Description of document:	**Department of Defense (DoD) Inspector General (IG) final report and closing memo for Defense Criminal Investigative Service (DCIS) Operation Flicker, 2007-2010**
Requested date:	25-May-2010
Released date:	30-August-2010
Posted date:	06-September-2010
Date/date range of documents:	06-June-2007 – 08-April-2010
Source of document:	DoD IG FOIA Requester Service Center Office of Freedom of Information 400 Army Navy Drive, Suite 1021 Arlington, VA 22202-4704 Fax: 703-602-0294

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VA 22202-4704

Ref: 10-00246-F
August 30, 2010

OCCL

This is the final response to your electronic Freedom of Information Act (FOIA) request dated May 25, 2010, seeking *"a copy of the final report and closing memo for DCIS Project Operation Flicker (Case Control Number 200701199X)."* We received your request on May 26, 2010, and assigned it case number 10-00246-F.

The enclosed documents are responsive to your request. I am, however, withholding portions of the records under the provisions of Exemptions 6 and 7(C) of the FOIA, specifically 5 U.S.C. § 552 (b)(6), which pertains to information, the release of which would constitute a clearly unwarranted invasion of personal privacy and 5 U.S.C. § 552(b)(7)(C), which pertains to information compiled for law enforcement purposes, the release of which could reasonably be expected to constitute an unwarranted invasion of the personal privacy of third parties.

If you are not satisfied with this action, you may submit an administrative appeal to Mr. John R. Crane, Assistant Inspector General, Office of Communications and Congressional Liaison, Room 1021, 400 Army Navy Drive, Arlington, VA 22202-4704. Your appeal should be postmarked within 60 days of the date of this letter, should cite case number 10-00246-F, and should be clearly marked "Freedom of Information Act Appeal." There are no fees associated with the processing of this request in this instance.

Sincerely,

Jeanne Miller
Chief, Freedom of Information and
Privacy Office

Enclosures:
As stated

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

(Investigations)

REPORT OF INVESTIGATION

200701199X-29-MAY-2007-60DC-W1/F January 24, 2008

PROJECT: OPERATION FLICKER

DISTRIBUTION:

DCIS Headquarters, National Security Program (03NS)
Immigration and Customs Enforcement, Cyber Crimes Center [redacted])
U.S. Attorney's Office, Eastern District of Virginia, Alexandria Division (AUSA G. Smagala)

b(6)
b(7)(C)

NARRATIVE:

1. In April 2007, [redacted] DCIS, Arlington Resident Agency received information from Assistant U.S. Attorney (AUSA) Gerald Smagala, U.S. Attorney's Office (USAO), Eastern District of Virginia (EDVA). AUSA Smagala provided information concerning a national investigation being conducted by ICE. ICE had identified over 5,000 individuals who subscribed to websites that were known to contain child pornography. ICE designated their operation as PROJECT FLICKER.

2. Several individuals identified under Project Flicker used their DoD/government e-mail address, Fleet Post Office (FPO) military address, or Army Post Office (APO) military address to register for the child pornography websites. AUSA Smagala requested that DCIS assist in the identification of individuals affiliated with the DoD. Initiation of a joint project into this matter was initiated to provide short term assistance to EDVA and ICE. As DoD subjects were identified, information was provided to the DCIS office within the appropriate area of responsibility for action deemed appropriate. Coordination was made throughout the project with the appropriate Military Criminal Investigative Organizations.

3. [redacted] obtained a complete list identifying all U.S. based subjects from the ICE Cyber Crime Center. The list contained the name, e-mail address, telephone number, and postal address of each subject. Queries of subjects were conducted through Autotrack, the Joint Personnel Adjudication System, the Defense Central Index of Investigations, and the DoD Employee Interactive Data System to obtain additional identifying information and establish a DoD nexus. In total, 20 states and D.C. were vetted.

4. As a result of the database queries, 264 individuals affiliated with DoD were identified, including 39 individuals within the Eastern District of Virginia. Of those identified, 9 individuals possessed a Top Secret Sensitive Compartmented Information security clearance, 13 possessed a Top Secret security clearance, 8 possessed a NATO Secret security clearance, 42 possessed a Secret security clearance, and 4 possessed an interim Secret security clearance.

5. The subject information containing DoD query results were divided by location and forwarded to the appropriate ICE and DCIS office for action.

6. To date, 31 spin-off cases have been initiated and 52 subjects have been titled:
   - 200701274Z – [redacted]
   - 200701277C – [redacted]
   - 200701301F – Sweeney, Daniel Joseph
   - 200701340S – [redacted]
   - 200701341T – Campbell, Cameron Morrison
   - 200701402H – Kartes, Thomas Edward
   - 200701403I – [redacted]

b(6)
b(7)(C)

- 200701463Q – Jones, Paul Burnell
- 200701511R – [redacted]
- 200701512S – [redacted]
- 200701516W – [redacted]
- 200701517X – [redacted]
- 200701553H – [redacted]
- 200701558M – Operation Flicker
- 200701567V – Operation Flicker
- 200701571Z – Fitzpatrick, Leland Chace
- 200701596Y – [redacted]
- 200701606N – Operation Flicker
- 200701619A – [redacted]
- 200701620B – Mullen, Shawn B.
- 200701623E – Lindimore, Shane Brewster
- 200701653I – [redacted]
- 200701665U – [redacted]
- 200701667W – Operation Flicker-50ES Targets
- 200701690T – [redacted]
- 200701691U – [redacted]
- 200701692V – [redacted]
- 200701756M – [redacted]
- 200701765V – Project Flicker-SDOH (Western Division)-WDKY-EDKY
- 200800031G – Demoulin, Stanley P.
- 200800080D – Operation Flicker

7. Six Information Reports were completed, to include 200800168S – [redacted]; 200800159J – [redacted]; 200800158I – [redacted]; 200800157H – [redacted]; 200701539T – [redacted] and 200701239Q – [redacted].

8. Two subjects were convicted of violating Title 18, U.S. Code, Section 2252A, Attempted Receipt of Child Pornography (200701402H - Kartes, Thomas and 200701463Q - Jones, Paul). Each subject received 60 months incarceration and 120 months probation. Five subjects are currently pending criminal prosecution in the USAO, EDVA.

9. Due to the short term nature of this project and the need to focus more resources on other DCIS investigative priorities, this project is closed as "finished." All cases generated from this project will be pursued to conclusion.

b(6)
b(7)(C)

(Investigations)

U.S. DEPARTMENT OF DEFENSE
OFFICE OF INSPECTOR GENERAL
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
Mid-Atlantic Field Office – Arlington Resident Agency
201 12th Street South, Suite 712
Arlington, Virginia 22202-5408

200701239Q-07-JUN-2007-60DC-W1/R (IR) June 6, 2007

[redacted] SSN: [redacted]
DPOB: [redacted]; UNK
[redacted]

INFORMATION REPORT/REFERRED: On May 29, 2007, the Defense Criminal Investigative Service (DCIS), Mid-Atlantic Field Office (MAFO), initiated a project based on information provided by Assistant United States Attorney (AUSA) Gerald Smagala, United States Attorney's Office (USAO), Eastern District of Virginia, Alexandria Division (DCIS Case Control Number 200701199X). AUSA Smagala advised that the Immigration and Customs Enforcement (ICE) is conducting a national investigation that has identified over 5,000 individuals who subscribed to predicated child pornography websites.

Among the 5,000 names ICE identified under Operation Flicker, several individuals used their .mil e-mail address, Fleet Post Office (FPO), or Army Post Office (APO) military zip codes. AUSA Smagala requested that the DCIS assist in identifying any additional Department of Defense (DoD) affiliated individuals and provide any investigative assistance. Additional background information on Operation Flicker is included as Attachment 1.

The Reporting Agent (RA) 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 [redacted], Retired Navy Captain (O-6).

[redacted] was flagged as a person of special interest because, according to DEIDS, [redacted] The DEIDS and JPAS results are included as Attachment 2.

The RA spoke with ICE Special Agent (SA) [redacted] in Tampa, Florida and briefed her on DCIS' joint efforts on Operation Flicker. [redacted] welcomed any assistance DCIS can provide. [redacted] can be reached by telephone at [redacted], extension [redacted] or [redacted] cellular.

Given the nature of the allegations, the potential for possibility of harm to the children, and the subject's location in the Tampa area, the MAFO is referring this case to the DCIS, Tampa Bay Resident Agency, for review and any action deemed appropriate.

b(6)
b(7)(C)

The investigative databases contained in National Crime Information Center (NCIC), Defense Clearance and Investigations Index (DCII), Treasury Enforcement Communications System (TECS) were queried for relevant information concerning the subject. No criminal information was found in NCIC or TECS. However, there is a record within DCII. The DCII results are included as Attachment 3.

Attachments:

1. Project Flicker Summary
2. [redacted] DEIDS/JPAS Results
3. [redacted] DCII Results

Prepared by Special Agent [redacted], Mid-Atlantic Field Office APPR: [redacted]
DISTR: 03NS/20FO/20TB/20RL [redacted]/ICE SAC DC [redacted])

b(6)
b(7)(C)

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
TAMPA RESIDENT AGENCY
400 North Tampa Street, Suite 1130
Tampa, Florida 33602-4707

(Investigations)

200701277C-15-JUN-2007-20TB-W1/U

June 5, 2008

[redacted]

DISTRIBUTION:
National Security Program Manager
Southeast Field Office
Mid-Atlantic Field Office
Immigration and Customs Enforcement-Tampa

b(6)
b(7)(C)

NARRATIVE:

1. On June 7, 2007, the Reporting Agent (RA) received an Information Report (IR), Case Control Number (CCN) 200701239Q, from the Defense Criminal Investigative Service (DCIS), Mid-Atlantic Field Office (MAFO). The IR advised that on May 29, 2007, DCIS MAFO initiated a project titled Operation Flicker (CCN 200701199X), based on information provided by Assistant U.S. Attorney (AUSA) Gerald Smagala, Eastern District of Virginia, 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.

2. Among the 5,000 names, ICE identified several individuals who used their .mil email address and/or their Fleet Post Office or Army Post Office military zip code. AUSA Smagala requested that DCIS assist in identifying any additional Department of Defense (DoD) affiliated individuals and provide investigative assistance.

3. The DCIS MAFO utilized information contained within the DoD Employee Interactive Data System (DEIDS) and the Joint Personnel Adjudication Systems, in order to identify DoD affiliated individuals. Among those identified was [redacted] a Retired U.S. Navy Captain (O-6). [redacted]

4. The DCIS MAFO spoke with ICE Special Agent (SA) [redacted] Tampa, FL, and briefed her on the DCIS joint efforts with Operation Flicker. [redacted], who was assigned to exploitation cases, requested investigative assistance from DCIS Tampa.

5. On June 18, 2007, the RA telephonically contacted [redacted] to offer DCIS assistance with the investigation. During the conversation, [redacted] clarified information previously received from the IR and subsequently was included in the case initiation. [redacted] did not use a .mil e-mail address and/or a Fleet Post Office or Army Post Office military zip code while subscribing to predicated child pornography websites. [redacted]

6. On September 19, 2007, the RA conducted a DEIDS check to verify [redacted] was still residing at [redacted] The DEIDS check revealed on August 27, 2007, [redacted] The location of the [redacted] was [redacted] The FPO AP address was assigned to the [redacted] located in Yokohama, Japan.

7. On September 27, 2007, the RA coordinated with [redacted], Naval Criminal Investigative Service (NCIS), Resident Agency, Yokosuka, Japan, to request assistance with the execution of a search warrant on [redacted] residence. [redacted] verified [redacted] was hired [redacted] b(6) b(7)(C)

[redacted] agreed to coordinate with the ICE, Attaché Office and the local Japanese Police Department in order to obtain a search warrant for [redacted] residence.

8. On October 15, 2007, the NCIS executed a search warrant on [redacted] residence located in [redacted] During the execution of the search warrant, [redacted] advised he gave the computer he used to access the Internet to [redacted] A Putty Tower Computer Millennia, serial number 2422181-0001, was seized from [redacted] residence.

9. On November 1, 2007, SAs from ICE Tampa, executed a search warrant on [redacted] A Compaq Presario Computer Tower SR1430NX, Serial Number MXF51408ZV, was seized from [redacted] residence.

10. On January 14, 2008, [redacted] provided the RA a copy of two computer forensic exams. The first forensic exam was performed on [redacted] laptop computer, which was seized during the execution of the search warrant on [redacted] residence located in Japan. The second forensic exam was performed on [redacted] desktop computer which was seized during the execution of the search warrant on [redacted] residence in [redacted] The examination of both computers did not result in the discovery of any child pornographic image files or movie files. However, the examination of the desktop computer indicated that a user of the computer had regularly used one or more privacy applications which wiped most of the history of Internet websites visited and any incriminating files that may have been viewed. Despite using the privacy applications, the examination did find traces that a user had accessed questionable Internet sites that appeared to be child pornographic in nature.

11. Due to the fact that no child pornographic images were found on the computers, this investigation is closed with the submission of this report. There were no fraud vulnerabilities identified during the course of this investigation.

b(6)
b(7)(C)

IDENTITY OF SUBJECT:

IDENTIFYING DATA

Name	:	[redacted]
Alias	:	
Social Security Number	:	
Date/Place of Birth	:	
Race	:	
Sex	:	
Height	:	
Weight	:	
Hair	:	
Eyes	:	
Residence	:	
Employment/Occupation	:	
Telephone Number	:	
Drivers License Number	:	
Education	:	

Prepared by [redacted] APPR: [redacted]

b(6)
b(7)(C)

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

(Investigations)

REPORT OF INVESTIGATION

200701340S-26-JUN-2007-60DC-W1/D

February 27, 2008

[redacted]

DISTRIBUTION:

DCIS Headquarters, National Security Program (03NS)
Immigration and Customs Enforcement, SAC Washington, D.C. ([redacted])
U.S. Army Criminal Investigation Command 902nd Military Intelligence [redacted])

b(6)
b(7)(C)

NARRATIVE:

1. This case was initiated based on information derived from DCIS Project: Operation Flicker (Case Control Number 200701199X). As background, 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.

2. This 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 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.

3. [redacted] 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 [redacted] Lieutenant Colonel (O-5), with the U.S. Army Reserve (USAR). Records revealed [redacted] was on active duty. A query of JPAS revealed he was a [redacted]

4. On June 27, 2007, agents from the DCIS, ICE, and the Fairfax County Police Department (FCPD) executed a search warrant on [redacted]'s residence located at [redacted]

5. Concurrent to the execution of the search warrant [redacted], ICE and [redacted] FCPD, attempted to interview [redacted] regarding his subscription to commercial child pornography websites. However, [redacted] invoked his right to legal counsel and the interview was terminated. [redacted] left his residence during the execution of the search warrant. Media seized from [redacted] residence was sent to the Defense Computer Forensics Laboratory (DCFL) for analysis.

6. DCIS [redacted] and [redacted] traveled to [redacted] office to seek consent to seize [redacted] work computers. Upon arrival at [redacted] office, [redacted] observed [redacted] using a desktop computer, later identified as a Gateway 300L desktop computer, serial number 0026921808. [redacted] observed [redacted] was logged into a Hotmail email account. To prevent [redacted] from destroying evidence, [redacted] instructed [redacted] to step away from the computer. [redacted] stated he wanted to leave and that he was going to see a lawyer. [redacted] allowed [redacted] to shutdown the desktop computer.

7. The DCFL's analysis of [redacted] media did not recover any child pornography images (Exhibit 1). However, the DCFL recovered 25 documents and one movie that was classified

b(6)
b(7)(C)

secret. The classified documents were recovered from compact discs that were seized from [redacted] residence.

8. On September 17, 2007, two additional search warrants were obtained; a warrant for [redacted] work computer and a warrant for [redacted] personal email.

9. A review of [redacted] personal email did not recover any evidence related to the receipt of child pornography. Before the analysis of [redacted] computer could be performed, AUSA [redacted] declined to criminally prosecute [redacted] for violations relating to possession and/or receipt of child pornography, due to insufficient evidence.

10. The matter relating to the mishandling of classified information will be referred to the USACIDC for action(s) deemed necessary. No fraud vulnerabilities were identified. DCIS will take no further criminal, civil, or administrative actions on this matter. No fraud vulnerabilities were identified. This case is closed as "declined."

b(6)
b(7)(C)

IDENTITY OF SUBJECTS:

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

b(6)
b(7)(C)

EXHIBIT:

1. DCFL Digital Forensic Analysis Report

Prepared by Special Agent [redacted], Arlington Resident Agency APPR: [redacted]

b(6)
b(7)(C)

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

(Investigations)

REPORT OF INVESTIGATION

200701402H-09-JUL-2007-60DC-W1/F February 25, 2008

KARTES, THOMAS EDWARD

DISTRIBUTION:

DCIS Headquarters, National Security Program (03NS)
Immigration and Customs Enforcement, SAC Washington, D.C. ([redacted])

b(6)
b(7)(C)

CLASSIFICATION:

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

NARRATIVE:

1. This case was initiated based on information derived from DCIS Project: Operation Flicker (Case Control Number 200701199X). As background, 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.

2. This 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 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.

3. [redacted] utilized information contained within the DoD Employee Interactive Data System (DEIDS) and the Joint Personnel Adjudication Systems (JPAS) to identify DoD employees who subscribed to the websites. Among those identified was Thomas Edward Kartes, Major (O-4), with the U.S. Army Reserve, [redacted] A query of JPAS revealed Kartes was on active duty [redacted]

4. On July 11, 2007, agents from the DCIS, ICE, and the Fairfax County Police Department (FCPD) executed a search warrant on Kartes's residence located at [redacted]

5. Concurrent to the execution of the search warrant, ICE [redacted] and FCPD [redacted] conducted a non-custodial interview of Kartes regarding his subscription to commercial child pornography websites. Kartes admitted to the subscribing to commercial child pornography sites and possessing child pornography images on his computers. Based on his admissions, Kartes was arrested and charged with violation of Title 18, U.S. Code, Section 2252A, attempted receipt of child pornography.

6. On August 29, 2007, Kartes pled guilty to a single count of attempted receipt of child pornography, a violation of Title 18, U.S. Code, Section 2252A.

7. On December 19, 2007, Kartes was sentenced to 60 months incarceration, 120 months supervised release, $3,000 fine and a $100 special assessment, for the attempted receipt of child pornography, a violation of Title 18, U.S. Code, Section 2252A.

8. No fraud vulnerabilities were discovered during the course of this investigation. DCIS will take no further criminal, civil, or administrative actions on this matter. This case is closed as "finished."

b(6)
b(7)(C)

IDENTITY OF SUBJECTS:

Name	:	Kartes, Thomas Edward
Alias	:	None
Social Security Number	:	[redacted]
Date/Place of Birth	:	[redacted]
Race	:	[redacted]
Sex	:	[redacted]
Height	:	[redacted]
Weight	:	[redacted]
Hair	:	[redacted]
Eyes	:	[redacted]
Residence	:	[redacted]
Employment/Occupation	:	Major (O-4), U.S. Army Reserve
Telephone Number	:	[redacted]
Driver's License Number and Issuing State	:	[redacted]
Education	:	[redacted]

Prepared by Special Agent [redacted], Arlington Resident Agency APPR: [redacted]

b(6)
b(7)(C)

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
PITTSBURGH RESIDENT AGENCY
1000 LIBERTY AVE, STE 1310
PITTSBURGH, PA 15222-4004

(Investigations)

REPORT OF INVESTIGATION

200701511R-24-JUL-2007-10PB-Z0/Z

April 8, 2010

DISTRIBUTION:

DCIS HQ – 03SO
Northeast Field Office
DCIS – 10PB
ICE – Pittsburgh

b(6)
b(7)(C)

200701511R-24-JUL-2007-10PB-Z0/Z

NARRATIVE

1. On July 11, 2007, the Reporting Agent received a lead referral from Special Agent [redacted], 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 who have subscribed to predicated child pornography websites. A listing was provided detailing individuals residing in the Western District of Pennsylvania who are employed by the Department of Defense and/or U.S. Military and have subscribed to websites that contain child pornographic images or other material that exploit children via the internet.

2. Among the 5,000 names ICE identified, several individuals used their .mil e-mail address, Fleet Post Office or Army Post Office military zip codes. DoD databases were queried to identify individuals that may be in possession of child pornographic material. One subject identified was [redacted] is currently enlisted in the Marine Corps Reserve as a Corporal (Pay rating/grade E-4, Enlisted). Unit identifying data was not available. Also according to DEIDS and REDD databases, [redacted]

3. RAC [redacted] coordinated with [redacted], Supervisor, ICE Pittsburgh, and [redacted] advised that he would assign an ICE agent to the case and agreed to work jointly with DCIS. Based upon previously established protocols, ICE will be the lead investigative agency for this matter and will prepare the Report of Investigation. Based on the agreement, the Reporting Agent initiated the case on July 24, 2007 (Exhibit 1).

4. On August 9, 2007, Reporting Agent received photo ID and [redacted] driver's license information on [redacted]

5. On January 14, 2008, Reporting Agent requested and later received military personnel files and records of [redacted] Reporting Agent reviewed military personnel files provided on [redacted] but was unable to determine [redacted] global location, let alone [redacted] specific location during the time period when he purchased access to the child pornography websites. Additionally, records did not indicate that a laptop computer and/or cell phone was issued to [redacted].

6. From discussion with Special Agent [redacted], NCIS along with personal experience as a Naval Officer, Reporting Agent is aware that multiple computers and cell phones are accessible by enlisted personnel whether onboard a ship or shore installation. Further discussion with [redacted], former Computer Crimes Coordinator and former RAC, led to the decision to close the case. Case closure was based upon the lack of any concrete evidence and the lack of probable cause that [redacted] may have downloaded photos and to which, if any, computer was utilized for such purpose. Further, the location of such computer and establishing that [redacted] alone used such computer was unlikely to be determined. Finally, due to the fact that this type of case is not a DCIS priority, case

b(6)
b(7)(C)

closure is the best use of current resources and best course of action for the DCIS Pittsburgh RA.

7. Based upon the above, it is recommended that matter be closed.

200701511R-24-JUL-2007-10PB-Z0/Z

IDENTITY OF SUBJECTS

[redacted]

IDENTIFYING DATA

Name: [redacted]
Alias:
Social Security Number:
Date/Place of Birth:
Race:
Sex:
Height:
Weight:
Hair:
Eyes:
Residence:

Employment/Occupation: Marine Corps Reserve
Telephone No:
Drivers License Number/State:
Education:

b(6)
b(7)(C)

200701511R-24-JUL-2007-10PB-Z0/Z

EXHIBITS

1. DCIS Form 1; Case Initiation, July 24, 2007
2. DCIS Letter to HQ USMC, Personnel Management Division, January 14, 2008
3. DCIS Form 1; Receipt of [redacted] Personnel File, January 18, 2008

b(6)
b(7)(C)

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

(Investigations)

REPORT OF INVESTIGATION

200701512S-24-JUL-2007-10SY-W1/F

09-MAY-2008

[redacted]

DISTRIBUTION

Headquarters, Investigative Operations Directorate
Northeast Field Office
Pittsburgh Resident Agency

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 t any party under investigation nor may this document be distributed outside the receiving agency without the specific prior authorization o ~~the~~ Assistant Inspector General for Investigations.

NARRATIVE

1. On July 11, 2007, the reporting agent received a lead referral from Special Agent [redacted], 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. [redacted] 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. On May 17, 2007, [redacted] attended a briefing at ICE, Fairfax, Virginia regarding Operation Flicker. The briefing included the following background information:

3. 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.

4. 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. This criminal organization has utilized a specific and identifiable payment website known as "iWest." The information developed during the course of the investigation has identified that the organization (1) uses various Pay Pal accounts to facilitate the customer payments; (2) uses specific subject identifiers within the Pay Pal accounts to identify purchases into the various member restricted websites; and (3) uses specific administrative e-mail accounts that are used to distribute access to the member restricted websites.

5. 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. [redacted] 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.

b(6)
b(7)(C)

6. [redacted] 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. [redacted] 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 [redacted] is a retired U.S. Army, Army National Guard Staff Sergeant (E-6).

7. The reporting agent queried the Defense Employee Interactive Data Systems (DEIDS), and obtained the following information regarding [redacted], SSN: [redacted], U.S. Army Reserve retiree, Enlisted, Grade:06, No Unit Identifying data, [redacted] Details of the DEIDS report will be attached.

8. The reporting agent also queried the Re-Enlistment Eligibility Data Display (REDD) database for [redacted] and obtained the following information [redacted] SSN [redacted], DOB: [redacted] Army National Guard, Service began [redacted]

9. The reporting agent contacted Special Agent [redacted] ICE Alexandria Bay, NY regarding Operation Flicker. [redacted] 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. [redacted] 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. [redacted] advised that another ICE agent would be assigned to specific investigation, but he would assist in the computer forensics part of the cases.

10. Upon review of the spreadsheet sent by [redacted], the reporting agent determined that [redacted] made four payments utilizing PayPal to the restricted access websites. The payments were for $79.95 each, and occurred on the following dates: November 7, 2006, November 21, 2007 (2 transactions), and December 16, 2006. The "trans.Item Title" was either listed as an invoice number or for "TV-2 collection 30 Days access." (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 dropped 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).

b(6)
b(7)(C)

11. This investigation was anticipated to be conducted jointly with Immigration and Customs Enforcement, Massena, NY. As ICE was determined to be the lead agency, and the fact that there was only a loose affiliation between the subject and the DoD, this investigation was deferred to ICE Massena for any action they deemed appropriate.

12. This investigation is closed.

IDENTITY OF SUBJECTS

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

b(6)
b(7)(C)

EXHIBITS

1 - Excel Spreadsheet titled "Flicker New York" – identifies [redacted] as a subject. .

Prepared by: [redacted], Syracuse Post of Duty APPR: [redacted]

b(6)
b(7)(C)

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
PITTSBURGH RESIDENT AGENCY
1000 LIBERTY AVE, Room 2101
PITTSBURGH, PA 15222-4004

(Investigations)

REPORT OF INVESTIGATION

200701517X-25-JUL-2007-10PB-Z0/Z 18-FEBRUARY-2008

[redacted]

DISTRIBUTION:
DCIS HQ – 03SO
Northeast Field Office
DCIS – 10PB
ICE - Pittsburgh

b(6)
b(7)(C)

TABLE OF CONTENTS

NARRATIVE

1. On July 11, 2007, the Reporting Agent received a lead referral from Special Agent [redacted], 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 who have subscribed to predicated child pornography websites. A listing was provided detailing individuals residing in the Western District of Pennsylvania who are employed by the Department of Defense and/or U.S. Military and have subscribed to websites that contain child pornographic images or other material that exploit children via the internet.

2. Among the 5,000 names ICE identified, several individuals used their .mil e-mail address, Fleet Post Office or Army Post Office military zip codes. DoD databases were queried to identify individuals that may be in possession of child pornographic material. One subject identified was [redacted] is enlisted in the Army Reserve as a Corporal (E-5, Enlisted). [redacted]

3. The Reporting Agent contacted Special Agent [redacted], ICE Pittsburgh, who agreed to jointly work the case, with ICE serving as the lead agency. Based on the agreement, the Reporting Agent initiated the case on July 25, 2007 (Exhibit 1).

4. On September 7, 2007, the Reporting Agent received copies of subpoena returns for subpoena's served on [redacted] email address and Internet service provider from Special Agent [redacted]. Also on that date, Special Agent [redacted] requested that the Reporting Agent obtain [redacted] military personnel file (Exhibit 2).

5. On November 16, 2007, the Reporting Agent obtained [redacted] personnel file and contacted Special Agent [redacted], but received no response. Since then, the Reporting Agent has attempted numerous times to contact Special Agent [redacted] through email and phone calls but he has continued to be non-responsive. In addition, [redacted] Resident Agent in Charge, contacted Special Agent [redacted] ICE Pittsburgh, and advised him of the situation. [redacted] advised he would speak with [redacted], however to date [redacted] has failed to respond.

6. Based upon the complete non-responsiveness of ICE, who has been named the lead agency regarding all Operation Flicker spin off cases, it is recommended that matter be closed.

b(6)
b(7)(C)

IDENTITY OF SUBJECTS:

[redacted]

COMMODITY: [redacted] is enlisted in the Army Reserve as a Corporal (E-5, Enlisted).
[redacted]

b(6)
b(7)(C)

EXHIBITS:

1. DCIS Form 1; Case Initiation, July 25, 2007
2. DCIS Form 1; Receipt of Subpoena Returns, October 3, 2007
3. DCIS Form 1; Receipt of [redacted] Personnel File, November 16, 2007

b(6)
b(7)(C)

Prepared by SA [redacted], Pittsburgh Resident Agency APPR: [redacted]

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

(Investigations)

200701539T-26-JUL-2007-40DY-W1/IR 26-July-2007

[redacted]
D/POB: [redacted] Unknown
[redacted]

INFORMATION REPORT: On July 26, 2007, information was received from the Federal Bureau of Investigation, Dayton, Ohio, concerning a telephonic complaint they received alleging illegal activity (child pornography) by [redacted] a DoD employee. The complaint is summarized below (see attachment for complete details).

[redacted]

On July 26, 2007, a check of the Department of Defense Employee Interactive Data System (DEIDS) disclosed that [redacted]

This information is being furnished to the SEFO/Nashville RA and the Western FO for any action deemed appropriate and to the MAFO (Operation Flicker) for information only. (Note: The complainant does not want to get involved beyond this initial reporting - see attached).

Attachment
1) FBI Complaint Form, July 9, 2006
2) DEIDS Report, 7/26/07
3) Autotrack on [redacted], 7/26/07
4) Autotrack on [redacted] 7/26/07
5) REDDReport, July 26, 2007

Prepared by SA [redacted] Dayton RA APPR: [redacted] b(6) b(7)(C)
DISTR: 20NV/20FO/50FO/60FO [redacted]/FBI, Dayton, OH (w/o attachments)

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
SIOUX FALLS POST OF DUTY
P.O. BOX 139
CASTLEWOOD, SD 57223

(Investigations)

REPORT OF INVESTIGATION

200701553H-31-JUL-2007-40SX-Y0/U 17-MARCH-2008

[redacted]

DISTRIBUTION

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

b(6)
b(7)(C)

NARRATIVE

1. This investigation was initiated based upon information received from the Defense Criminal Investigative Service (DCIS) Project, Operation Flicker. The DCIS Mid-Atlantic Field Office initiated Operation Flicker based on information provided by Assistant United States Attorney Gerald Smagala, United States Attorney's Office, Eastern District of Virginia, Alexandria Division, regarding a national investigation conducted by the United States Immigration and Customs Enforcement (ICE). This investigation has identified over 5,000 individuals who subscribed to predicated child pornography websites. The DCIS Sioux Falls Post of Duty was notified of one of these identified individuals, [redacted] who is a full time Army National Guard member [redacted]

2. A database check through the Defense Manpower Data Center was conducted which revealed tha[redacted] is a Sergeant First Class and works [redacted] with the North Dakota Army National Guard (NDANG). [redacted]

3. According to the ICE Cyber Crimes Center, on December 18, 2006, [redacted] made a purchase through his PayPal account for $79.95 that was processed through a previously identified target PayPal account utilizing the email address [redacted]. This particular transaction follows virtually the exact same pattern as the other transactions that led to child pornography web sites, and was purchased through a PayPal account that appeared to be used almost exclusively for processing payments to these types of sites.

4. A search of the IP address identified during the transaction revealed it belonged to the internet service provider ND Telephone Company located in Devils Lake, ND. A summons to ND Telephone was served by ICE, Grand Forks, ND, on August 7, 2007, which requested subscriber information for the identified IP address for the date and time of the transaction in question. Pursuant to the summons, ND Telephone identified the subscriber as [redacted] residing in [redacted]

5. [redacted] Camp Grafton, NDANG, was contacted and agreed to provide any assistance necessary. [redacted] advised that he has had several problems with [redacted] Joint Forces, NDANG, Bismarck, ND, was also contacted and briefed on the matter.

6. The Reporting Agent (RA) coordinated with [redacted] regarding the internet history file on the government computer used by [redacted] On October 24, 2007, the reporting agent received a memorandum for record from the Joint Force Headquarters, North Dakota Army National Guard (NDARNG), regarding a cursory computer check conducted on the government computer used by [redacted] The review was conducted remotely and consisted of a check of the computer's Internet Explorer internet favorites directory, temporary internet files, internet

b(6)
b(7)(C)

history, and internet cookies. A general review of files and directories was also conducted. Nothing was found outside of the NDARNG's acceptable use policy.

7. On December 5, 2007, the RA and Special Agent [redacted] ICE, Grand Forks, ND, interviewed [redacted] at Camp Grafton Army National Guard Headquarters building, Camp Grafton, ND. [redacted] was cooperative and related that he enjoyed watching young female models progress throughout their career. [redacted] related that occasionally he would come across images that depicted young girls naked but he would immediately delete those images. [redacted] states that he bought memberships to a handful of pay sites and advised that most of those sites dealt with young modeling. He claimed that if he bought into a site that contained anything offensive, he wouldn't return to that site.

8. [redacted] subsequently provided consent to search his home computer. A search of the computer included the internet history file which was commensurate with the kinds of images that [redacted] claimed interest in, including teen and preteen modeling sites. While looking at these files, [redacted] again related that if he visited a web site with inappropriate content, he would leave the site immediately. [redacted] had a shortcut on his desktop to a file containing approximately four subfolders. Two of these sub folders contained images that were very similar in nature to what Grove described would be on his computer. Most depicted young females and appeared to be in either photo shoot type settings or in swimwear. There were some images of naked females in each of the folders, but these females appeared to be over the age of eighteen. SA [redacted] used a "presearch" software program to view all of the image files on [redacted] computer. A couple of images located in the "temporary internet files" area of the computer appeared to be females of questionable age, possibly younger than eighteen. These images and the location of the images on the computer appear to be consistent with [redacted] description of his internet interests and activities.

9. Based on the information developed during the course of this investigation, the DCIS, Sioux Falls Post of Duty and ICE, Grand Forks, ND, consider this investigation closed. All investigative leads have been covered and no further investigative activity is anticipated.

b(6)
b(7)(C)

IDENTITY OF SUBJECTS

IDENTIFYING DATA

Name	:	[redacted]
Alias	:	
Social Security Number	:	
Date of Birth	:	
Race	:	
Sex	:	
Residence	:	
Employment/Occupation	:	
Telephone Number	:	

b(6)
b(7)(C)

EXHIBITS

None. Previously submitted.

Prepared by: [redacted], Sioux Falls Post of Duty APPR: [redacted] b(6) b(7)(C)

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
WESTERN FIELD OFFICE
26722 PLAZA ST, STE 130
MISSION VIEJO, CA 92691-6300

(Investigations)

REPORT OF INVESTIGATION

200701606N-08-AUG-2007-50LA-W1 November 17, 2009

GRANT, GARY DOUGLASS

DISTRIBUTION

DCIS, Headquaters (03NS)
ICE, Santa Ana, CA

b(6)
b(7)(C)

NARRATIVE

1. On July 18, 2007, [redacted], DCIS Arlington Resident Agency, referred identifying information for sixteen persons with ties to the Department of Defense (DoD) who are in the DCIS Mission Viejo Resident Agency (MVRA) area of responsibility (AOR) and are suspected of involvement in child pornography. [redacted] initially received the information from Assistant United States Attorney 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 and all of whom used ".mil" e-mail addresses to register for access to child pornography websites.

2. In April 2006, the Immigration and Customs Enforcement/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 same organization is operating numerous commercial child pornography websites. In addition, the organization utilizes various PayPal accounts to process the payments for access to the member restricted websites. The investigation was worked jointly with ICE/C3/CES, ICE/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 as Project Flicker.

3. ICE/C3/CES conducted over 60 undercover transactions at 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 and identifiable 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 are used to distribute access to the member restricted websites.

4. Project Flicker data was sorted to identify individuals who used their .mil e-mail address, Fleet Post Office, or Army Post Office military zip codes to register for the PayPal service to access the child pornography websites. Gary Grant, Captain, U.S. Army Reserves was one of the individuals identified from this data. Grant is a JAG assigned to the Judge Advocate detachment at the Los Alamitos Army Reserve Base, Los Alamitos, CA.

5. On August 28, 2007, a search warrant was conducted at Grant's residence. The investigation revealed that Grant sent, through the Internet, an image depicting minors engaged in sexually explicit conduct as set forth in California Penal Code Section 311.4(d)(1). Specifically, on October 6, 2006, Grant sent America Online users '[redacted]' and '[redacted]' an email with image "YGP5A9.jpg". Image "YGP5A9.jpg" depicts a nude minor female leaning back in the sand and facing the viewer. The minor female has her left leg bent and is exposing her genitals.

b(6)
b(7)(C)

6. On August 5, 2008, Grant was arrested pursuant to a State of California warrant. The arrest occurred at Grant's residence located at 55 Bluff Cove Drive, Aliso Viejo, CA, 92656. Also participating with DCIS in the arrest were Special Agents from Immigration and Customs Enforcement (ICE) and investigators with the Orange County, CA Sheriff's Department. Grant was arrested for three counts of California Penal Code 311.11(a), possession of obscene matter of a minor in a sexual act (Refer to Exhibit 1).

7. On April 8, 2009, Grant pled guilty in Superior Court of California, County of Orange, to possession of obscene matter of a minor in a sexual act, California Penal Code 311.11(a). Grant was sentenced to 90 days confinement and three years probation (Refer to Exhibit's 2 & 3).

8. In light of the successful prosecution of Grant, this investigation is considered formally closed. The DCIS, Mission Viejo Resident Agency, will devote no further resources to the matter. This case was conducted jointly with the ICE, Santa Ana, CA. The Orange County District Attorney's Office, handled the criminal prosecution.

9. No operational readiness or safety issues were identified during the investigation, and no systemic weaknesses were revealed. Therefore, no Fraud Vulnerability Report will be generated.

IDENTITY OF SUBJECT

IDENTIFYING DATA

NAME	:	Gary Douglass Grant
ALIAS	:	Gary Dougalss Grant; Gary Dougals Grant
DOB	:	August 21, 1957
SSN	:	[redacted]
HEIGHT	:	68"
WEIGHT	:	170 lbs.
HAIR	:	Brown
EYES	:	Blue
ADDRESS	:	[redacted]
PHONE	:	
DRIVERS LICENSE #	:	
STATUS	:	Unknown
OCCUPATION	:	Lawyer

b(6)
b(7)(C)

EXHIBITS

1. DCIS Form 1, "Arrest Report," dated August 5, 2008, with attachments.
2. DCIS Form 1, "Significant Incident-Guilty Plea & Sentencing," dated April 27, 2009, with attachment.
3. DCIS Form 1, "People Vs Grant Minute Order," dated November 11, 2009, with attachment.

Prepared by Special Agent [redacted] Mission Viejo Resident Agency
APPR: [redacted]

b(6)
b(7)(C)

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
KANSAS CITY RESIDENT AGENCY
500 STATE AVE, STE 565
KANSAS CITY, KS 66101-2453

(Investigations)

REPORT OF INVESTIGATION

200701620B-10-AUG-2007-40KC-Y0/F

SEPTEMBER 7, 2009

SHAWN MULLEN
JAMES MATTES

DISTRIBUTION

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

TABLE OF CONTENTS

SYNOPSIS

Immigration and Customs Enforcement (ICE) conducted a national investigation that identified over 5,000 individuals who subscribed to predicated child pornography websites. The Reporting Agent (RA) utilized information contained within the DoD Employee Interactive Data System (DEIDS) and the Joint Personnel Adjudication Systems (JPAS) to identify DoD affiliated individuals. The RA identified 14 possible subjects with a DoD nexus, and with ties to the DCIS Kansas City Resident Agency areas of responsibility. After further interviews and data checks, two individuals were named as subjects in this case, Shawn Mullen (Mullen) and James Mattes (Mattes).

A search warrant was executed at Mullen's residence. Analysis of the computers seized during the warrant identified images of child pornography. Mullen was indicted on one count receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2), and one count possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B) of which he pleaded guilty. Mullen was sentenced to 78 months confinement and 8 years supervised release.

Mattes was interviewed and consented to a search of his personal computer. Analysis of the computer identified images of child pornography. Mattes was indicted on one count receipt of visual depictions involving the use of minors engaging in sexually explicit conduct by means of computer in violation of 18 U.S.C. § 2252(a)(2), and one count possession of material involving sexual exploitation of minors, 18 U.S.C. § 2252(a)(4)(B). Mattes pleaded guilty to Count 1 of the indictment, 18 U.S.C. § 2252(a)(2), receipt. Mattes was sentenced to 65 months confinement, 5 years supervised release and $5,000 in restitution.

The case was successfully prosecuted by the U.S. Attorney's Office, District of Kansas and District of Southern Iowa.

STATUTES

The following violations of the United States Code apply to this investigation:

18 USC § 2252(a)(2)	(Receipt of Child Pornography)
18 USC § 2252(a)(4)(B)	(Possession of Child Pornography)

BACKGROUND

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) conducted 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 Department of Defense (DoD) affiliated individuals and provide investigative assistance.

The Reporting Agent (RA) utilized information contained within the DoD Employee Interactive Data System (DEIDS) and the Joint Personnel Adjudication Systems (JPAS) to identify DoD affiliated individuals. The RA identified 14 possible subjects (listed below) with a DoD nexus, and with ties to the DCIS Kansas City Resident Agency areas of responsibility.

Search warrants and computer analysis were techniques used during the course of this investigation.

NARRATIVE

1. A search warrant was served on the residence of Shawn Mullen, DoD contractor. The computers and digital media seized from Mullen's house were submitted by the RA to the Defense Computer Forensics Laboratory (DCFL) in Linthicum, MD.

2. The RA and ICE SA [redacted] conducted three interviews with [redacted] and [redacted] on September 4, 2007. [redacted] consented to an interview and a review of his laptop. [redacted] admitted to subscribing to the child pornography website. The RA discovered several images of child pornography on his laptop and [redacted] consented to [redacted] seizing the laptop for further forensic review. ICE will continue the investigation involving [redacted] without DCIS because he has since separated from the military and no longer has any DoD affiliation.

The RA and [redacted] interviewed [redacted] who denied purchasing any subscriptions to child pornography websites. [redacted] has since retained an attorney. The RA contacted the Federal Bureau of Investigation Innocent Images to search their database for any information on [redacted], his name and user name yielded no results.

[redacted] consented to an interview and a review of his computer. No images of child pornography were found and the agents will not continue the investigation on [redacted].

3. The RA and [redacted] interviewed James Mattes who admitted to possessing child pornography and consented to a review of his computer. The review showed that the computer

b(6)
b(7)(C)

did have child pornography on the hard drive and Mattes consented to the seizure of the computer. The RA has been conducting a forensic examination of the computer and will submit the results to the National Center for Missing and Exploited Children upon completion to identify known victims. [redacted] is coordinated the case with the U.S. Attorney's Office, Southern District of Iowa, which agreed to prosecute this case. Mattes was added as a subject.

4. The RA and ICE Springfield, MO interviewed [redacted] consented to a review of his computer and no child pornography was found.

5. Mattes was indicted on January 23, 2008 on one count receipt of visual depictions involving the use of minors engaging in sexually explicit conduct by means of computer in violation of 18 U.S.C. § 2252(a)(2), and one count possession of material involving sexual exploitation of minors, 18 U.S.C. § 2252(a)(4)(B).

6. The computer analysis of Mullen's computers was completed by the Defense Computer Forensics Laboratory. Child pornography was identified. On May 21, 2008, Mullen was charged by a federal grand jury as part of a two count indictment in United States District Court, District of Kansas. Mullen was indicted on one count receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2), and one count possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B).

7. Mullen pleaded guilty to both counts of the May 21, 2008 indictment, one count receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2), and one count possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B).

8. On October 3, 2008, Mattes signed a plea agreement. Mattes pleaded guilty to Count 1 of the January 23, 2008 indictment, 18 U.S.C. § 2252(a)(2), receipt. Count 2 of the indictment, 18 U.S.C. § 2252(a)(4)(B), possession, was dismissed at the conclusion of the sentencing hearing.

9. On April 6, 2009, Mullen was sentenced by U.S. District Judge John W. Lungstrum in United States District Court, District of Kansas. Mullen was sentenced to 78 months confinement, 8 years supervised release (to include sex offender registration) and was ordered to pay a $200 assessment fee.

10. On May 15, 2009, Mattes was sentenced by Chief U.S. District Court Judge Robert W. Pratt, in United States District Court, Southern District of Iowa. Mattes was sentenced to 65 months confinement, 5 years supervised release (to include sex offender registration) and was ordered to pay a $100 assessment fee. Mattes was also ordered to forfeit the Dell Dimension Computer 4600, Serial Number 14PKF31 used in the commission of the crime. The victim of the [redacted] filed for $6 million dollars of restitution be paid.

11. On June 22, 2009, Mattes was also ordered to pay restitution in the amount of $5,000 to the Marsh Law Firm, White Plains, New York. The Marsh Law Firm represents the victim from the [redacted] which was among the images identified on Mattes' computer.

b(6)
b(7)(C)

IDENTITY OF SUBJECTS

		IDENTIFYING DATA
Name	:	Shawn Mullen
Alias	:	UNK
Social Security Number	:	[redacted]
Date/Place of Birth	:	4/30/1964, UNK
Race	:	Caucasian
Sex	:	Male/Female
Height	:	6'1"
Weight	:	185 lbs
Hair	:	Brown
Eyes	:	Brown
Residence	:	[redacted]
Employment/Occupation	:	Former database analyst Northrop Grumman
Telephone Number	:	UNK
Home	:	UNK
Driver's License Number and Issuing State	:	UNK
Education	:	UNK

b(6)
b(7)(C)

IDENTITY OF SUBJECTS

		IDENTIFYING DATA
Name	:	James Dean Mattes
Alias	:	UNK
Social Security Number	:	[redacted]
Date/Place of Birth	:	7/11/1970, UNK
Race	:	Caucasian
Sex	:	Male/Female
Height	:	6'2"
Weight	:	200 lbs
Hair	:	Brown
Eyes	:	Brown
Residence	:	[redacted]
Employment/Occupation	:	Former Navy Recruiter E-7
Telephone Number	:	UNK
Home	:	UNK
Driver's License Number and Issuing State	:	UNK
Education	:	UNK

b(6)
b(7)(C)

LAW ENFORCEMENT RECORDS

The files of the Defense Clearance and Investigations Index (DCII) were queried for records of Shawn Mullen and James Mullen. A check did not reveal anything pertinent to this investigation. A National Crime Information Center (NCIC) query of Shawn Mullen and James Mattes revealed no criminal records, either state or Federal.

EVIDENCE

A. Subjects

Shawn Mullen

18 USC § 2252(a)(2) (Receipt of Child Pornography)
18 USC § 2252(a)(4)(B) (Possession of Child Pornography)

James Mattes

18 USC § 2252(a)(2) (Receipt of Child Pornography)
18 USC § 2252(a)(4)(B) (Possession of Child Pornography)

B. Documents

Previously submitted

C. Witnesses

None

STATUS OF INVESTIGATION

This investigation was successfully prosecuted by U.S. Attorney's Office, District of Kansas, Kansas City, KS and Southern District of Iowa, Des Moines, IA.

Shawn Mullen was indicted on one count 18 USC § 2252 (a)(2) and one count 18 USC § 2252(a)(4)(B). He pleaded guilty both counts and was sentenced to 78 months confinement, 8 years supervised release (to include sex offender registration) and was ordered to pay a $200 assessment fee.

James Mattes was indicted on one count 18 USC § 2252 (a)(2) and one count 18 USC § 2252(a)(4)(B). He pleaded guilty to one count of 18 USC § (a)(2) and sentenced to 65 months confinement, 5 years supervised release (to include sex offender registration) and was ordered to pay a $100 assessment fee. Mattes was also ordered to forfeit the Dell Dimension Computer 4600, Serial Number 14PKF31 used in the commission of the crime. The victim of the [redacted] filed for $6 million dollars of restitution to be paid. An amended judgment was filed and ordered Mattes to pay $5,000 in restitution.

PROSECUTIVE CONSIDERATIONS

There are no prosecutive considerations to date.

b(6)
b(7)(C)

EXHIBITS

Previously submitted.

Prepared by: [redacted], Kansas City Resident Agency APPR: [redacted]

b(6)
b(7)(C)

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

(Investigations)

REPORT OF INVESTIGATION

200701623E-10-AUG-2007-60DC-W1/D July 8, 2008

[redacted]

DISTRIBUTION:

DCIS Headquarters, National Security Program (03NS)

b(6)
b(7)(C)

NARRATIVE:

1. This case was initiated based on information derived from the DCIS Project: Operation Flicker (Case Control Number 200701199X). On May 29, 2007, the DCIS Arlington Resident Agency initiated 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 (ICE) was conducting a nationwide investigation that identified over 5,000 individuals that subscribed to predicated child pornography websites. AUSA Smagala requested DCIS assistance in identifying individuals affiliated with the DoD and investigate those individuals with ICE. AUSA Smagala identified [redacted] as one individual with a DoD affiliation that subscribed to predicated child pornography websites.

2. A query of the DoD Employee Interactive Data System indicated [redacted] was in the U.S. Navy Reserves, E-05. A query of the Joint Personnel Adjudication Systems indicated that [redacted]

3. AUSA Smagala informed [redacted] that ICE did not purchase a subscription to the website [redacted] purchased. AUSA Smagala declined criminal prosecution of [redacted] because it could not be proven that the website [redacted] purchased contained child pornography.

4. On January 16, 2008, [redacted] and [redacted], ICE, interviewed [redacted] at his residence. [redacted] denied allegations he purchased a subscription to a child pornography website. [redacted] admitted he purchased subscriptions to several online pornography websites over the past few years. [redacted] stated he encountered child pornography on the Internet on several occasions. On one occasion, after [redacted] began downloading a pornographic video that he believed was adult pornography, [redacted] read reviews of the video that were posted by other people that previously viewed the video. The posts were calling the individual that posted the video on the Internet a pedophile. After seeing the comments posted by people about the video, [redacted] stopped downloading the video because he believed it may have been child pornography. [redacted] also encountered child pornography in the form of "pop ups" on the Internet on several occasions. [redacted] was questioned about a website called "Red Lagoon Mags" and stated he had no knowledge of the website. [redacted] was informed that his credit card was used to purchase a subscription to Red Lagoon Mags for $79.99. [redacted] repeated he had no knowledge of the website and stated he did not remember purchasing a subscription to the website. At the conclusion of the interview, [redacted] requested [redacted] voluntarily turn over computer for forensic review, but [redacted] refused. [redacted] then terminated the interview.

5. On January 30, 2008 [redacted] met with [redacted], regarding [redacted] and status of the DCIS investigation.

b(6)
b(7)(C)

6. On July 7, 2008, [redacted]

7. DCIS will take no further action on this matter. No fraud vulnerabilities were identified during this investigation. The investigation is closed as "declined."

b(6)
b(7)(C)

IDENTITY OF SUBJECTS

Name	:	[redacted]
Social Security Number	:	
Date of Birth	:	
Sex	:	
Residence	:	
Employment/Occupation	:	

Prepared by Special Agent [redacted], Arlington Resident Agency APPR: [redacted]

b(6)
b(7)(C)

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
LONG BEACH RESIDENT AGENCY
501 W. OCEAN BLVD, SUITE 7300
LONG BEACH, CA 90802

(Investigations)

REPORT OF INVESTIGATION

200701667W-17-AUG-2007-50ES-W1/Z

31-JANUARY-2008

[redacted]

DISTRIBUTION

Western Field Office

b(6)
b(7)(C)

NARRATIVE

1. On July 18, 2007 [redacted], DCIS Arlington Resident Agency, referred identifying information for sixteen persons with ties to the Department of Defense (DoD) who are in the DCIS Long Beach Resident Agencies (50ES) Area of Responsibility (AOR) and are suspected of purchasing and supporting the child pornography trade. [redacted] initially received the information from Assistant United States Attorney Gerald Smagala, United States Attorney's Office (USAO), Eastern District of Virginia. The persons identified are active, reserve & retired military members, DoD civilians and DoD contractor employees, several of whom have security clearances.

2. In April 2006, the Immigration and Customs Enforcement/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 same organization is operating numerous commercial child pornography websites. In addition, the organization utilizes various PayPal accounts to process the payments for access to the member restricted websites. The investigation is being worked jointly with ICE/C3/CES, ICE/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 conducted over 60 undercover transactions at the advertising websites associated with this investigation. The investigation determined that a specific criminal organization operates approximately 18 commercial child pornography portal websites which provide access to approximately 18 child pornography member-restricted websites, using a specific and identifiable payment website known as "iWest." The investigation identified that the criminal organization (1) uses various PayPal accounts to facilitate the customer payments; (2) uses specific subject identifiers within the PayPal accounts to identify purchases into the various member restricted websites; and (3) uses specific administrative e-mail accounts that are 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 address, Fleet Post Office, or Army Post Office military zip codes to register for the PayPal service to access the child pornography websites. The four suspects identified in the 50ES AOR have been titled as subjects based upon the initial evidence that was provided to the DCIS by ICE. Based upon the fact that the subjects are DoD employees and possess security clearances, ICE has listed them as a Tier 1 priority. This investigation was coordinated with ICE [redacted], Child Exploitation Unit, Long Beach, CA, [redacted] ICE [redacted] has been assigned as the investigating agent, [redacted]

b(6)
b(7)(C)

5. After a review of [redacted] transactions in December 2007, it was determined that the probable cause for a search warrant was stale and that more recent evidence was not available. In addition to this information, it was also determined that a portion of the original nexus for the initiation of the investigation was incorrect. The information report referred had indicated that the subject had used his/her .mil account to conduct the illegal purchase of child pornography. At the time it was decided that the use of a .mil account in conjunction with the fact that the subject was a contractor to the U.S. military was sufficient nexus to initiate an investigation. However, once it was determined that the use of a .mil account did not occur and that the PC was stale and no further evidence is available, this investigation is closed. There were no management control deficiencies identified during the course of this investigation.

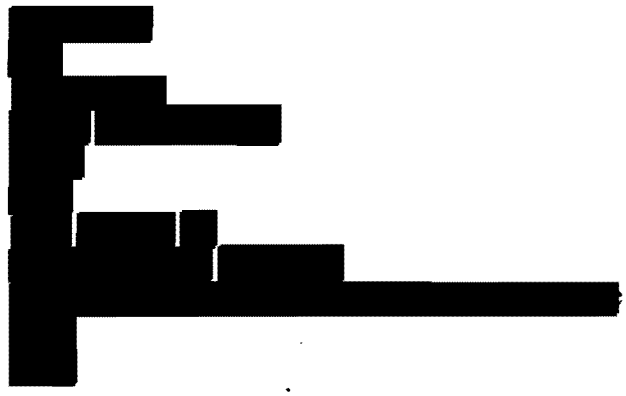
b(6)
b(7)(C)

IDENTITY OF SUBJECTS

Identifying Data:

Name
Alias
Social Security Number
Date/Place of Birth
Race
Sex
Residence

Employment/Occupation
Telephone Number
Education



b(6)
b(7)(C)

EXHIBITS

No Exhibits

Prepared By; SA [redacted], Long Beach Resident Agency APPR: [redacted]

b(6)
b(7)(C)

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
LONG BEACH RESIDENT AGENCY
501 W. OCEAN BLVD, SUITE 7300
LONG BEACH, CA 90802

(Investigations)

REPORT OF INVESTIGATION

200701690T-23-AUG-2007-50ES-W1/Z 31-JANUARY-2008

[redacted]

DISTRIBUTION

Western Field Office

b(6)
b(7)(C)

NARRATIVE

1. On July 18, 2007 [redacted], DCIS Arlington Resident Agency, referred identifying information for sixteen persons with ties to the Department of Defense (DoD) who are in the DCIS Long Beach Resident Agencies (50ES) Area of Responsibility (AOR) and are suspected of purchasing and supporting the child pornography trade. [redacted] initially received the information from Assistant United States Attorney Gerald Smagala, United States Attorney's Office (USAO), Eastern District of Virginia. The persons identified are active, reserve & retired military members, DoD civilians and DoD contractor employees, several of whom have security clearances.

2. In April 2006, the Immigration and Customs Enforcement/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 same organization is operating numerous commercial child pornography websites. In addition, the organization utilizes various PayPal accounts to process the payments for access to the member restricted websites. The investigation is being worked jointly with ICE/C3/CES, ICE/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 conducted over 60 undercover transactions at the advertising websites associated with this investigation. The investigation determined that a specific criminal organization operates approximately 18 commercial child pornography portal websites which provide access to approximately 18 child pornography member-restricted websites, using a specific and identifiable payment website known as "iWest." The investigation identified that the criminal organization (1) uses various PayPal accounts to facilitate the customer payments; (2) uses specific subject identifiers within the PayPal accounts to identify purchases into the various member restricted websites; and (3) uses specific administrative e-mail accounts that are 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 address, Fleet Post Office, or Army Post Office military zip codes to register for the PayPal service to access the child pornography websites. The four suspects identified in the 50ES AOR have been titled as subjects based upon the initial evidence that was provided to the DCIS by ICE. Based upon the fact that the subjects are DoD employees and possess security clearances, ICE has listed them as a Tier 1 priority. This investigation was coordinated with ICE [redacted], Child Exploitation Unit, Long Beach, CA, [redacted] ICE [redacted] has been assigned as the investigating agent, [redacted]

b(6)
b(7)(C)

5. After a review of [redacted] transactions in December 2007, it was determined that the probable cause for a search warrant was stale and that more recent evidence was not available. In addition to this information, it was also determined that a portion of the original nexus for the initiation of the investigation was incorrect. The information report referred had indicated that the subject had used his/her .mil account to conduct the illegal purchase of child pornography. At the time it was decided that the use of a .mil account in conjunction with the fact that the subject was a active member of the military was sufficient nexus to initiate an investigation. However, once it was determined that the use of a .mil account did not occur and that the PC was stale and no further evidence is available, this investigation is closed. There were no management control deficiencies identified during the course of this investigation.

200701690T-23-AUG-2007-50ES-W1/Z 31-JANUARY-2008

EXHIBITS

No Exhibits

Prepared By; SA [redacted], Long Beach Resident Agency APPR[redacted] b(6) b(7)(C)

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
LONG BEACH RESIDENT AGENCY
501 W. OCEAN BLVD, SUITE 7300
LONG BEACH, CA 90802

(Investigations)

REPORT OF INVESTIGATION

200701691U-23-AUG-2007-50ES-W1/Z 31-JANUARY-2008

[redacted]

DISTRIBUTION

Western Field Office

b(6)
b(7)(C)

NARRATIVE

1. On July 18, 2007 [redacted], DCIS Arlington Resident Agency, referred identifying information for sixteen persons with ties to the Department of Defense (DoD) who are in the DCIS Long Beach Resident Agencies (50ES) Area of Responsibility (AOR) and are suspected of purchasing and supporting the child pornography trade. [redacted] initially received the information from Assistant United States Attorney Gerald Smagala, United States Attorney's Office (USAO), Eastern District of Virginia. The persons identified are active, reserve & retired military members, DoD civilians and DoD contractor employees, several of whom have security clearances.

2. In April 2006, the Immigration and Customs Enforcement/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 same organization is operating numerous commercial child pornography websites. In addition, the organization utilizes various PayPal accounts to process the payments for access to the member restricted websites. The investigation is being worked jointly with ICE/C3/CES, ICE/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 conducted over 60 undercover transactions at the advertising websites associated with this investigation. The investigation determined that a specific criminal organization operates approximately 18 commercial child pornography portal websites which provide access to approximately 18 child pornography member-restricted websites, using a specific and identifiable payment website known as "iWest." The investigation identified that the criminal organization (1) uses various PayPal accounts to facilitate the customer payments; (2) uses specific subject identifiers within the PayPal accounts to identify purchases into the various member restricted websites; and (3) uses specific administrative e-mail accounts that are 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 address, Fleet Post Office, or Army Post Office military zip codes to register for the PayPal service to access the child pornography websites. The four suspects identified in the 50ES AOR have been titled as subjects based upon the initial evidence that was provided to the DCIS by ICE. Based upon the fact that the subjects are DoD employees and possess security clearances, ICE has listed them as a Tier 1 priority. This investigation was coordinated with ICE [redacted], Child Exploitation Unit, Long Beach, CA, [redacted] ICE [redacted] has been assigned as the investigating agent, [redacted]

5. After a review of [redacted] transactions in December 2007, it was determined that the probable cause for a search warrant was stale and that more recent evidence was not available. In addition

b(6)
b(7)(C)

to this information, it was also determined that a portion of the original nexus for the initiation of the investigation was incorrect. The information report referred had indicated that the subject had used his/her .mil account to conduct the illegal purchase of child pornography. At the time it was decided that the use of a .mil account in conjunction with the fact that the subject was a active member of the military was sufficient nexus to initiate an investigation. However, once it was determined that the use of a .mil account did not occur and that the PC was stale and no further evidence is available, this investigation is closed. There were no management control deficiencies identified during the course of this investigation.

IDENTITY OF SUBJECTS

Identifying Data:

Name
Alias
Social Security Number
Date/Place of Birth
Race
Sex
Residence

Employment/Occupation
Telephone Number
Education

[redacted]

b(6)
b(7)(C)

EXHIBITS

No Exhibits

Prepared By: [redacted], Long Beach Resident Agency APPR: [redacted] b(6) b(7)(C)

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
LONG BEACH RESIDENT AGENCY
501 W. OCEAN BLVD, SUITE 7300
LONG BEACH, CA 90802

(Investigations)

REPORT OF INVESTIGATION

200701692V-23-AUG-2007-50ES-W1/Z

31-JANUARY-2008

[redacted]

DISTRIBUTION

Western Field Office

b(6)
b(7)(C)

NARRATIVE

1. On July 18, 2007 [redacted], DCIS Arlington Resident Agency, referred identifying information for sixteen persons with ties to the Department of Defense (DoD) who are in the DCIS Long Beach Resident Agencies (50ES) Area of Responsibility (AOR) and are suspected of purchasing and supporting the child pornography trade. [redacted] initially received the information from Assistant United States Attorney Gerald Smagala, United States Attorney's Office (USAO), Eastern District of Virginia. The persons identified are active, reserve & retired military members, DoD civilians and DoD contractor employees, several of whom have security clearances.

2. In April 2006, the Immigration and Customs Enforcement/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 same organization is operating numerous commercial child pornography websites. In addition, the organization utilizes various PayPal accounts to process the payments for access to the member restricted websites. The investigation is being worked jointly with ICE/C3/CES, ICE/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 conducted over 60 undercover transactions at the advertising websites associated with this investigation. The investigation determined that a specific criminal organization operates approximately 18 commercial child pornography portal websites which provide access to approximately 18 child pornography member-restricted websites, using a specific and identifiable payment website known as "iWest." The investigation identified that the criminal organization (1) uses various PayPal accounts to facilitate the customer payments; (2) uses specific subject identifiers within the PayPal accounts to identify purchases into the various member restricted websites; and (3) uses specific administrative e-mail accounts that are 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 address, Fleet Post Office, or Army Post Office military zip codes to register for the PayPal service to access the child pornography websites. The four suspects identified in the 50ES AOR have been titled as subjects based upon the initial evidence that was provided to the DCIS by ICE. Based upon the fact that the subjects are DoD employees and possess security clearances, ICE has listed them as a Tier 1 priority. This investigation was coordinated with ICE [redacted], Child Exploitation Unit, Long Beach, CA, [redacted] ICE [redacted] has been assigned as the investigating agent, [redacted]

b(6)
b(7)(C)

5. After a review of [redacted] transactions in December 2007, it was determined that the probable cause for a search warrant was stale and that more recent evidence was not available. In addition to this information, it was also determined that a portion of the original nexus for the initiation of the investigation was incorrect. The information report referred had indicated that the subject had used his/her .mil account to conduct the illegal purchase of child pornography. At the time it was decided that the use of a .mil account in conjunction with the fact that the subject was a military service member was sufficient nexus to initiate an investigation. However, once it was determined that the use of a .mil account did not occur and that the PC was stale and no further evidence is available, this investigation is closed. There were no management control deficiencies identified during the course of this investigation.

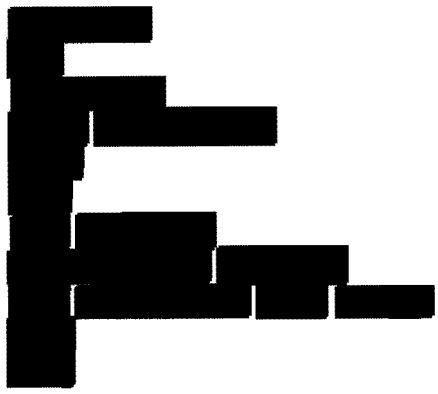
b(6)
b(7)(C)

IDENTITY OF SUBJECTS

Identifying Data:

Name
Alias
Social Security Number
Date/Place of Birth
Race
Sex
Residence

Employment/Occupation
Telephone Number
Education



b(6)
b(7)(C)

EXHIBITS

None

Prepared By; [redacted] Long Beach Resident Agency APPR: [redacted] b(6) b(7)(C)

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
SAN FRANCISCO RESIDENT AGENCY
1301 CLAY ST, STE 480N
OAKLAND, CA 94612-5217

(Investigations)

REPORT OF INVESTIGATION

200701756M-06-SEP-2007-50SF-W1/E

January 29, 2009

[redacted]

DISTRIBUTION

Western Field Office

b(6)
b(7)(C)

NARRATIVE

1. This investigation was initiated based upon a referral from [redacted], DCIS Arlington Resident Agency, Arlington VA identifying four individuals within the DCIS San Francisco Resident Agency area of responsibility who were suspected of involvement in child pornography. [redacted] initially received the information from Assistant United States Attorney (AUSA) Gerald Smagala, United States Attorney's Office (USAO), Eastern District of Virginia, Alexandria, VA. The subjects identified were reserve and retired military members, DoD contractor employees, and in one case a sub-contractor to a DoD contractor, all of whom used ".mil" e-mail addresses to allegedly register for access to child pornography websites. This investigation was conducted jointly with Immigration and Customs Enforcement (ICE) agents located in Oakland, CA, San Francisco, CA, and San Jose, CA.

2. Upon coordination with ICE regarding all four subjects, it was understood that as a matter of policy the United States Attorney's Offices (USAO), Northern District of California, San Francisco, Oakland, and San Jose, CA usually declined to accept any child pornography investigation where the subject of the investigation had not engaged in any download activity within the past six months. Due to the USAO's policy, ICE issued administrative subpoenas to PayPal to determine if the subjects had any recent download activity with known child pornography websites within the past six months. All PayPal information returned in response to the subpoenas revealed that none of the subjects had accessed child pornography within the required timeframe. At their discretion ICE agents plan to perform knock-and-talk interviews of all four subjects in order to ascertain their involvement with child pornography; however, due to the heavy case load of the assigned ICE agents and higher priority investigations, the knock-and-talk interviews are not expected to be conducted for an extended period of time.

3. Due to the policy of the USAO, the limited activity on the part of the subjects, the length of time until the interviews will be conducted by ICE, and the need to focus on other higher priority investigations, this investigation is being closed by DCIS. It is understood that the investigations will be completed by ICE as time and their case load permits. At this time, no judicial or administrative actions are expected. There were no fraud vulnerabilities identified during the course of the investigation.

b(6)
b(7)(C)

IDENTITY OF SUBJECTS

Identifying Data:

Name	:	[redacted]
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	:	
DoD Affiliation:	:	E-4, Marine Corp Reserve, Unit unknown

b(6)
b(7)(C)

IDENTITY OF SUBJECTS

		Identifying Data:
Name	:	[redacted]
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	:	
DoD Affiliation	:	E-7, U.S. Navy, Retired

b(6)
b(7)(C)

IDENTITY OF SUBJECTS

Identifying Data:

Name	:	[redacted]
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	:	
DoD Affiliation	:	

b(6)
b(7)(C)

IDENTITY OF SUBJECTS

Identifying Data:

Name	:	[redacted]
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	:	
DoD Affiliation	:	

Prepared by [redacted] San Francisco RA APPR: [redacted]

b(6)
b(7)(C)

(Investigations)

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
COLUMBUS RESIDENT AGENCY
EASTON PLAZA ONE
4449 EASTON WAY, SUITE 375
COLUMBUS, OH 43219

REPORT OF INVESTIGATION

200800080D-18-OCT-2007-40CO-W1/Z

December 3, 2007

OPERATION FLICKER, Columbus, OH

SPECIAL INTEREST CASE

NARRATIVE

1. This investigation into individuals who subscribed to predicated child pornography websites was initiated based upon information received October 15, 2007, from a Special Agent (SA) with the Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Columbus Resident Agency (RAC/Columbus) and as a result of DCIS Project "Operation Flicker" (CCN: 200701199X-29-MAY-2007-60DC-W1). ICE-Columbus referred identifying information for four individuals with ties to the Department of Defense (DoD) that are in the Columbus Resident Agency area of responsibility and are suspected of involvement in child pornography. In addition to the information provided by ICE Columbus, six additional DoD related subjects in the Cleveland, OH and Detroit, MI area were identified by the DHS-ICE Detroit, MI field office and through the efforts of the Mid-Atlantic Field Office (MAFO) in Project Flicker. The persons identified are active and retired military service members, DoD civilians, and DoD contractor employees; several of the individuals have Secret or higher clearances and some may have used .mil e-mail addresses to register for access to child pornography websites.

2. In April 2006, the Immigration and Customs Enforcement/Cyber Crimes Center/Child Exploitation Section (ICE/C3/CES) initiated an investigation of a criminal organization operating a commercial child pornography website known as "Home Collection." The investigation revealed that the same organization is 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. The is a joint investigation 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 multiple USAO offices, including the USAO for the Northern District of Alabama. ICE designated this effort Project Flicker. DCIS-MAFO and DCIS field office representatives assisted ICE after determining that DoD personnel and/or contractor personnel may have been involved in accessing and obtaining child pornography.

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

4. Project Flicker data was sorted to identify individuals who used their .mil e-mail address, Fleet Post Office (FPO), or Army Post Office (APO) military zip codes to register for the PayPal service for access to the child pornography websites. The suspects identified in the Columbus RA AOR will be titled as subjects if the investigation determines the individuals were involved in acquiring and/or transmitting child pornography. The priority for investigating suspects will be assessed based on their security clearances, position in their DoD organizations, whether their DoD position provides access to children, and whether they are a recidivist.

5. Prior to opening this investigation, the reporting agent met with Immigration and Customs Enforcement (ICE) Special Agen[redacted] Columbus, OH regarding Operation Flicker. An investigative plan was discussed. [redacted] also provided identifying information on Department of Defense employees that are in the Columbus Resident Agency area of responsibility and are suspected of being involved in child pornography. [redacted] offered ICE cooperation in this investigation.

b(6)
b(7)(C)

6. Due to DCIS Headquarters' direction and other DCIS investigative priorities, this investigation is cancelled. No subjects were formally titled in the DCIS IDS System. No judicial or administrative action will occur. There is no loss to the U.S. Government. There were no management control deficiencies identified during the course of this investigation.

Prepared by SA [redacted], Columbus RA APPR: [redacted]

b(6)
b(7)(C)

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

(Investigations)

200800157H-02-NOV-2007-40DY-W1 02-November-2007

[redacted]; SSN: [redacted]
DPOB: [redacted] Unknown
[redacted]

INFORMATION REPORT/ REFERRED: The Dayton Resident Agency (RA) received information from the Kansas City RA regarding a project that was initiated based upon information provided by the United States Attorney's Office (USAO), Eastern District of Virginia, Alexandria Division that advised the Immigration and Customs Enforcement (ICE) of a national investigation that identified over 5,000 individuals who subscribed to predicated child pornography websites. As a result of this information ICE and the U.S. Department of Justice/Child Exploitation and Obscenity Section designated this operation as Project Flicker.

As a result of Project Flicker and the initiative from the USAO, ICE identified individuals under Project Flicker associated with the military by either providing their .mil e-mail addresses, Fleet Post Office (FPO), or Army Post Office (APO) military zip codes. DCIS was requested to assist in identifying additional Department of Defense (DoD) affiliated individuals and provide investigative assistance. Targets of Operation Project Flicker that are affiliated with the military put national security at risk by compromising computer systems/e-mail systems and individuals with security clearances from the DoD compromise their clearance and put themselves and the interests of DoD at risk of blackmail, bribery, and threats.

[redacted] (SSN: [redacted], DOB: [redacted]) was identified by Project Flicker as one of these targets. Information he provided to an online payment website for subscribed child pornography websites listed an address [redacted] (attachment 1).

A DEIDS Report on [redacted] revealed that he is an enlisted 05, active duty Army, stationed at Fort Campbell, Kentucky. It provides a [redacted] (attachment 2).

A REDD Report shows that [redacted] (attachment 3).

A National Comprehensive Report provided from Choice Point was generated and lists [redacted] address abovementioned (attachment 4). 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.~~

[redacted] does not have a current Kentucky driver's license.

Army Criminal Investigation Division (CID), Fort Campbell, Kentucky, Special Agent [redacted] advised that [redacted] resides off-base and provided the address [redacted], telephone [redacted] advised that because [redacted] lives off-base housing that CID would not be involved in the investigation as it would most likely be handled by the United States Attorney's Office, unless information was gleaned that [redacted] was participating in criminal activity on-base.

Contact with [redacted], ICE Bowling Green, Kentucky office revealed that he was referring this information to the ICE Nashville, Tennessee office because [redacted] resides in Clarksville, Tennessee.

This information is being forwarded to the Nashville Post of Duty (POD) for further action since Clarksville, Tennessee falls under Nashville POD Area of Response. Any further questions regarding this report should be directed to the undersigned at telephone number [redacted]

Attachments:

1) Flicker Targets in Kentucky, 1 page
2) DEIDS Report, 1 page
3) REDD Report, 1 page
4) National Comprehensive Report, 26 pages

Prepared by [redacted], Dayton RA APPR: [redacted] b(6) b(7)(C)

DISTR: 40SL/20FO/20AT/20NV (electronically only)

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

(Investigations)

200800158I-02-NOV-2007-40DY-W1 02-November-2007

[redacted]; SSN: [redacted]
DPOB: [redacted]; Unknown
E-5 US Army (former) Ft. Campbell, KY

INFORMATION REPORT/ REFERRED: The Dayton Resident Agency (RA) received information from the Kansas City RA regarding a project that was initiated based upon information provided by the United States Attorney's Office (USAO), Eastern District of Virginia, Alexandria Division that advised the Immigration and Customs Enforcement (ICE) of a national investigation that identified over 5,000 individuals who subscribed to predicated child pornography websites. As a result of this information ICE and the U.S. Department of Justice/Child Exploitation and Obscenity Section designated this operation as Project Flicker.

As a result of Project Flicker and the initiative from the USAO, ICE identified individuals under Project Flicker associated with the military by either providing their .mil e-mail addresses, Fleet Post Office (FPO), or Army Post Office (APO) military zip codes. DCIS was requested to assist in identifying additional Department of Defense (DoD) affiliated individuals and provide investigative assistance. Targets of Operation Project Flicker that are affiliated with the military put national security at risk by compromising computer systems/e-mail systems and individuals with security clearances from the DoD compromise their clearance and put themselves and the interests of DoD at risk of blackmail, bribery, and threats.

[redacted] (SSN: [redacted], DOB: [redacted]) was identified by Project Flicker as one of these targets. Information he provided to an online payment website for subscribed child pornography websites listed an address of [redacted].

A check with the DEIDS database revealed no record of [redacted]

A REDD Report shows that [redacted] begin date with the Army was [redacted] and his end date with the Army was [redacted] was an enlisted 05 with the Army (attachment 1).

A National Comprehensive Report provided from Choice Point was generated and lists an address for [redacted] (attachment 2).

[redacted] does not have a current Kentucky driver's license.

b(6)
b(7)(C)

Army Criminal Investigation Division (CID), Fort Campbell, Kentucky, Special Agent [redacted] advised that [redacted] never lived on-base at Fort Campbell and that the address he provided, [redacted] does not exist. [redacted] advised that because [redacted] lives off-base, CID would not be involved in the investigation as it would most likely be handled by the United States Attorney's Office, unless information was gleaned that [redacted] was participating in criminal activity on-base.

Contact with [redacted], ICE Bowling Green, Kentucky office revealed that he was referring this information to the ICE Nashville, Tennessee office because [redacted] resides in Clarksville, Tennessee.

This information is being forwarded to the Nashville Post of Duty (POD) for further action since Clarksville, Tennessee falls under Nashville POD Area of Response. Any further questions regarding this report should be directed to the undersigned at telephone number [redacted]

Attachments:

1) REDD Report, 1 page
2) National Comprehensive Report, 5 pages

Prepared by [redacted], Dayton RA APPR: [redacted]
DISTR: 40SL/20FO/20AT/20NV (electronically only)

b(6)
b(7)(C)

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

(Investigations)

200800159J-02-NOV-2007-40DY-W1 02-November-2007

[redacted]; SSN: [redacted]
DPOB: [redacted]

INFORMATION REPORT/ REFERRED: On June 25, 2007, the Dayton Resident Agency (RA) received information from the Kansas City RA regarding a project that was initiated based upon information provided by the United States Attorney's Office (USAO), Eastern District of Virginia, Alexandria Division that advised the Immigration and Customs Enforcement (ICE) of a national investigation that identified over 5,000 individuals who subscribed to predicated child pornography websites. As a result of this information ICE and the U.S. Department of Justice/Child Exploitation and Obscenity Section designated this operation as Project Flicker.

As a result of Project Flicker and the initiative from the USAO, ICE identified individuals under Project Flicker associated with the military by either providing their .mil e-mail addresses, Fleet Post Office (FPO), or Army Post Office (APO) military zip codes. DCIS was requested to assist in identifying additional Department of Defense (DoD) affiliated individuals and provide investigative assistance. Targets of Operation Project Flicker that are affiliated with the military put national security at risk by compromising computer systems/e-mail systems and individuals with security clearances from the DoD compromise their clearance and put themselves and the interests of DoD at risk of blackmail, bribery, and threats.

[redacted] (SSN: [redacted], DOB: [redacted]) was identified by Project Flicker as one of these targets. Information he provided to an online payment website for subscribed child pornography websites listed an address [redacted] and an email address of [redacted] (attachment 1).

A DEIDS Report on [redacted] revealed that he is an enlisted 03, active duty Army, stationed at [redacted] Fort Bliss, Texas 79916. It provides a home address of [redacted] telephone [redacted] (SSN: [redacted], DOB: [redacted], [redacted] (attachment 2).

A REDD Report shows that [redacted] begin date was [redacted] and his end date with the Army is [redacted] (attachment 3).

b(6)
b(7)(C)

A National Comprehensive Report provided from Choice Point was generated and lists [redacted] at [redacted] (attachment 4).

[redacted] does not have a current Kentucky driver's license.

A criminal history was run for [redacted] which revealed a charge of "wrongful use of marijuana" by the US Army at Fort Belvoir on February 2, 2005. It lists [redacted] as being a [redacted] (attachment 5).

Army Criminal Investigation Division (CID), Fort Campbell, Kentucky, Special Agent [redacted] advised that [redacted] never resided on-base while stationed at Fort Campbell, Kentucky and that he is currently stationed at Fort Bliss, Texas. CID forwarded this information to CID Fort Bliss, Texas.

This information is being forwarded to the El Paso Post of Duty (POD) for further action since Fort Bliss, Texas falls under El Paso POD Area of Response. Any further questions regarding this report should be directed to the undersigned at telephone number [redacted]

Attachments:

1) Flicker Targets in Kentucky, 1 page
2) DEIDS Report, 1 page
3) REDD Report, 1 page
4) National Comprehensive Report, 10 pages
5) Criminal History, 5 pages

Prepared by [redacted], Dayton RA
DISTR: 40SL/30FO/30HS/30EP (electronically only)

APPR: [redacted] b(6) b(7)(C)

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
SACRAMENTO POST OF DUTY
2800 COTTAGE WAY, SUITE W-1946
SACRAMENTO, CA 95825

(Investigations)

200800168S-05-NOV-2007-50SM-U0/X (IR) 5-November-2007

[redacted] SSN: [redacted]
DPOB: [redacted]; UNK
[redacted]

INFORMATION REPORT: The DCIS Arlington Resident Agency referred identifying information for persons with ties to the Department of Defense (DoD) that are in the DCIS Sacramento Post of Duty (POD) area of responsibility (AOR) and are suspected of involvement in child pornography. The DCIS Arlington Resident Agency initially received the information from the 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 or had Top Secret security clearances and all of whom used .mil e-mail addresses to register for access to child pornography websites.

As background, in April 2006, the Immigration and Customs Enforcement/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 same organization was operating numerous commercial child pornography websites. In addition, the organization utilized various Pay Pal accounts to process the payments for access to the member restricted 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**. ICE/C3/CES conducted over 60 undercover transactions at the advertising websites associated with this investigation. The investigation determined that a specific criminal organization operates approximately 18 commercial child pornography portal websites which provide access to approximately 18 child pornography member-restricted websites, using a specific and identifiable payment website known as "iWest." The investigation identified that the criminal organization (1) uses various Pay Pal accounts to facilitate the customer payments; (2) uses specific subject identifiers within the Pay Pal accounts to identify purchases into the various member restricted websites; and (3) uses specific administrative e-mail accounts that are used to distribute access to the member restricted websites. **Project Flicker** data was sorted to identify individuals who used their .mil e-mail address, Fleet Post Office (FPO), or Army Post Office (APO) military zip codes to register for the Pay Pal service to access the child pornography websites. The suspects' names were queried in DCII, Auto Track and other

b(6)
b(7)(C)

[redacted]

applicable databases. This investigation was coordinated with the Air Force Office of Special Investigations (AFOSI), Travis Air Force Base, CA.

In Summary, SUBJECT was identified by PROJECT FLICKER, as a possible paying member of a website containing child pornography. On September 27, 2007, an interview of SUBJECT was conducted by [redacted], DCIS, Sacramento POD, Sacramento, CA and [redacted] AFOSI Detachment 303, Travis AFB, CA. SUBJECT was advised of his rights according to Article 31, Uniform Code of Military Justice (UCMJ). SUBJECT acknowledged he understood his rights, declined legal counsel and stated he was willing to answer questions. SUBJECT admitted to paying approximately $97.00 through a Pay Pal account for access to a pornography website. SUBJECT stated he logged on and viewed the site for 1-2 hours before noticing thumbnail images of females approximately 10 years of age. SUBJECT stated he immediately left the site and never went back. ICE records indicate SUBJECT only visited the site once. SUBJECT was released to his supervisor with no further investigative steps planned.

SUBJECT was advised of his rights in accordance with Article 31, (UCMJ). SUBJECT acknowledged his rights, declined legal counsel and agreed to answer questions. SUBJECT provided the following information in a signed, sworn statement: SUBJECT stated some time in the past he signed up for a pornographic website. SUBJECT did not remember the exact amount he paid for access to the site. SUBJECT stated he received a username and password via his HOTMAIL account. SUBJECT logged into the site and began browsing. SUBJECT stated he got to a page containing what appeared to be underage females. SUBJECT stated he immediately left the website and never went back again. SUBJECT signed up using a Pay Pal online cash account. SUBJECT reported the loss of his credit card number in the past and had unknown charges on the stolen card. SUBJECT related one of the charges was for "Video Professor" software which was mailed to his address. SUBJECT checked with the card company and they told him there were several other charges. SUBJECT stated he disputed the charges, cancelled the card and was issued a new card. SUBJECT believes he lost the card last year. SUBJECT stated he has never "surfed" for child porn. SUBJECT has received several emails advertising porn sites but he just deletes them. The site he paid to access had adult women on the first page. On subsequent pages of the site, there were thumbnail images showing females approximately 10 years of age. SUBJECT stated he left the site when he saw the underage females. SUBJECT stated he never looked at the child porn images. Additionally, SUBJECT stated verbally he looked at the website for "one or two hours" before noticing the underage females. Agents inquired into the possibility of a consent search of his computer. SUBJECT stated he didn't feel comfortable with anyone looking on his computer. Consent was refused. Due to SUBJECT currently being on terminal leave awaiting his retirement and no substantial evidence found concerning the allegation, no further investigation is warranted. SUBJECT provided investigators with a signed, sworn statement.

b(6)
b(7)(C)

[redacted]

Attachments

1. Rights Advisement form, September 27, 2007
2. Signed, Sworn Statement of [redacted] dated September 27, 2007.

Prepared by: [redacted], Sacramento Post of Duty APPR: [redacted] b(6) b(7)(C)

DISTR: 60DC