 712  
ARLINGTON, VIRGINIA 22202-5408

REPORT OF INVESTIGATION

200201147Z-22-MAY-2002-60DC-W1/D

March 17, 2009

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

DISTRIBUTION:

DCIS Headquarters, National Security Program (03NS)  
Pentagon Force Protection Agency (b)(6), (b)(7)(C)

CLASSIFICATION:

~~FOR OFFICIAL USE ONLY~~  
~~LAW ENFORCEMENT SENSITIVE~~

**WARNING**

This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without specific prior authorization of the Deputy Inspector General for Investigations.

March 17, 2009

**NARRATIVE:**

1. This case was initiated based on a referral from the Defense Protective Service (DPS), now Pentagon Force Protection Service (PFPA), on May 16, 2002. SA (b)(6),(b)(7)(C) DPS advised SA (b)(6),(b)(7)(C) Arlington Resident Agency (RA), that (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) Management Support Division, Navy Annex, Washington, DC, used his assigned government computer to access pornographic websites and download material that appeared to be child pornography.

2. As background, on May 15, 2002, SA (b)(6),(b)(7)(C) interviewed (b)(6),(b)(7)(C) Network Security Administrator, Dyncorp Incorporated (Dyncorp). As part of computer virus protection efforts, Dyncorp was under contract to the Information Technology Division (ITD), Real Estate and Facilities Directorate (REFD), Washington Headquarters Services, to track computer viruses. According to (b)(6),(b)(7)(C) on May 10, 2002, he performed a McAfee virus scan of the network of the REFD at the Pentagon and Navy Annex. The software created an "E-Policy" report of the top ten computers affected by viruses. (b)(6),(b)(7)(C) computer was number one with 218 viruses detected.

3. (b)(6),(b)(7)(C) created a "SQUID User Access Report" which captured every instance of (b)(6),(b)(7)(C) internet access. (b)(6),(b)(7)(C) provided the E-Policy report and the Squid report to Alex Benton, Network Security Manger, Dyncorp.

4. On May 15, 2002, SA (b)(6),(b)(7)(C) interviewed (b)(6),(b)(7)(C). According to (b)(6),(b)(7)(C) she used the SQUID User Access Report to review websites (b)(6),(b)(7)(C) visited to identify potential sources of the viruses. (b)(6),(b)(7)(C) accessed several of the sites listed in the SQUID report and noticed nude images of women and what she believed to be prepubescent girls. (b)(6),(b)(7)(C) informed supervisors (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C). The matter was presented to (b)(6),(b)(7)(C) REFD, ITD, and (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) REFD. Collectively, a decision was made to disable (b)(6),(b)(7)(C) account to make it impossible for him to logon to the network.

5. On May 15, 2002, (b)(6),(b)(7)(C) to covertly secure (b)(6),(b)(7)(C) government computer (CPU), disabled (b)(6),(b)(7)(C) account so he couldn't logon to the network. Once the helpdesk received (b)(6),(b)(7)(C) call for assistance, his CPU was retrieved and replaced with another under the ruse of a technical difficulty or CPU problem. ITD transferred the CPU to DPS to create a forensic image of the hard drive and maintain as evidence. On May 20, 2002, DPS transferred the CPU to the Arlington RA for analysis.

6. On June 7, 2002, SA (b)(6),(b)(7)(C) DCIS Arlington RA, High Technology Crimes Team (HTCT), conducted an interim forensic media analysis of the retrieved CPU and reviewed (b)(6),(b)(7)(C) SQUID report. SA (b)(6),(b)(7)(C) recovered 75 images and internet artifacts (index.dat files) from the CPU. Analysis of the recovered internet artifacts verified (b)(6),(b)(7)(C) visited prohibited sites such as [www.crazy-lola.com](http://www.crazy-lola.com), [www.cyber-lolita.com](http://www.cyber-lolita.com), [www.x-lolitas.com](http://www.x-lolitas.com), and [www.topless-lolita.com](http://www.topless-lolita.com).

A-1

CLASSIFICATION:

**WARNING**

This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without specific prior authorization of the Deputy Inspector General for Investigations.

~~FOR OFFICIAL USE ONLY~~  
LAW ENFORCEMENT SENSITIVE

March 17, 2009

7. Assistant United States Attorney (AUSA), (b)(6),(b)(7)(C) Eastern District of Virginia, accepted the case for prosecution. On June 25, 2002, the Arlington RA executed search warrants at the following locations belonging to (b)(6),(b)(7)(C) work area, home and network directories, network email archive, and his personal America OnLine (AOL) account. The Arlington RA also conducted a consent search of his residence at (b)(6),(b)(7)(C) (b)(6),(b)(7)(C)

8. Contemporaneous to the search, (b)(6),(b)(7)(C) provided a sworn statement acknowledging his misuse of the government computer. (b)(6),(b)(7)(C) stated he did not knowingly search and download child pornography. (b)(6),(b)(7)(C) explained while intentionally viewing and downloading adult pornography, he was redirected to websites containing child pornography.

9. On September 23, 2002, the Directorate for Personnel and Security, Labor and Management Employee Relations Division, Washington Headquarters Services, DoD, issued a memorandum of final decision to remove (b)(6),(b)(7)(C) from employment with the Department of Defense (DoD). The agreement detailed a five year employment separation from DoD, which at its conclusion was to be expunged from (b)(6),(b)(7)(C) Official Personnel File and related databases. The removal was effective September 24, 2002.

10. SA (b)(6),(b)(7)(C) Arlington RA, and SA (b)(6),(b)(7)(C) DCIS, Baltimore RA, who was assigned to the FBI's Mid-Atlantic Child Exploitation Task Force (MACET), sent images recovered from (b)(6),(b)(7)(C) CPU to three different agencies in an attempt to identify known victims. On October 7, 2002, the FBI reported no known victims were identified. On April 23, 2003, the National Center for Missing Exploited Children's Child Recognition and Identification System (CRIS) reported no known victims were identified. On June 24, 2003, the Cyber Crime Smuggling Center, U.S. Customs Service, DHS, reported no known victims were identified.

11. In August 2003, due to the federal requirements regarding child pornography prosecutions, the case was presented to the Office of the Attorney General, Commonwealth of Virginia. The Arlington RA presented the recovered images for review to SA (b)(6),(b)(7)(C) Office of the Attorney General's Computer Crime Unit, Richmond, Virginia. The Arlington RA did not receive a response for a substantial amount of time. While waiting for a response from SA (b)(6),(b)(7)(C) SA (b)(6),(b)(7)(C) proceeded to verify (b)(6),(b)(7)(C) employment status, whereabouts, and close the case.

12. In the spring of 2005, SA (b)(6),(b)(7)(C) contacted SA (b)(6),(b)(7)(C) and informed him that (b)(6),(b)(7)(C) (b)(6),(b)(7)(C), Computer Crime Unit, Commonwealth of Virginia, accepted the case for prosecution. SA (b)(6),(b)(7)(C) imaged and reviewed the electronic media that was seized at the subject's residence, work area, and network directories. SA (b)(6),(b)(7)(C) copied recovered images and movies to a compact disk then submitted the compact disk to NCMEC on April 22, 2005, for review. NCMEC, which had expanded its CRIS database of known victims since 2003, identified six "series" of known child victims. Additionally, (b)(6),(b)(7)(C) NCMEC analyst, identified one image that contained an unknown child.

A-2

CLASSIFICATION:

**FOR OFFICIAL USE ONLY**  
**LAW ENFORCEMENT SENSITIVE**

**WARNING**

This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without specific prior authorization of the Deputy Inspector General for Investigations.



INSPECTOR GENERAL  
 DEPARTMENT OF DEFENSE  
 DEFENSE CRIMINAL INVESTIGATIVE SERVICE  
 MINNEAPOLIS POST OF DUTY  
 414 GALTIER PLAZA, 380 JACKSON ST, STE 4  
 ST PAUL, MN 55101-2901

(Investigations)

REPORT OF INVESTIGATION

200500963R-18-APR-2005-40MN-W1/F

December 7, 2009

RONALD RICHARD SHANKEY, SSN: (b)(6),(b)(7)(C)  
 DPOB: (b)(6),(b)(7)(C)  
 (b)(6),(b)(7)(C)

ROBERT A MACCINI, SSN: (b)(6),(b)(7)(C)  
 DPOB: (b)(6),(b)(7)(C)  
 (b)(6),(b)(7)(C)

STEPHEN H. MCCONNAUGHAY, SSN: (b)(6),(b)(7)(C)  
 DPOB: (b)(6),(b)(7)(C)  
 (b)(6),(b)(7)(C)

RONALD E. ELMQUIST, SSN: (b)(6),(b)(7)(C)  
 DOB: (b)(6),(b)(7)(C)  
 (b)(6),(b)(7)(C)

DISTRIBUTION

DCISHQ (03NS)  
 Central Field Office (40FO)

WARNING

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without the specific prior authorization of the Deputy Inspector General for Investigations.~~

NARRATIVE

1. This investigation was initiated based upon a request from SA (b)(6),(b)(7)(C) Federal Bureau of Investigation (FBI), EauClaire, WI, relative to allegations of distribution of child pornography against Ronald Shankey. Computer logins by (b)(6),(b)(7)(C) in January and February 2004, were confirmed by ACS Government Solutions and the U. S. Army that the communications were from UserID (b)(6),(b)(7)(C). That UserID was assigned to Ronald Shankey. Logins originated from phone numbers (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C). Shankey was the First Sergeant for the Minneapolis Recruiting Company, Minneapolis Recruiting Battalion, U.S. Army Recruiting Command (USAREC) for about one year prior to his retirement on August 31, 2004. Shankey was then hired as a civilian contractor for MPRI, a subsidiary of DOD Top 100 Contractor L-3 Communications, providing personal services under contract with the USAREC, Ft. Knox, KY. He acted in the capacity of a military enlistment counselor since the middle of February 2005. Numerous images of child pornography were posted to (b)(6),(b)(7)(C) by someone using the e-mail address (b)(6),(b)(7)(C). Using Yahoo ID information, hotmail e-mail address, and IP number (b)(6),(b)(7)(C) associated with the postings, the login was made via a dial in connection from (b)(6),(b)(7)(C). This phone number is the residence number belonging to (b)(6),(b)(7)(C) at (b)(6),(b)(7)(C). The e-mail address was registered by (b)(6),(b)(7)(C) WI zip code 54016, from (b)(6),(b)(7)(C) on 01/09/2002 with a birth year of 1965. This case was worked jointly with the FBI at EauClaire, WI and the St. Croix Sheriff's Office.

2. Shankey was interviewed on May 17, 2005 and while initially denying knowledge of or involvement with child pornography, Shankey later became emotional and requested a lawyer before discussing details of his activities. A search warrant was executed at Shankey's residence also on May 17, 2005 and two computers were among the items seized. Shankey's work computer was provided by the U.S. Army Recruiting Command and is being analyzed. Logs of Shankey's computer activity were obtained from the Recruiting Command. Shankey resigned his position as a civilian contractor without returning to work. Pornographic images obtained from Shankey's computers were submitted to the National Center for Missing and Exploited Children (NCMEC) for comparison with previously identified victims of child pornography with negative results. (b)(6),(b)(7)(C) were interviewed by St. Croix County (b)(6),(b)(7)(C)

3. The FBI – EauClaire developed information that child pornography was being stored at the Shankey residence. A search warrant was obtained and executed on September 7, 2006 which yielded numerous items of child pornography. On October 4, 2006, a grand jury for the Western District of Wisconsin, Madison, Wisconsin returned a two-count indictment with distributing a visual depiction of minors engaging in sexually explicit conduct, and possessing a computer hard drive containing such visual depictions.

4. On May 15, 2007, District Judge John C. Shabaz, for the Western District of Wisconsin, Madison, Wisconsin sentenced Shankey on one count of violating Title 18, United States Code Section 2252(a)(4)(B), Possession of Child Pornography; a Class C felony, a second count of distribution of child pornography was dismissed. Shankey was sentenced to a period of imprisonment of 108 months, followed by supervised release for life and to register as a sex offender. Additionally, he was required to pay a \$100 criminal assessment.
5. Maccini was titled as a subject on December 5, 2006 in cooperation with the Massachusetts State Police. Maccini was indicted on December 20, 2006 on child pornography charges, including distribution based upon information provided by the DCIS Minneapolis Post of Duty. Maccini was sentenced on December 12, 2007 to 5 years probation in Massachusetts state court.
6. The Illinois Attorney General's office has requested assistance for an e-mail associate of Shankey's going by the name (b)(6),(b)(7)(C). Information related to distribution of child pornography by this e-mail account was provided. On February 21, 2008, McConnaughay, aka. (b)(6),(b)(7)(C) was charged in Illinois with possession and dissemination of child pornography, class 3 and class 1 felony respectively. On May 29, 2009, McConnaughay was sentenced in McHenry County Illinois pursuant to a plea agreement on a Class 3 felony charge of possession of child pornography. He is to serve 4 months incarceration, 2 years probation, pay a \$1,00 fine and register as a sex offender.
7. The FBI, Kansas City requested assistance with another associate of Shankey's using the screen name (b)(6),(b)(7)(C). Information was retrieved from Shankey's computer showing 13 messages between Shankey and (b)(6),(b)(7)(C). This information was provided to assist in their prosecution. AUSA Roseann Ketchmark, Western District of Missouri advised that on July 10, 2009, Ronald Elmquist (b)(6),(b)(7)(C) pled guilty to attempted possession of child pornography in violation of Title 18, United States Code Section 2252 (A)(4)(B) and (B)(2). On October 30, 2009, Elmquist was sentenced to 30 months incarceration, 5 yrs supervised release, 120 hours of community service, 12 months of home detention, participate in sex offender counseling, register under the Sex Offender registration and Notification Act, a \$150,000 fine, and \$100 special assessment.
8. All known subjects associated with this case have been sentenced. This case is therefore being closed as completed. Any evidence will be disposed of in accordance with DCIS policy.

200500963R-18-APR-2005-40MN-W1/F

December 7, 2009

**EXHIBITS – Previously submitted.**

Prepared by: SA (b)(6), (b)(7)(C) Minneapolis Post of Duty

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



(Investigations)

DEPARTMENT OF DEFENSE  
OFFICE OF INSPECTOR GENERAL  
DEFENSE CRIMINAL INVESTIGATIVE SERVICE  
ARLINGTON RESIDENT AGENCY  
201 12<sup>th</sup> STREET SOUTH, SUITE 712  
ARLINGTON, VIRGINIA 22202-5408

REPORT OF INVESTIGATION

200701301F-20-JUN-2007-60DC-W1/F

April 9, 2009

SWEENEY, DANIEL JOSEPH

DISTRIBUTION:

Defense Criminal Investigative Service Headquarters, National Security Program (03NS)  
Immigration and Customs Enforcement, SAC Washington, D.C. (SA (b)(6),(b)(7)(C))

CLASSIFICATION:

~~FOR OFFICIAL USE ONLY~~  
~~LAW ENFORCEMENT SENSITIVE~~

**WARNING**

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without specific prior authorization of the Deputy Inspector General for Investigations.~~



**NARRATIVE:**

1. On May 29, 2007, the DCIS, Arlington Resident Agency, initiated Project: Operation Flicker (CCN: 200701199X) based on information provided by Assistant U.S. Attorney (AUSA) Gerald Smagala, U.S. Attorney's Office (USAO), Eastern District of Virginia (EDVA), Alexandria Division. AUSA Smagala advised that the ICE was conducting a national investigation that identified over 5,000 individuals who subscribed to predicated child pornography websites. AUSA Smagala specifically requested DCIS assistance relative to any identified DoD personnel.

2. SA (b)(6),(b)(7)(C) utilized information contained within the DoD Employee Interactive Data System and the Joint Personnel Adjudication Systems (JPAS) to identify DoD affiliated individuals. Among those identified was Daniel Joseph Sweeney, an Active Duty, Petty Officer Second Class (E-5), with the U.S. Navv. (b)(6),(b)(7)(C)  
(b)(6),(b)(7)(C)

3. AUSA Smagala advised that Sweeney (b)(6),(b)(7)(C)  
(b)(6),(b)(7)(C) As background, Paypal is an account based system that lets anyone with an email address securely send and receive online payments using their credit card or bank account.

4. Information derived from Operation Flicker revealed that Sweeney (b)(6),(b)(7)(C)  
(b)(6),(b)(7)(C)

5. On June 21, 2007, a search warrant was executed on Sweeney's residence located at (b)(6),(b)(7)(C)  
(b)(6),(b)(7)(C)

6. During a non-custodial interview of Sweeney, he stated that he was active duty U.S. Navy, E-6 and worked at the Navy Yard in Washington, D.C. (b)(6),(b)(7)(C)  
(b)(6),(b)(7)(C)

7. Sweeney stated that he was aware that downloading and possessing child pornography was a violation of law. He admitted to accessing child pornography while stationed on the U.S.S. Mason. He said a few guys on the ship saw him doing it and warned him to stop.

8. During the search warrant, agents seized two laptop computers, one external hard disk drive, one thumb drive, two memory cards, and approximately 77 other media items from the

**WARNING**

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without specific prior authorization of the Deputy Inspector General for Investigations.~~

residence. Computer forensics revealed child pornography on one of the laptop computers belonging to Sweeney.

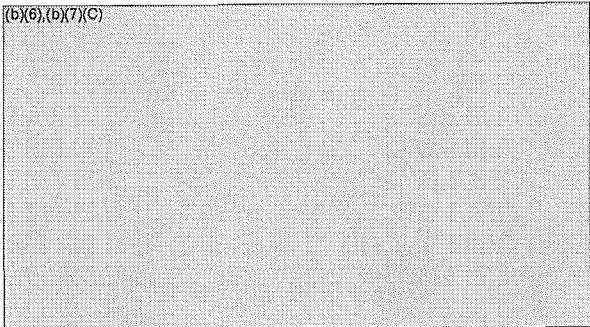
(b)(6),(b)(7)(C)

9. The recovered images were submitted to the National Center for Missing and Exploited Children (NCMEC) in Alexandria, Virginia. The NCMEC reported that images recovered from Sweeney's residence included children previously identified by law enforcement as victims of sexual abuse.
10. On October 7, 2008, a warrant was issued for the arrest of Sweeney by the U.S. District Court (USDC), EDVA. On October 8, 2008, agents executed an arrest warrant on Sweeney in Norfolk, Virginia, where he was station aboard the U.S.S. Anzio.
11. On October 23, 2008, Sweeney was indicted in the Eastern District of Virginia on two counts of attempted receipt of child pornography and possession of child pornography, a violation of Title 18, U.S. Code (USC), Sections 2252A(a)(2) and 2252A(a)(5)(B).
13. On December 12, 2008, Sweeney appeared before the Honorable James C. Cacheris, District Judge, USDC, EDVA, Alexandria Division. Sweeney pled guilty to a single count of possession of child pornography, a violation of Title 18, USC, Section 2252A.
14. On March 13, 2009, Sweeney was sentenced to 41 months incarceration, 240 months supervised release, and a \$100 penalty, for the possession of child pornography, a violation of Title 18, USC, Section 2252A
15. No further criminal, civil or administrative activity by the DCIS will occur. This case is closed as "finished."

**WARNING**

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without specific prior authorization of the Deputy Inspector General for Investigations.~~

**IDENTITY OF SUBJECTS:**

Name	:	Sweeney, Daniel Joseph
Alias	:	None
Social Security Number	:	
Date/Place of Birth	:	
Race	:	
Sex	:	
Height	:	
Weight	:	
Hair	:	
Eyes	:	
Residence	:	
Employment/Occupation	:	
Telephone Number	:	Unknown
Driver's License Number and Issuing State	:	Unknown
Education	:	Unknown

Prepared by Special Agent  Arlington Resident Agency APPR: 

B-1

CLASSIFICATION:

**~~FOR OFFICIAL USE ONLY~~**  
**~~LAW ENFORCEMENT SENSITIVE~~**

**WARNING**

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without specific prior authorization of the Deputy Inspector General for Investigations.~~



(Investigations)

DEPARTMENT OF DEFENSE  
INSPECTOR GENERAL  
DEFENSE CRIMINAL INVESTIGATIVE SERVICE  
ARLINGTON RESIDENT AGENCY  
201 12<sup>TH</sup> STREET SOUTH, SUITE 712  
ARLINGTON, VIRGINIA 22202-5408

REPORT OF INVESTIGATION

200701341T-26-JUN-2007-60DC-W1/F

November 23, 2009

CAMPBELL, CAMERON MORRISON

**DISTRIBUTION:**

DCIS Headquarters, National Security Program (03NS)

CLASSIFICATION:

~~FOR OFFICIAL USE ONLY~~  
~~LAW ENFORCEMENT SENSITIVE~~

**WARNING**

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without specific prior authorization of the Deputy Inspector General for Investigations.~~

**NARRATIVE:**

1. This case was initiated based on information derived from Defense Criminal Investigative Service (DCIS) Project: Operation Flicker (Case Control Number 200701199X).

2. As background, on May 29, 2007, the DCIS Arlington Resident Agency, initiated Project: Operation Flicker based on information provided by Assistant U.S. Attorney (AUSA) Gerald Smagala, U.S. Attorney's Office, Eastern District of Virginia, Alexandria Division. AUSA Smagala advised that the Immigration and Customs Enforcement was conducting a national investigation that identified over 5,000 individuals who subscribed to predicated child pornography websites. AUSA Smagala specifically requested DCIS assist in identifying DoD affiliated individuals and provide investigative assistance.

3. Cameron Morrison Campbell was identified as (b)(6),(b)(7)(C)  
(b)(6),(b)(7)(C)

4. On June 28, 2007, agents executed a search warrant on Campbell's residence located at (b)(6). Subsequent to the execution of the search warrant, agents conducted a non-custodial interview of Campbell. (b)(6),(b)(7)(C)  
(b)(6),(b)(7)(C)

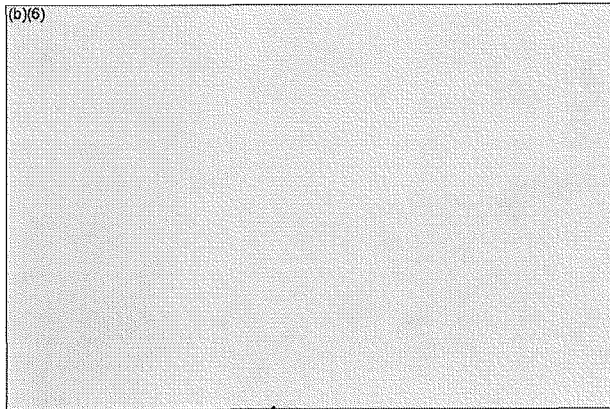
5. On August 6, 2009, a criminal information was filed against Campbell for receipt of child pornography, a violation of Title 18, U.S. Code, Section 2252A(a)(2).

6. On August 26, 2009, Campbell pled guilty to receipt of child pornography, a violation of Title 18, U.S. code, Section 2252A(a)(2).

7. On November 20, 2009, Campbell appeared before the Honorable Gerald Bruce Lee, District Judge, U.S. District Court, Eastern District of Virginia, Alexandria, Virginia and was sentenced to 60 months in prison, 60 months supervised released, and a \$100 penalty assessment.

**IDENTIFY OF SUBJECTS:**

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



**WARNING**



(Investigations)

DEPARTMENT OF DEFENSE  
OFFICE OF INSPECTOR GENERAL  
DEFENSE CRIMINAL INVESTIGATIVE SERVICE  
ARLINGTON RESIDENT AGENCY  
201 12<sup>th</sup> STREET SOUTH, SUITE 712  
ARLINGTON, VIRGINIA 22202-5408

REPORT OF INVESTIGATION

200701463Q-17-JUL-2007-60DC-W1/F

August 26, 2008

JONES, PAUL BURNELL

DISTRIBUTION:

DCIS Headquarters, National Security Program (03NS)

Immigration and Customs Enforcement, SAC Washington, D.C. (SA (b)(6), (b)(7)(C))

CLASSIFICATION:

~~FOR OFFICIAL USE ONLY~~  
~~LAW ENFORCEMENT SENSITIVE~~

**WARNING**

This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without the specific prior authorization of the Deputy Inspector General for Investigations.

NARRATIVE

1. This investigation was initiated based on information derived from DCIS Project: Operation Flicker (Case Control Number 200701199X). Flicker was initiated based upon a national ICE investigation which identified over 5,000 individuals who subscribed to predicated child pornography websites. DCIS was requested to assist in the identification and investigation of DoD affiliated individuals.
2. SA (b)(6),(b)(7)(C), DCIS, utilized information contained within the DoD Employee Interactive Data System and the Joint Personnel Adjudication Systems (JPAS) to identify DoD employees who subscribed to the websites. Among those identified was Paul Burnell Jones, a Contract Specialist with the (b)(6),(b)(7)(C).
3. Based on information obtained from ICE regarding Jones' subscriptions to known child pornography sites, agents from DCIS and ICE executed a search warrant on Jones' residence on July 25, 2007. Jones' residence was located at (b)(6),(b)(7)(C). In addition a warrant was executed at Jones' office located at (b)(6),(b)(7)(C).
4. Simultaneous to the executions of the search warrants, SA (b)(6),(b)(7)(C) DCIS, and SA (b)(6),(b)(7)(C) ICE, conducted a non-custodial interview of Jones. Jones admitted to (b)(6),(b)(7)(C) further provided he regularly accessed child pornography from (b)(6),(b)(7)(C) home. After establishing probable cause, Jones was arrested.
5. On July 25, 2007, a search warrant was executed on the home of Jones' (b)(6),(b)(7)(C).
6. On October 11, 2007, Jones pled guilty to one count of Attempted Receipt of Child Pornography, a violation of Title 18 U.S.C 2252A(b)(1).
7. On January 11, 2008, Jones was sentenced to 60 months in prison and 120 months supervised release. Jones was also fined \$2,000 in restitution and a \$100 special assessment fee.
8. No fraud vulnerabilities were discovered during the course of this investigation. No further criminal, civil or administrative actions will be taken on this matter. The case is closed as "finished."

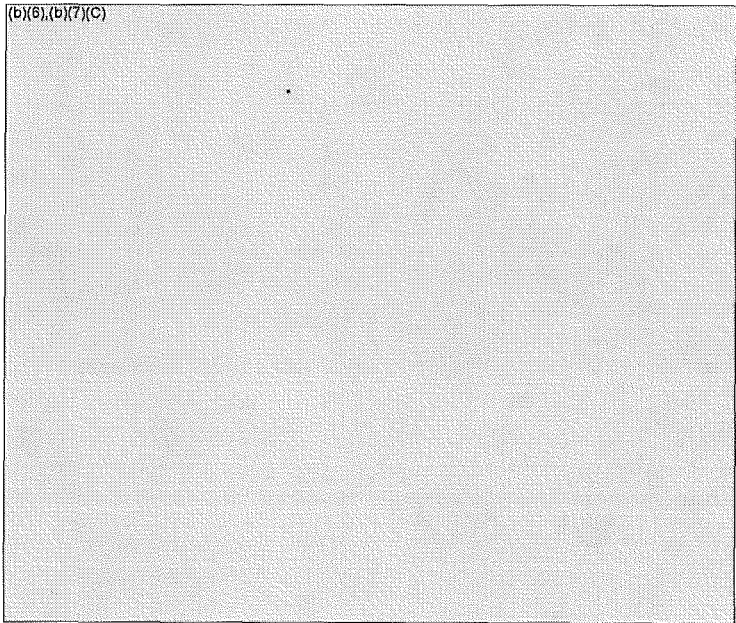


IDENTITY OF SUBJECTS

IDENTIFYING DATA

Name :  
 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 :

Paul Burnell Jones  
 (b)(6),(b)(7)(C)



B-1

Prepared by: SA (b)(6),(b)(7)(C) Arlington Resident Agency

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

CLASSIFICATION:

**FOR OFFICIAL USE ONLY**  
**LAW ENFORCEMENT SENSITIVE**

**WARNING**

This document is the property of the Department of Defense Inspector General and is loaned to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without the specific prior authorization of the Deputy Inspector General for Investigations.



(Investigations)

DEPARTMENT OF DEFENSE  
OFFICE OF INSPECTOR GENERAL  
DEFENSE CRIMINAL INVESTIGATIVE SERVICE  
ARLINGTON RESIDENT AGENCY  
201 12<sup>th</sup> STREET SOUTH, SUITE 712  
ARLINGTON, VIRGINIA 22202-5408

REPORT OF INVESTIGATION

200701403I-09-JUL-2007-60DC-W1/D

April 29, 2009

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

DISTRIBUTION:

DCIS Headquarters, National Security Program (03NS)  
Immigration and Customs Enforcement, SAC Washington, D.C. (b)(6),(b)(7)(C)

CLASSIFICATION:

**FOR OFFICIAL USE ONLY**  
**LAW ENFORCEMENT SENSITIVE**

**WARNING**

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without specific prior authorization of the Deputy Inspector General for Investigations.~~

**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, on May 29, 2007, the DCIS, Mid-Atlantic Field Office (MAFO), initiated Operation Flicker based on information provided by Assistant United States Attorney (AUSA) Gerald Smagala, United States Attorney's Office (USAO), Eastern District of Virginia, Alexandria Division. AUSA Smagala advised that the Immigration and Customs Enforcement (ICE) was conducting a national investigation that had identified over 5,000 individuals who subscribed to predicated child pornography websites. AUSA Smagala specifically requested that DCIS assist in identifying Department of Defense (DoD) affiliated individuals and provide investigative assistance.

2. SA <sup>(b)(6),(b)(7)(C)</sup> utilized information contained within the DoD Employee Interactive Data System (DEIDS) and the Joint Personnel Adjudication Systems (JPAS) to identify DoD affiliated individuals. Among those identified was <sup>(b)(6),(b)(7)(C)</sup> a civilian with an unknown DoD agency. A query of JPAS revealed that he was a civilian contract employee within the Office of the Secretary of Defense, and held a top secret clearance. Law enforcement database checks were conducted and no criminal history was located for <sup>(b)(6),(b)(7)(C)</sup>. A check of the Defense Central Index of Investigations (DCII) revealed one record for <sup>(b)(6),(b)(7)(C)</sup>. A query of the Investigative Data System revealed no open or closed investigations of <sup>(b)(6),(b)(7)(C)</sup>.

3. On July 10, 2007, SA <sup>(b)(6)</sup> and SA <sup>(b)(6)</sup> met with <sup>(b)(6)</sup> <sup>(b)(6)</sup> immediate supervisor <sup>(b)(6),(b)(7)(C)</sup> <sup>(b)(6),(b)(7)(C)</sup> to obtain <sup>(b)(6),(b)(7)(C)</sup> work computer. <sup>(b)(6),(b)(7)(C)</sup> advised a subpoena or search warrant was required for him to release the computer and that he would safe guard the computer in the interim.

4. On July 10, 2007, DCIS and ICE executed a search warrant at <sup>(b)(6),(b)(7)(C)</sup> residence. SA <sup>(b)(6),(b)(7)(C)</sup> was the primary Seized Computer Evidence and Recovery Specialist (SCERS) during the execution the search warrant. During the search warrant ICE entered all evidence into their evidence system and transferred all electronic media items to SA <sup>(b)(6),(b)(7)(C)</sup> SA <sup>(b)(6),(b)(7)(C)</sup> used the Forensic Toolkit Imager and created a primary and secondary forensic image copy of all electronic media. The primary image copy was made on a 500 Giga Byte (GB) Western Digital hard drive that had a serial number WCANU2233037. A secondary image copy was made on a 500 GB Western Digital hard drive that had a serial number WCANCU223888. Both primary and secondary image copies were entered into the DCIS evidence custody system (ECS) on July 10, 2007 under evidence log # 0003-08.

5. On November 29, 2007, SA <sup>(b)(6),(b)(7)(C)</sup> served a search warrant via facsimile to the <sup>(b)(6),(b)(7)(C)</sup>. The search warrant was issued from the U.S. District Court, Eastern District of Virginia, Alexandria Division, by the Honorable Barry R. Portez, U.S. Magistrate Judge. The search warrant requested electronic mail

(e-mail) subscriber information and e-mails sent and received from (b)(6),(b)(7)(C) E-mail account.

6. On December 3, 2007, SA (b)(6),(b)(7)(C) received documents and a compact disk (CD) from (b)(6),(b)(7)(C) pursuant to the search warrant that was served on November 29, 2007.

7. On January 3, 2008, AUSA Smagala advised that an affidavit was not necessary to seize the work computer of (b)(6),(b)(7)(C).

8. On February 4, 2008, AUSA Smagala requested that the forensic examination of the home computer (b)(6),(b)(7)(C) be completed by (b)(6),(b)(7)(C)

9. On May 19, 2008, SA (b)(6),(b)(7)(C) contacted (b)(6),(b)(7)(C) and he verified that a search warrant was not needed to obtain (b)(6),(b)(7)(C) work laptop computer.

10. On September 9, 2008, SA (b)(6),(b)(7)(C) met with (b)(6),(b)(7)(C) at (b)(6),(b)(7)(C) and obtained the original hard drive of the work laptop computer that was issued to (b)(6),(b)(7)(C) also provided a (b)(6),(b)(7)(C) forensic report on work laptop computer.

11. On September 15, 2008, SA (b)(6),(b)(7)(C) reviewed the (b)(6),(b)(7)(C) forensic report regarding (b)(6),(b)(7)(C) work laptop and the results indicated there was no evidence of child pornography on (b)(6),(b)(7)(C) work laptop computer.

12. On September 20, 2008, SA (b)(6),(b)(7)(C) contacted SA (b)(6),(b)(7)(C), ICE, and she requested all of (b)(6),(b)(7)(C) electronic media obtained from the (b)(6),(b)(7)(C) residence search warrant, be transferred back to ICE.

13. On September 25, 2008, SA (b)(6),(b)(7)(C) returned all electronic media obtained from the (b)(6),(b)(7)(C) residence search warrant to SA (b)(6),(b)(7)(C) SA (b)(6),(b)(7)(C) then forwarded all electronic media to (b)(6),(b)(7)(C) for forensic analysis.

14. On February 5, 2009, SA (b)(6),(b)(7)(C) was contacted by SA (b)(6),(b)(7)(C) and she disclosed information that the forensic report from (b)(6),(b)(7)(C) revealed that the (b)(6),(b)(7)(C) electronic media contained no evidence of child pornography violations. As a result, AUSA Smagala declined federal prosecution.

15. On March 26, 2009, SA (b)(6),(b)(7)(C) met with (b)(6),(b)(7)(C) and returned (b)(6),(b)(7)(C) confiscated work laptop hard drive back to Lockheed Martin. (b)(6),(b)(7)(C) stated he will update (b)(6),(b)(7)(C) regarding AUSA Smagala's decision not to prosecute

April 29, 2009

16. A review of (b)(6),(b)(7)(C) personal email and the results of the computer forensic reports of (b)(6),(b)(7)(C) personal and work computers did not reveal evidence related to the receipt of child pornography. AUSA Smagala declined to criminally prosecute (b)(6),(b)(7)(C) for violations relating to possession and/or receipt of child pornography, due to insufficient evidence. DCIS will take no further criminal, civil, or administrative actions on this matter. This case is closed as "declined."

CLASSIFICATION:

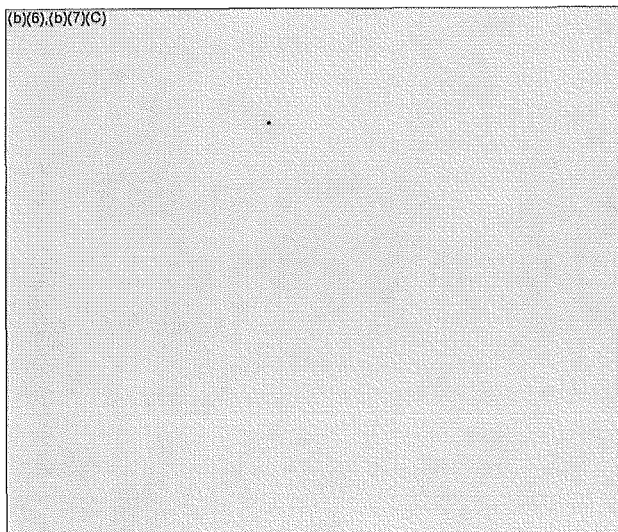
~~FOR OFFICIAL USE ONLY~~  
~~LAW ENFORCEMENT SENSITIVE~~

**WARNING**

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without specific prior authorization of the Deputy Inspector General for Investigations.~~

**IDENTITY OF SUBJECTS:**

Name :  
Alias :  
Social Security Number :  
Date/Place of Birth :  
Race :  
Sex :  
Hair :  
Eyes :  
Residence :  
Employment/Occupation :  
Telephone Number :  
Driver's License Number :  
and Issuing State :  
Education :



April 29, 2009

**EXHIBIT:**

1. U.S. Attorney's Office, Eastern District of Virginia Electronic Forensic Examination Report, dated October 7, 2008.

Prepared by Special Agent (b)(6),(b)(7)(C) Arlington Resident Agency

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

C-1

CLASSIFICATION:

**~~FOR OFFICIAL USE ONLY~~**  
**~~LAW ENFORCEMENT SENSITIVE~~**

**WARNING**

~~This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without specific prior authorization of the Deputy Inspector General for Investigations.~~