PROJECT: OPERATION FLICKER

DISTRIBUTION:

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

1. In April 2007, 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. 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
   • 200701277C
   • 200701301F - Sweeney, Daniel Joseph
   • 200701340S
   • 200701341T - Campbell, Cameron Morrison
   • 200701402H - Kartes, Thomas Edward
   • 200701403I
   • 200701403J

A-1
Six Information Reports were completed, to include 200800168S; 200800159J; 2008001581; 200800157H; and 200701239Q.

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.

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.
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 Retired Navy Captain (O-6).

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

The RA spoke with ICE Special Agent (SA) in Tampa, Florida and briefed her on DCIS’ joint efforts on Operation Flicker. welcomed any assistance DCIS can provide. can be reached by telephone at extension or 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.
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. DEIDS/JPAS Results
3. DCII Results
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 a Retired U.S. Navy Captain (O-6).

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

5. On June 18, 2007, the RA telephonically contacted to offer DCIS assistance with the investigation. During the conversation, clarified information previously received from the IR and subsequently was included in the case initiation. 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.

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

7. On September 27, 2007, the RA coordinated with, Naval Criminal Investigative Service (NCIS), Resident Agency, Yokosuka, Japan, to request assistance with the execution of a search warrant of residence. verified was hired.
agreed to coordinate with the ICE, Attaché Office and the local Japanese Police Department in order to obtain a search warrant for residence.

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

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

10. On January 14, 2008, provided the RA a copy of two computer forensic exams. The first forensic exam was performed on laptop computer, which was seized during the execution of the search warrant on residence located in Japan. The second forensic exam was performed on desktop computer which was seized during the execution of the search warrant on residence in 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.
IDENTITY OF SUBJECT:
IDENTIFYING DATA

Name
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-1
REPORT OF INVESTIGATION

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

February 27, 2008

DISTRIBUTION:

DCIS Headquarters, National Security Program (03NS)
Immigration and Customs Enforcement, SAC Washington, D.C. (opacity) 
U.S. Army Criminal Investigation Command 902nd Military Intelligence (opacity)
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. 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 Lieutenant Colonel (O-5), with the U.S. Army Reserve (USAR). Records revealed was on active duty. A query of JPAS revealed he was a

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

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

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

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


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.”
IDENTITY OF SUBJECTS:

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

February 27, 2008

b(8) FOR OFFICIAL USE ONLY
b(7)(C) LAW ENFORCEMENT SENSITIVE

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

1. DCFL Digital Forensic Analysis Report

Prepared by Special Agent [Redacted], Arlington Resident Agency   APPR: [Redacted]
REPORT OF INVESTIGATION

200701402H-09-JUL-2007-60DC-W1/F

KARTES, THOMAS EDWARD

February 25, 2008

DISTRIBUTION:

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

CLASSIFICATION:

FOR OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE

WARNING: This document is the property of the Department of Defense Inspector General and is on loan to your agency. Documents may not be disseminated to anyone under investigation nor may this document be distributed outside the receiving agency without specific prior authorization of the Deputy Inspector General for Investigations.
NARRATIVE:

1. This case was initiated based on information derived from DCIS Project: Operation Flicker (Case Control Number 200701199X). 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. 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. A query of JPAS revealed Kartes was on active duty.

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.

5. Concurrent to the execution of the search warrant, ICE and FCPD 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.”

A-1

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Kartes, Thomas Edward</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>None</td>
</tr>
<tr>
<td>Social Security Number</td>
<td>000-00-0000</td>
</tr>
<tr>
<td>Date/Place of Birth</td>
<td>1970-01-01</td>
</tr>
<tr>
<td>Race</td>
<td>000</td>
</tr>
<tr>
<td>Sex</td>
<td>M</td>
</tr>
<tr>
<td>Height</td>
<td>000</td>
</tr>
<tr>
<td>Weight</td>
<td>000</td>
</tr>
<tr>
<td>Hair</td>
<td>000</td>
</tr>
<tr>
<td>Eyes</td>
<td>000</td>
</tr>
<tr>
<td>Residence</td>
<td>000</td>
</tr>
<tr>
<td>Employment/Occupation</td>
<td>Major (O-4), U.S. Army Reserve</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>000-00-0000</td>
</tr>
<tr>
<td>Driver's License Number and Issuing State</td>
<td>000-00-0000, State</td>
</tr>
<tr>
<td>Education</td>
<td>000</td>
</tr>
</tbody>
</table>

Prepared by Special Agent [Blank], Arlington Resident Agency  APPR: [Blank]
On July 11, 2007, the Reporting Agent received a lead referral from Special Agent 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.

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 have possessed child pornographic material. One subject identified was 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, 

RAC coordinated with , Supervisor, ICE Pittsburgh, and 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).

On August 9, 2007, Reporting Agent received photo ID and driver’s license information on.

On January 14, 2008, Reporting Agent requested and later received military personnel files and records of . Reporting Agent reviewed military personnel files provided on but was unable to determine global location, let alone 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.

From discussion with Special Agent 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 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 may have downloaded photos and to which, if any, computer was utilized for such purpose. Further, the location of such computer and establishing that 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
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.
IDENTITY OF SUBJECTS

IDENTIFYING DATA

Name:
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:

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 agency without the specific prior authorization of the Deputy Inspector General for investigations.
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
REPORT OF INVESTIGATION

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

DISTRIBUTION

Headquarters, Investigative Operations Directorate
Northeast Field Office
Pittsburgh Resident Agency

CLASSIFICATION:
OFFICIAL USE ONLY

This document is the property of the Department of Defense Inspector General and is intended for use by the receiving agency. Contents may not be disclosed to any party under investigation and this document must not be distributed outside the receiving agency without the specific prior authorization of the Assistant Inspector General for Investigations.
NARRATIVE

1. On July 11, 2007, the reporting agent received a lead referral from Special Agent [Redacted] of the 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 predatory child pornography websites. The [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.
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:  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: 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 PayPal accounts still identify the specific member restricted sites an individual purchased).
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

<table>
<thead>
<tr>
<th>Name</th>
<th>:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>:</td>
</tr>
<tr>
<td>Social Security Number</td>
<td>:</td>
</tr>
<tr>
<td>Date of Birth</td>
<td>:</td>
</tr>
<tr>
<td>Sex</td>
<td>:</td>
</tr>
<tr>
<td>Race</td>
<td>:</td>
</tr>
<tr>
<td>Height</td>
<td>:</td>
</tr>
<tr>
<td>Weight</td>
<td>:</td>
</tr>
<tr>
<td>Eyes</td>
<td>:</td>
</tr>
<tr>
<td>Hair</td>
<td>:</td>
</tr>
<tr>
<td>Residence</td>
<td>:</td>
</tr>
</tbody>
</table>
EXHIBITS

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

Prepared by: [redacted], Syracuse Post of Duty

APPR: [redacted]
REPORT OF INVESTIGATION

200701517X-25-JUL-2007-10PB-Z0/Z

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

CLASSIFICATION:

FOR OFFICIAL USE ONLY

WARNING: This document is the property of the Department of Defense Inspector General and is confidential 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.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>NARRATIVE</th>
<th>A</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDENTITY OF SUBJECT(S)</td>
<td>B</td>
</tr>
<tr>
<td>EXHIBIT(S)</td>
<td>C</td>
</tr>
</tbody>
</table>
NARRATIVE

1. On July 11, 2007, the Reporting Agent received a lead referral from Special Agent, 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 a Corporal (E-5, Enlisted) 

3. The Reporting Agent contacted Special Agent, 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 email address and Internet service provider from Special Agent. Also on that date, Special Agent requested that the Reporting Agent obtain military personnel file (Exhibit 2).

5. On November 16, 2007, the Reporting Agent obtained personnel file and contacted Special Agent, but received no response. Since then, the Reporting Agent has attempted numerous times to contact Special Agent through email and phone calls but he has continued to be non-responsive. In addition, Resident Agent in Charge, contacted Special Agent, ICE Pittsburgh, and advised him of the situation. However to date 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.
IDENTITY OF SUBJECTS:

OFFICIAL

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

WARNING: This document is the property of the Department of Defense Inspector General and is subject 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.
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 Personnel File, November 16, 2007
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).

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
REPORT OF INVESTIGATION

200701553H-31-JUL-2007-40SX-Y0/U

17-MARCH-2008

DISTRIBUTION

DCISHQ (03NS)
Central Field Office (40FO)
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 that [redacted] is a Sergeant First Class and works [redacted] with the North Dakota Army National Guard (NDANG).

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. 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
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 the 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.
IDENTITY OF SUBJECTS

<table>
<thead>
<tr>
<th>Name</th>
<th>:</th>
</tr>
</thead>
</table>
| Alias| :
| Social Security Number| :
| Date of Birth| :
| Race | :
| Sex | :
| Residence | :
| Employment/Occupation | :
| Telephone Number | :

IDENTIFYING DATA

- [Redacted]
EXHIBITS

None. Previously submitted.
REPORT OF INVESTIGATION

200701606N-08-AUG-2007-50LA-W1

GRANT, GARY DOUGLASS

November 17, 2009

DISTRIBUTION

DCIS, Headquarters (03NS)
ICE, Santa Ana, CA
NARRATIVE

1. On July 18, 2007, 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. 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 and 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.
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

<table>
<thead>
<tr>
<th>NAME</th>
<th>Gary Douglass Grant</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALIAS</td>
<td>Gary Douglass Grant; Gary Dougals Grant</td>
</tr>
<tr>
<td>DOB</td>
<td>August 21, 1957</td>
</tr>
<tr>
<td>SSN</td>
<td>[redacted]</td>
</tr>
<tr>
<td>HEIGHT</td>
<td>68&quot;</td>
</tr>
<tr>
<td>WEIGHT</td>
<td>170 lbs.</td>
</tr>
<tr>
<td>HAIR</td>
<td>Brown</td>
</tr>
<tr>
<td>EYES</td>
<td>Blue</td>
</tr>
<tr>
<td>ADDRESS</td>
<td>[redacted]</td>
</tr>
<tr>
<td>PHONE</td>
<td>[redacted]</td>
</tr>
<tr>
<td>DRIVERS LICENSE #</td>
<td>[redacted]</td>
</tr>
<tr>
<td>STATUS</td>
<td>Unknown</td>
</tr>
<tr>
<td>OCCUPATION</td>
<td>Lawyer</td>
</tr>
</tbody>
</table>
EXHIBITS

3. DCIS Form 1, "People Vs Grant Minute Order," dated November 11, 2009, with attachment.
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>
<thead>
<tr>
<th>SECTION</th>
<th>TABLE OF CONTENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Synopsis</td>
</tr>
<tr>
<td>A</td>
<td>Statutes</td>
</tr>
<tr>
<td>B</td>
<td>Background</td>
</tr>
<tr>
<td>B</td>
<td>Narrative</td>
</tr>
<tr>
<td>C</td>
<td>Identity of Subjects</td>
</tr>
<tr>
<td>D</td>
<td>Law Enforcement Records</td>
</tr>
<tr>
<td>E</td>
<td>Evidence</td>
</tr>
<tr>
<td>F</td>
<td>Status of Investigation</td>
</tr>
<tr>
<td>F</td>
<td>Prosecutive Considerations</td>
</tr>
<tr>
<td>G</td>
<td>Exhibits</td>
</tr>
</tbody>
</table>
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 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
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. The RA 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 and 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).


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 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 which was among the images identified on Mattes’ computer.
IDENTITY OF SUBJECTS

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

IDENTIFYING DATA
IDENTITY OF SUBJECTS

<table>
<thead>
<tr>
<th>Name</th>
<th>James Dean Mattes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>UNK</td>
</tr>
<tr>
<td>Social Security Number</td>
<td>[redacted]</td>
</tr>
<tr>
<td>Date/Place of Birth</td>
<td>7/11/1970, UNK</td>
</tr>
<tr>
<td>Race</td>
<td>Caucasian</td>
</tr>
<tr>
<td>Sex</td>
<td>Male/Female</td>
</tr>
<tr>
<td>Height</td>
<td>6'2&quot;</td>
</tr>
<tr>
<td>Weight</td>
<td>200 lbs</td>
</tr>
<tr>
<td>Hair</td>
<td>Brown</td>
</tr>
<tr>
<td>Eyes</td>
<td>Brown</td>
</tr>
<tr>
<td>Residence</td>
<td>[redacted]</td>
</tr>
<tr>
<td>Employment/Occupation</td>
<td>Former Navy Recruiter</td>
</tr>
<tr>
<td></td>
<td>E-7</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>UNK</td>
</tr>
<tr>
<td>Home</td>
<td>UNK</td>
</tr>
<tr>
<td>Driver’s License Number and Issuing State</td>
<td>UNK</td>
</tr>
<tr>
<td>Education</td>
<td>UNK</td>
</tr>
</tbody>
</table>
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.
EXHIBITS

Previously submitted.
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] was in the U.S. Navy Reserves, E-05.

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 voluntarily turn over computer for forensic review, but [redacted] refused. [redacted] then terminated the interview.

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

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

Prepared by Special Agent [Redacted], Arlington Resident Agency  APPR: [Redacted]
REPORT OF INVESTIGATION


DISTRIBUTION

Western Field Office
NARRATIVE

1. On July 18, 2007, the 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. 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 Child Exploitation Unit, Long Beach, CA. ICE has been assigned as the investigating agent.
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.
IDENTITY OF SUBJECTS

Identifying Data:

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

Employment/Occupation
Telephone Number
Education
EXHIBITS

No Exhibits
REPORT OF INVESTIGATION


DISTRIBUTION

Western Field Office
NARRATIVE

1. On July 18, 2007, 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. 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, Child Exploitation Unit, Long Beach, CA, and ICE, has been assigned as the investigating agent.
5. After a review of 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.
EXHIBITS

No Exhibits

Prepared By; SA __________________, Long Beach Resident Agency               APPR __________________
REPORT OF INVESTIGATION


DISTRIBUTION

Western Field Office
1. On July 18, 2007, the 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. 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 I priority. This investigation was coordinated with ICE Child Exploitation Unit, Long Beach, CA, and has been assigned as the investigating agent.

5. After a review of 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.
IDENTITY OF SUBJECTS

Identifying Data:

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

Employment/Occupation
Telephone Number
Education
EXHIBITS

No Exhibits

Prepared By [Redacted], Long Beach Resident Agency

APPR [Redacted]
REPORT OF INVESTIGATION


DISTRIBUTION

Western Field Office
NARRATIVE

1. On July 18, 2007, 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. 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, Child Exploitation Unit, Long Beach, CA, and has been assigned as the investigating agent.
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.
IDENTITY OF SUBJECTS

Identifying Data:

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

Employment/Occupation
Telephone Number
Education
EXHIBITS

None
REPORT OF INVESTIGATION

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

January 29, 2009

DISTRIBUTION

Western Field Office
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.
IDENTITY OF SUBJECTS

<table>
<thead>
<tr>
<th>Identifying Data:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td></td>
</tr>
<tr>
<td>Alias</td>
<td></td>
</tr>
<tr>
<td>Social Security Number</td>
<td></td>
</tr>
<tr>
<td>Date/Place of Birth</td>
<td></td>
</tr>
<tr>
<td>Race</td>
<td></td>
</tr>
<tr>
<td>Sex</td>
<td></td>
</tr>
<tr>
<td>Height</td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td></td>
</tr>
<tr>
<td>Hair</td>
<td></td>
</tr>
<tr>
<td>Eyes</td>
<td></td>
</tr>
<tr>
<td>Residence</td>
<td></td>
</tr>
<tr>
<td>Employment/Occupation</td>
<td></td>
</tr>
<tr>
<td>Telephone Number</td>
<td></td>
</tr>
<tr>
<td>Driver’s License Number and Issuing State</td>
<td></td>
</tr>
<tr>
<td>Education</td>
<td></td>
</tr>
<tr>
<td>DoD Affiliation:</td>
<td>E-4, Marine Corp Reserve, Unit unknown</td>
</tr>
</tbody>
</table>
IDENTITY OF SUBJECTS

Identifying Data:

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

Employment/Occupation : 
Telephone Number : 
Driver’s License Number and Issuing State : 
Education : 

DoD Affiliation : E-7, U.S. Navy, Retired
IDENTITY OF SUBJECTS

Identifying Data:

<table>
<thead>
<tr>
<th>Name</th>
<th>:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>:</td>
</tr>
<tr>
<td>Social Security Number</td>
<td>:</td>
</tr>
<tr>
<td>Date/Place of Birth</td>
<td>:</td>
</tr>
<tr>
<td>Race</td>
<td>:</td>
</tr>
<tr>
<td>Sex</td>
<td>:</td>
</tr>
<tr>
<td>Height</td>
<td>:</td>
</tr>
<tr>
<td>Weight</td>
<td>:</td>
</tr>
<tr>
<td>Hair</td>
<td>:</td>
</tr>
<tr>
<td>Eyes</td>
<td>:</td>
</tr>
<tr>
<td>Residence</td>
<td>:</td>
</tr>
<tr>
<td>Employment/Occupation</td>
<td>:</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>:</td>
</tr>
<tr>
<td>Driver’s License Number and Issuing State</td>
<td>:</td>
</tr>
<tr>
<td>Education</td>
<td>:</td>
</tr>
<tr>
<td>DoD Affiliation</td>
<td>:</td>
</tr>
</tbody>
</table>
IDENTITY OF SUBJECTS

Identifying Data:

<table>
<thead>
<tr>
<th>Name</th>
<th>:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>:</td>
</tr>
<tr>
<td>Social Security Number</td>
<td>:</td>
</tr>
<tr>
<td>Date/Place of Birth</td>
<td>:</td>
</tr>
<tr>
<td>Race</td>
<td>:</td>
</tr>
<tr>
<td>Sex</td>
<td>:</td>
</tr>
<tr>
<td>Height</td>
<td>:</td>
</tr>
<tr>
<td>Weight</td>
<td>:</td>
</tr>
<tr>
<td>Hair</td>
<td>:</td>
</tr>
<tr>
<td>Eyes</td>
<td>:</td>
</tr>
<tr>
<td>Residence</td>
<td>:</td>
</tr>
<tr>
<td>Employment/Occupation</td>
<td>:</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>:</td>
</tr>
<tr>
<td>Driver’s License Number and Issuing State</td>
<td>:</td>
</tr>
<tr>
<td>Education</td>
<td>:</td>
</tr>
<tr>
<td>DoD Affiliation</td>
<td>:</td>
</tr>
</tbody>
</table>
REPORT OF INVESTIGATION

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

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 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 Agent [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.
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.
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.

Project Flicker as one of these targets. Information he provided to an online payment website for subscribed child pornography websites listed an address (attachment 1).

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

A REDD Report shows that (attachment 3).

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

(SSID: , DOB: ) 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 .

A check with the DEIDS database revealed no record of .

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

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

does not have a current Kentucky driver’s license.
Army Criminal Investigation Division (CID), Fort Campbell, Kentucky, Special Agent advised that he never lived on-base at Fort Campbell and that the address he provided does not exist. advised that because he 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 was participating in criminal activity on-base.

Contact with, ICE Bowling Green, Kentucky office revealed that he was referring this information to the ICE Nashville, Tennessee office because 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.

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

Prepared by, Dayton RA
DISTR: 40SL/20FO/20AT/20NV (electronically only)
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 Fort Bliss, Texas 79916. It provides a home address of [redacted] telephone [redacted] (SSN: [redacted], DOB: [redacted]) (attachment 2).

A REDD Report shows that [redacted] begin date was [redacted] and his end date with the Army is [redacted] (attachment 3).
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)
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
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 "surf ed" 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.
Attachments
1. Rights Advisement form, September 27, 2007

Prepared by: [redacted], Sacramento Post of Duty
DISTR: 60DC

APPRE: [redacted]
REPORT OF INVESTIGATION


DISTRIBUTION

Headquarters, Investigative Operations Directorate
Northeast Field Office
Pittsburgh Resident Agency

CLASSIFICATION: FOR OFFICIAL USE ONLY

WARNING

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

1. On July 11, 2007, the reporting agent received a lead referral from Special Agent [DELETED] DCIS Mid-Atlantic Field Office regarding the Immigration and Customs Enforcement (ICE) initiated Operation Flicker. Operation Flicker is a nationwide investigation that has identified over 5,000 individuals that have subscribed to predicated child pornography websites. SA [DELETED] sent a list of individuals in New York State that are employed by the Department of Defense/U.S. Military, that have subscribed to websites that contain child pornographic images or other material that exploit children via the internet.

2. In April 2006, the ICE/Cyber Crimes Center/Child Exploitation Section (ICE/C3/CES) initiated an investigation into a criminal organization operating a commercial child pornography website known as “Home Collection.” The investigation has revealed that the same organization is operating numerous commercial child pornography websites. In addition, the organization utilizes various Pay Pal accounts to process the payments for access to the member restricted areas of these websites. The investigation is being worked jointly with ICE/C3/CES, ICE/RAC/Birmingham, the U.S. Postal Inspection Service, the U.S. Department of Justice/Child Exploitation and Obscenity Section, and the USAO for the Northern District of Alabama. ICE has designated this operation as PROJECT FLICKER.

3. ICE/C3/CES has conducted over 60 undercover transactions at the advertising websites associated with this investigation. The investigation has identified that a specific criminal organization is operating approximately 18 different commercial child pornography advertising websites which provide access to approximately 18 child pornography member restricted websites.

4. Among the 5,000 names ICE identified under Project Flicker, several individuals used their .mil e-mail address, Fleet Post Office (FPO), or Army Post Office (APO) military zip codes. SA [DELETED] advised the U.S. Attorney’s Office and ICE that the DCIS will assist in identifying any additional Department of Defense (DoD) affiliated individuals and provide any investigative assistance.

5. SA [DELETED] conducted queried DoD databases to identify individuals that may be in possession of child pornographic material or access, and has forwarded the results of his queries to the respective DCIS office for consideration for possible DCIS case initiations. SA [DELETED] 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 [DELETED].

6. The reporting agent queried the Defense Employee Interactive Data Systems (DEIDS), and obtained the following information regarding [DELETED].
7. The reporting agent also queried the Re-Enlistment Eligibility Data Display (REDD) database for and obtained the following information:

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

9. Upon review of the spreadsheet sent by the reporting agent determined that made one payment utilizing PayPal to the restricted access websites. The transaction occurred on January 30, 2007 for $79.95. The “trans.Item Title” was either listed as an invoice number: Invoice # 41041. (Agent Note: this is the subject line identifier which indicates which member restricted site a specific customer purchased. In the Project Flicker Overview report, it stated that in November 2006, the criminal organization omitted the subject line identifiers, and began using Invoice numbers. The ICE agent stated that the PayPal accounts still identify the specific member restricted sites an individual purchased). The reporting agent will review the spreadsheet, and will report the details under a separate Form 1.

10. On November 16, 2007, the reporting agent, and conducted a consent search at the residence of The interview report was written by SA

11. and SA conducted a preliminary computer forensic review of two desktop computers and one laptop computer. During the initial review of the computers, the agents discovered numerous child pornographic materials on one of the computers believed to be utilized by The computer that contained the child pornographic material was seized by and ICE will maintain custody of the computer. The review/analysis of the computer will be conducted by after a search warrant is issued by the U.S. District Court, Northern District of New York. During the next reporting period, it is anticipated that the search warrant will be issued for the complete examination of the seized computer.

12. The reporting agent and have been in contact with Assistant United States Attorney (AUSA) for consideration of criminal prosecution in violation of Certain Activities Related to the Sexual Exploitation of Minors, Title 18 USC § 2252.
13. In February 2008, the reporting agent obtained a copy of military service records from the National Archives and Records Administration in St. Louis, MO. The records indicated that

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

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

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

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

<table>
<thead>
<tr>
<th>Name</th>
<th>:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>:</td>
</tr>
<tr>
<td>Social Security Number</td>
<td>:</td>
</tr>
<tr>
<td>Date of Birth</td>
<td>:</td>
</tr>
<tr>
<td>Sex</td>
<td>:</td>
</tr>
<tr>
<td>Race</td>
<td>:</td>
</tr>
<tr>
<td>Height</td>
<td>:</td>
</tr>
<tr>
<td>Weight</td>
<td>:</td>
</tr>
<tr>
<td>Eyes</td>
<td>:</td>
</tr>
<tr>
<td>Hair</td>
<td>:</td>
</tr>
<tr>
<td>Residence</td>
<td>:</td>
</tr>
</tbody>
</table>

(b)(6),(b)(7)(C)
REPORT OF INVESTIGATION

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

April 9, 2009

DISTRIBUTION:

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

FOR OFFICIAL USE ONLY

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

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

2. SA Victor [Redacted] DCIS Arlington RA, utilized information contained within the DoD Employee Interactive Data System and the Joint Personnel Adjudication Systems to identify DoD affiliated individuals. Among those identified was [Redacted], an employee of Oracle Corporation who supported a contract for the National Security Agency. A query of JPAS revealed that [Redacted] held a top secret clearance.

3. AUSA Smagala advised that [Redacted] was previously identified in another ICE operation that collected subscriber information to predicated child pornography sites. In 2003, under Operation Falcon, ICE executed a search warrant in Florida of a credit card processing company called Regpay. Among the items seized during the warrant were subscriber records. [Redacted] was 1 of 400 targets in Virginia who purchased subscriptions to various child pornography websites. [Redacted] had approximately 21 purchases, making him the largest buyer in Virginia. In addition, two other people at [Redacted] residence purchased approximately 11 additional subscriptions. A review of [Redacted] credit card records revealed multiple purchases to child pornography websites. Federal search warrants were unattainable due to the staleness of the information gathered from Operation Falcon. [Redacted] was never interviewed. However, under Operation Flicker [Redacted] was identified as making approximately four purchases.


5. During a non-custodial interview of [Redacted] he stated that he worked for [Redacted] and he had been doing computer work for several years to include website consulting for

6. [Redacted] said that it was fair to say that he had an interest in child pornography for about 3 years prior to his interview. [Redacted] said that he spent about $50 to $60 monthly on the various sexually explicit sites. [Redacted] said that after each session on the computer (porn sites) he wiped the Internet history off the system. [Redacted] said that there would be a mixture of pornography on the computer; there will be adult porn, child porn, and sexual activity with animals. [Redacted] said that his wife had no knowledge of his pornography interests.
On June 20, 2007, SA... representatives at their office located at... representatives agreed to the release of both computers to SA... for forensic analysis. The human resources manager advised that she was suspending all access to... and was putting... on administrative leave with pay.

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

On July 25, 2007, an additional search warrant was obtained for... issued desktop computer.

A forensic examination of... computers revealed images of child pornography.

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

SA... advised that... fled the U.S. and was believed to be in Libya. On March 28, 2008, an arrest warrant was issued for...


Until... is arrested and extradited to the U.S., no further criminal, civil or administrative activity by the DCIS will occur. This case is closed as “finished.”
<table>
<thead>
<tr>
<th>Identity of Subjects</th>
</tr>
</thead>
</table>
| Name                         | [redacted]  
| Social Security Number       | [redacted]  
| Date/Place of Birth          |  
| Race                         |  
| Sex                          |  
| Height                       |  
| Weight                       |  
| Hair                         |  
| Eyes                         |  
| Residence                    |  
| Employment/Occupation        |  
| Telephone Number             |  
| Driver's License Number      |  
| and Issuing State            |  
| Passport Number              |  
| Education                    |  

Prepared by Special Agent [redacted] Arlington Resident Agency
APPR: [redacted]
REPORT OF INVESTIGATION

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

21-NOVEMBER-2008

Distribution
DCIS Headquarters
Northeast Field Office
<table>
<thead>
<tr>
<th>Table of Contents</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Narrative</td>
<td>A</td>
</tr>
<tr>
<td>Identity of Subjects</td>
<td>B</td>
</tr>
</tbody>
</table>
Narrative

1. This case was initiated upon referral of the Defense Contract Management Agency (DCMA), Hartford, CT. On March 14, 2007, DCMA Hartford, requested DCIS assistance in evaluating possible child pornography images contained on the hard drive of a government owned computer assigned to DCMA Hamilton Sundstrand.

2. In January 2007, DCMA received a complaint indicating that was using his government computer to play games. DCMA Information Technology personnel remotely accessed government computer and found evidence that he was accessing internet gaming websites and pornographic websites. On January 26, 2007, DCMA seized government computer hard drive for analysis. During a subsequent analysis of the hard drive, DCMA forensic examiners identified images that they thought could constitute child pornography.

3. On March 14, 2007, DCMA Hartford, requested DCIS assistance in reviewing the contents of hard drive for evidence of child pornography. DCIS forensic examiners analyzed the hard drive, and identified approximately 40 images suspected of being child pornography. Each of these images was a so called "thumbnail" image, indicating that the image was reviewed on line, but was not downloaded. The images were run against the National Child Victim Identification Program (NCVIP), and none of the images was positively identified as a known child victim.

4. On May 18, 2007, the reporting agent met with Assistant United States Attorney (AUSA) to review the "suspect" images contained on hard drive. After reviewing the images, AUSA indicated that while he believed the thumbnail images themselves did not constitute sufficient evidence to merit prosecution, any final decision regarding prosecution would have to be made by the Chief of the Criminal Division. Peter Jongbloed, Chief, Criminal Division, US Attorney's Office for the District of Connecticut, was briefed by the reporting agent and requested that DCIS interview prior to any final decision on the disposition of the case.

5. On June 21, 2007, the reporting agent interviewed admitted to playing on line games on his work computer for an average of three hours a day during his work day. He also admitted to accessing pornographic websites on his work computer during the work day, but denied ever downloading pornography on his work computer, and
denied ever intending to view or possess child pornography. [redacted] indicated that he also accessed pornography from his home computer, and over several years had downloaded approximately 5000 pornographic images on to a memory stick that he maintained at his home. When asked whether this memory stick contained images that would constitute child pornography, [redacted] stated that some of the images might “raise some eyebrows” and might be “questionable.”

6. On June 22, 2007, [redacted] voluntarily relinquished the memory stick and agreed to allow DCIS to search the memory stick for evidence of child pornography. Given the volume of forensic analysis already accomplished, and the amount required to complete this inquiry, the decision to open an investigation was made on June 25, 2007.

7. The 2701 files contained on the memory stick were run against the National Child Victim Identification Program (NCVIP), and none of the images was positively identified as a known child victim. A number of suspect images were identified that possibly depicted minors engaged in sexual posing and sexual acts. Analysis of the images indicated that the individuals were not pre-teen in age, but pubescent and developed females, some of whom might be teenagers.

8. On October 11, 2007, the US Attorney’s Office declined prosecution for possession of child pornography. The declination was based upon an inability to determine the age or identity of the individuals depicted in the files. [redacted] stated that he did not intend to possess child pornography, [redacted] cooperation in the investigation, and the number and nature of the vast majority of the images which were not child pornography.

9. On July 8, 2008 [redacted] completed a thirty day suspension imposed upon him by the Defense Contract Management Agency (DCMA). [redacted] suspension resulted from admissions he made to the reporting agent during an interview relating to his extensive misuse of government time and resources. DCMA [redacted] stated that she was attempting to recoup approximately $20,000.00 from [redacted] through the Defense Finance and Accounting Service (DFAS). This amount represents the dollar value of the time [redacted] spent computer gaming during the workday.

10. On November 17, 2008, DCMA [redacted] advised that she was unsuccessful in recouping funds from [redacted] through DFAS.

11. This case is closed. There were no management control deficiencies identified during the course of this investigation.
Identity of Subject

Name
DoB
SSN
Alias
Race
Sex
Employment/Occupation

Prepared by SA New Haven RA

APR: [redacted]
REPORT OF INVESTIGATION

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

DOD-RELATED CHILD PORNOGRAPHERS – NORTHERN LOS ANGELES

August 14, 2009

DISTRIBUTION

Western Field Office
ICE – Camarillo
ICE – Bakersfield
NARRATIVE

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

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

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

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

5. is the husband of a Navy E-5. was interviewed by SA about his alleged purchases of child pornography. At the conclusion of the interview,
determined that purchase was accidental and not indicative of criminal behavior. SA interview was reviewed by the USA’s office in Fresno, CA and prosecution against was declined.

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

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

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

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

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Alias</th>
<th>Social Security Number</th>
<th>Date of Birth</th>
<th>Place of Birth</th>
<th>Race</th>
<th>Sex</th>
<th>Height/Weight</th>
<th>Hair</th>
<th>Eyes</th>
<th>Residence</th>
<th>Employment</th>
<th>Occupation</th>
<th>Telephone Number Home</th>
<th>Telephone Number Bus</th>
<th>Drivers License Number/Issuing State</th>
<th>Dependents</th>
<th>Identifying Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Redacted]</td>
<td>[Redacted]</td>
<td>[Redacted]</td>
<td>[Redacted]</td>
<td>[Redacted]</td>
<td>[Redacted]</td>
<td>[Redacted]</td>
<td>[Redacted]</td>
<td>[Redacted]</td>
<td>[Redacted]</td>
<td>[Redacted]</td>
<td>[Redacted]</td>
<td>[Redacted]</td>
<td>[Redacted]</td>
<td>[Redacted]</td>
<td>[Redacted]</td>
<td>[Redacted]</td>
<td>[Redacted]</td>
</tr>
</tbody>
</table>
# Identity of Subjects

<table>
<thead>
<tr>
<th>Name</th>
<th>Christopher Lester Oswald</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>Chris Oswald</td>
</tr>
<tr>
<td>Social Security Number</td>
<td>(b)(6), (b)(7)(C)</td>
</tr>
<tr>
<td>Date of Birth</td>
<td></td>
</tr>
<tr>
<td>Place of Birth</td>
<td></td>
</tr>
<tr>
<td>Race</td>
<td></td>
</tr>
<tr>
<td>Sex</td>
<td></td>
</tr>
<tr>
<td>Height/Weight</td>
<td></td>
</tr>
<tr>
<td>Hair</td>
<td></td>
</tr>
<tr>
<td>Eyes</td>
<td></td>
</tr>
<tr>
<td>Residence</td>
<td></td>
</tr>
<tr>
<td>Employment</td>
<td>Unemployed</td>
</tr>
<tr>
<td>Occupation</td>
<td>Telecommunications Repair</td>
</tr>
<tr>
<td>Telephone Number Home</td>
<td>(b)(6), (b)(7)(C)</td>
</tr>
<tr>
<td>Telephone Number Bus</td>
<td></td>
</tr>
<tr>
<td>Drivers License Number/Issuing State</td>
<td></td>
</tr>
<tr>
<td>Dependents</td>
<td></td>
</tr>
<tr>
<td>Identifying Characteristics</td>
<td></td>
</tr>
</tbody>
</table>
### IDENTITY OF SUBJECTS

<table>
<thead>
<tr>
<th>Name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td></td>
</tr>
<tr>
<td>Social Security Number</td>
<td></td>
</tr>
<tr>
<td>Date of Birth</td>
<td></td>
</tr>
<tr>
<td>Place of Birth</td>
<td></td>
</tr>
<tr>
<td>Race</td>
<td></td>
</tr>
<tr>
<td>Sex</td>
<td></td>
</tr>
<tr>
<td>Height/Weight</td>
<td></td>
</tr>
<tr>
<td>Hair</td>
<td></td>
</tr>
<tr>
<td>Eyes</td>
<td></td>
</tr>
<tr>
<td>Residence</td>
<td></td>
</tr>
<tr>
<td>Employment</td>
<td></td>
</tr>
<tr>
<td>Occupation</td>
<td></td>
</tr>
<tr>
<td>Telephone Number Home</td>
<td></td>
</tr>
<tr>
<td>Telephone Number Bus</td>
<td></td>
</tr>
<tr>
<td>Drivers License Number/Issuing State</td>
<td></td>
</tr>
<tr>
<td>Dependents</td>
<td></td>
</tr>
<tr>
<td>Identifying Characteristics</td>
<td><a href="b">b</a>(7)(c)</td>
</tr>
</tbody>
</table>
IDENTITY OF SUBJECTS

<table>
<thead>
<tr>
<th>Name</th>
<th>[redacted]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>[redacted]</td>
</tr>
<tr>
<td>Social Security Number</td>
<td>[redacted]</td>
</tr>
<tr>
<td>Date of Birth</td>
<td>[redacted]</td>
</tr>
<tr>
<td>Place of Birth</td>
<td>[redacted]</td>
</tr>
<tr>
<td>Race</td>
<td>[redacted]</td>
</tr>
<tr>
<td>Sex</td>
<td>[redacted]</td>
</tr>
<tr>
<td>Height/Weight</td>
<td>[redacted]</td>
</tr>
<tr>
<td>Hair</td>
<td>[redacted]</td>
</tr>
<tr>
<td>Eyes</td>
<td>[redacted]</td>
</tr>
<tr>
<td>Residence</td>
<td>[redacted]</td>
</tr>
<tr>
<td>Employment</td>
<td>[redacted]</td>
</tr>
<tr>
<td>Occupation</td>
<td>[redacted]</td>
</tr>
<tr>
<td>Telephone Number Home</td>
<td>[redacted]</td>
</tr>
<tr>
<td>Telephone Number Bus</td>
<td>[redacted]</td>
</tr>
<tr>
<td>Drivers License Number/Issuing State</td>
<td>[redacted]</td>
</tr>
<tr>
<td>Dependents</td>
<td>[redacted]</td>
</tr>
<tr>
<td>Identifying Characteristics</td>
<td>[redacted]</td>
</tr>
</tbody>
</table>
# IDENTITY OF SUBJECTS

<table>
<thead>
<tr>
<th>Field</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>(b)(6), (b)(7)(C)</td>
</tr>
<tr>
<td>Alias</td>
<td></td>
</tr>
<tr>
<td>Social Security Number</td>
<td></td>
</tr>
<tr>
<td>Date of Birth</td>
<td></td>
</tr>
<tr>
<td>Place of Birth</td>
<td></td>
</tr>
<tr>
<td>Race</td>
<td></td>
</tr>
<tr>
<td>Sex</td>
<td></td>
</tr>
<tr>
<td>Height/Weight</td>
<td></td>
</tr>
<tr>
<td>Hair</td>
<td></td>
</tr>
<tr>
<td>Eyes</td>
<td></td>
</tr>
<tr>
<td>Residence</td>
<td></td>
</tr>
<tr>
<td>Employment</td>
<td></td>
</tr>
<tr>
<td>Occupation</td>
<td></td>
</tr>
<tr>
<td>Telephone Number Home</td>
<td></td>
</tr>
<tr>
<td>Telephone Number Bus</td>
<td></td>
</tr>
<tr>
<td>Drivers License Number/Issuing State</td>
<td></td>
</tr>
<tr>
<td>Dependents</td>
<td></td>
</tr>
<tr>
<td>Identifying Characteristics</td>
<td></td>
</tr>
<tr>
<td><strong>IDENTITY OF SUBJECTS</strong></td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>---</td>
</tr>
<tr>
<td>Name</td>
<td></td>
</tr>
<tr>
<td>Alias</td>
<td></td>
</tr>
<tr>
<td>Social Security Number</td>
<td></td>
</tr>
<tr>
<td>Date of Birth</td>
<td></td>
</tr>
<tr>
<td>Place of Birth</td>
<td></td>
</tr>
<tr>
<td>Race</td>
<td></td>
</tr>
<tr>
<td>Sex</td>
<td></td>
</tr>
<tr>
<td>Height/Weight</td>
<td></td>
</tr>
<tr>
<td>Hair</td>
<td></td>
</tr>
<tr>
<td>Eyes</td>
<td></td>
</tr>
<tr>
<td>Residence</td>
<td></td>
</tr>
<tr>
<td>Employment</td>
<td></td>
</tr>
<tr>
<td>Occupation</td>
<td></td>
</tr>
<tr>
<td>Telephone Number Home</td>
<td></td>
</tr>
<tr>
<td>Telephone Number Bus</td>
<td></td>
</tr>
<tr>
<td>Drivers License Number/Issuing State</td>
<td></td>
</tr>
<tr>
<td>Dependents</td>
<td></td>
</tr>
<tr>
<td>Identifying Characteristics</td>
<td>(b) (b) (N/Y X) (C)</td>
</tr>
</tbody>
</table>
## IDENTITY OF SUBJECTS

<table>
<thead>
<tr>
<th>Name</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social Security Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date of Birth</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Place of Birth</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Race</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sex</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Height/Weight</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hair</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Eyes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Residence</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Occupation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telephone Number Home</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telephone Number Bus</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Drivers License Number/Issuing State</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dependents</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identifying Characteristics</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
REPORT OF INVESTIGATION

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

FITZPATRICK, LELAND CHACE

November 24, 2009

DISTRIBUTION:

DCIS Headquarters, National Security Program (03NS)
NARRATIVE:

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

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

3. Leland Chace Fitzpatrick was identified as "[Redacted]."

4. On August 2, 2007, agents executed a search warrant on Fitzpatrick’s residence located at "[Redacted]." Subsequent to the execution of the search warrant, agents conducted a non-custodial interview of Fitzpatrick.

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

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

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

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

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Fitzpatrick, Leland Chace</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Security Number</td>
<td>(b)(6), (b)(7)(C)</td>
</tr>
<tr>
<td>Date/Place of Birth</td>
<td>Unknown</td>
</tr>
<tr>
<td>Race</td>
<td>Unknown</td>
</tr>
<tr>
<td>Sex</td>
<td>Unknown</td>
</tr>
<tr>
<td>Height</td>
<td>Unknown</td>
</tr>
<tr>
<td>Weight</td>
<td>Unknown</td>
</tr>
<tr>
<td>Hair</td>
<td>Unknown</td>
</tr>
<tr>
<td>Eyes</td>
<td>Unknown</td>
</tr>
<tr>
<td>Residence</td>
<td>Unknown</td>
</tr>
<tr>
<td>Employment/Occupation</td>
<td>Unknown</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>Unknown</td>
</tr>
<tr>
<td>Driver’s License Number</td>
<td>Unknown</td>
</tr>
<tr>
<td>and Issuing State</td>
<td>Unknown</td>
</tr>
<tr>
<td>Education</td>
<td>Unknown</td>
</tr>
</tbody>
</table>

---

**WARNING**

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

None.
REPORT OF INVESTIGATION

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

31-OCTOBER-2008

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

Distribution
DCIS Headquarters
Central Field Office
NARRATIVE

1. This project was initiated based upon information and a request from the DCIS Mid­Atlantic Field Office regarding information received from Project Flicker, an Immigration and Customs Enforcement (ICE) national undercover investigation into commercial child pornography websites.

2. Project Flicker identified over 5,000 individuals who subscribed to the commercial child pornography websites that were targeted by ICE. The names and identifying data on the individuals who subscribed to the commercial child pornography websites were checked against the Department of Defense (DoD) databases to identify those individuals who were associated with the DoD and subscribing to child pornography.

3. Child pornography is illegal and subscribers of commercial child pornography that are associated with the DoD put the DoD, the military and national security at risk by compromising computer systems, military installations and security clearances to name a few. Additionally, it puts the DoD at risk of blackmail, bribery, and threats, especially since these individuals typically have access to military installations.

4. This investigation developed sufficient information for three (3) Federal Search Warrants (subjects), one (1) criminal charge, and one (1) arrest.

5. As dictated by DCIS Headquarters, this project is canceled. Additionally, a conclusion about Management Control Deficiencies could not be made.
IDENTITY OF SUBJECTS

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

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

CLASSIFICATION:
FOR OFFICIAL USE ONLY

WARNING
IDENTITY OF SUBJECTS

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

Home Phone Number:
Driver's License Number:
Employment/Occupation:
IDENTITY OF SUBJECTS

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

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

(b)(6), (b)(7)(C)
IDENTITY OF SUBJECTS

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

Home Phone Number: 
Driver's License Number: 
Employment/Occupation: 
IDENTITY OF SUBJECTS

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

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

(b)(6),(b)(7)(C)
IDENTITY OF SUBJECTS

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

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

[Redacted]
IDENTITY OF SUBJECTS

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

(b)(e)(b)(7)(C)
IDENTITY OF SUBJECTS

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

Home Phone Number: [Redacted]
Driver's License Number: [Redacted]
Employment/Occupation: [Redacted]
IDENTITY OF SUBJECTS

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

Home Phone Number:
Driver's License Number:
Employment/Occupation:
IDENTITY OF SUBJECTS

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

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

Prepared by SA[Redacted] Dayton RA 
APPR. [Redacted]
REPORT OF INVESTIGATION

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

STOKES, CHRISTOPHER MICHAEL

February 10, 2009

DISTRIBUTION

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

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

2. Evidence collected during the course of this investigation revealed that on October 11, 2006 and again on December 29, 2006, Stokes

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

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

5. On April 11, 2008, AUSA Norfolk Division, Criminal Section, filed a Criminal Information with the U.S. District Court, EDVA, Norfolk, VA, which charged Stokes with Possession of Material Containing Child Pornography (Title 18, U.S. Code, Section
2252(a)(5)(B)) and Criminal Forfeiture (Title 18, U.S. Code, Section 2253).

6. On May 20, 2008, Stokes pled guilty in U.S. District Court, EDVA, Norfolk to the single count Criminal Information filed on April 11, 2008, charging him with Possession of Material Containing Child Pornography. As part of his guilty plea, Stokes agreed to forfeit assorted computer equipment and digital media which contained and facilitated the viewing of child pornography.

7. On October 24, 2008, pursuant to his guilty plea, Stokes was sentenced by Senior United States District Judge Henry Coke Morgan, Jr. in U.S. District Court, EDVA, Norfolk to 60 months confinement and lifetime supervised release. In addition, Stokes was ordered to immediately pay $12,500 in fines, as a $100 Special Assessment had already been paid to the court. Additional rules were established concerning Stokes' supervised release, which are to be monitored by his Probation Officer upon his release from confinement. Stokes was allowed to remain on bond pending notification of his assignment to a federal penitentiary.

8. On January 12, 2009, the Final Order of Forfeiture was signed by Senior United States District Judge Henry Coke Morgan, Jr., and filed in the U.S. District Court, EDVA, Norfolk.

9. All investigative and judicial actions have been completed. No fraud vulnerabilities were uncovered during the course of this investigation.

10. This investigation is now closed as finished.
# IDENTITY OF SUBJECTS

<table>
<thead>
<tr>
<th>Name</th>
<th>Christopher Michael Stokes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>[Redacted]</td>
</tr>
<tr>
<td>Social Security Number</td>
<td>[Redacted]</td>
</tr>
<tr>
<td>Date/Place of Birth</td>
<td>[Redacted]</td>
</tr>
<tr>
<td>Race</td>
<td>[Redacted]</td>
</tr>
<tr>
<td>Sex</td>
<td>[Redacted]</td>
</tr>
<tr>
<td>Height</td>
<td>[Redacted]</td>
</tr>
<tr>
<td>Weight</td>
<td>[Redacted]</td>
</tr>
<tr>
<td>Hair</td>
<td>[Redacted]</td>
</tr>
<tr>
<td>Eyes</td>
<td>[Redacted]</td>
</tr>
<tr>
<td>Residence</td>
<td>[Redacted]</td>
</tr>
<tr>
<td>Employment/Occupation</td>
<td>[Redacted]</td>
</tr>
<tr>
<td>Driver’s License Number and Issuing State</td>
<td>[Redacted]</td>
</tr>
<tr>
<td>Education</td>
<td>[Redacted]</td>
</tr>
</tbody>
</table>

Prepared by Special Agent [Redacted] Norfolk RA

APPR: [Redacted]
REPORT OF INVESTIGATION

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

November 30, 2009

DISTRIBUTION:

DCIS Headquarters, National Security Program (03NS)
NARRATIVE:

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

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

3. [Redacted] was identified as an employee of Audio Video Systems, Incorporated, a DoD contractor.

4. On August 15, 2007, agents executed a search warrant on [Redacted] residence located at [Redacted]. Subsequent to the execution of the search warrant, agents conducted a non-custodial interview of [Redacted] admitted to subscribing to approximately five websites that offered child pornography images. [Redacted] stated he was looking for images of high school age girls. [Redacted] admitted to viewing pornographic images of individuals under age 18. [Redacted] stated he knew it was wrong.

5. Due to a lack of resources, this case will be closed. ICE, as the lead investigative agency, will be responsible for the final adjudication of this matter. No management control deficiencies were identified during this investigation.
IDENTIFY OF SUBJECTS:

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

Employment/Occupation:
Telephone Number:
Driver's License Number:
and Issuing State:
Education:

Unknown
Unknown
Unknown
Unknown
Unknown
EXHIBITS:

None.
NARRATIVE:

1. This case was initiated based on information derived from DCIS Project: Operation Flicker (Case Control Number 200701199X). The project identified a former U.S. Navy reservist (E-05), as an individual who downloaded child pornography.

2. As background, Immigration and Customs Enforcement (ICE) initiated an investigation into a criminal organization operating a commercial child pornography website known as “Home Collection.” The investigation revealed “Home Collection” was operating numerous commercial child pornography websites. In addition, the organization utilized various PayPal accounts to process the payments for access to the member-restricted websites. Assistant United States Attorney (AUSA) Gerald Smagala, Eastern District of Virginia, requested DCIS assist in identifying individuals affiliated with the DoD and provide investigative assistance. In response, the DCIS Arlington Resident Agency (RA) initiated Operation Flicker.

3. The criminal organization utilized a specific and identifiable payment website known as “iWest.” The information developed during the course of the investigation identified that the organization (1) used various PayPal accounts to facilitate the customer payments; (2) used specific subject identifiers within the PayPal accounts to identify purchases of subscriptions to various member restricted websites; and (3) used specific administrative e-mail accounts that were used to distribute access to the member restricted websites.

4. DCIS Arlington RA, utilized information contained within the DoD Employee Interactive Data System and the Joint Personnel Adjudication Systems (JPAS) to identify DoD personnel and contract employees who joined the member restricted sites. Among those identified was.

5. On August 29, 2007, DCIS and ICE executed a search warrant based on evidence resided there. Upon entry, it was determined no longer resided there. The occupants related continued to receive mail at that address. It was later determined new address was.

6. On August 29, 2007, interviewed owner of the property at Drive for over a year. During his occupancy, had three roommates moved out of on February 1, 2007, informed he was moving to find cheaper rent. believed was a at Fair Oaks Mall, Fairfax, VA.

7. On August 29, 2007, Information Control Officer, Virginia Employment Commission, provided SA employed contacted in Fair Oaks Mall and
was informed no longer worked there. Instead, he was employed at Tyson’s Corner Center Mall, McLean, VA.

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

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


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

11. On July 23, 2008, DCIS Arlington RA, reviewed the images NCMEC identified and concluded all images were found in “free space.” On October 20, 2008, SA Carson completed a final media analysis that concluded all images were carved from “free space.”

12. On June 28, 2008, analyzed Internet search logs and visited each website. Although many websites advertised teen and child models, no websites advertised child pornography.

13. On July 28, 2008, AUSA Smagala declined prosecution on the matter. AUSA Smagala advised he did not intend to prosecute because the images NCMEC identified were in “free space.” AUSA Smagala explained items in “free space” do not constitute possession.

14. No judicial or administrative action will occur. No fraud vulnerabilities were identified during this investigation. DCIS will take no further action on this matter. The investigation is closed as “declined.”
IDENTITY OF SUBJECTS:

<table>
<thead>
<tr>
<th>Name</th>
<th>:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>:</td>
</tr>
<tr>
<td>Social Security Number</td>
<td>:</td>
</tr>
<tr>
<td>Date/Place of Birth</td>
<td>:</td>
</tr>
<tr>
<td>Race</td>
<td>:</td>
</tr>
<tr>
<td>Sex</td>
<td>:</td>
</tr>
<tr>
<td>Height</td>
<td>:</td>
</tr>
<tr>
<td>Weight</td>
<td>:</td>
</tr>
<tr>
<td>Hair</td>
<td>:</td>
</tr>
<tr>
<td>Eyes</td>
<td>:</td>
</tr>
<tr>
<td>Residence</td>
<td>:</td>
</tr>
<tr>
<td>Employment/Occupation</td>
<td>:</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>:</td>
</tr>
<tr>
<td>Driver's License Number</td>
<td>:</td>
</tr>
<tr>
<td>and Issuing State</td>
<td>:</td>
</tr>
<tr>
<td>Education</td>
<td>:</td>
</tr>
</tbody>
</table>
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

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

December, 09 2009

DISTRIBUTION:

DCIS Headquarters, National Security Program (03NS)

B-1
NARRATIVE:

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

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

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

4. On July 22, 2009, was contacted by who reported had permanently relocated to a NRO facility in New Mexico and was currently residing at .

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

<table>
<thead>
<tr>
<th>Name</th>
<th>:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>:</td>
</tr>
<tr>
<td>Social Security Number</td>
<td>:</td>
</tr>
<tr>
<td>Date/Place of Birth</td>
<td>:</td>
</tr>
<tr>
<td>Race</td>
<td>:</td>
</tr>
<tr>
<td>Sex</td>
<td>:</td>
</tr>
<tr>
<td>Residence</td>
<td>:</td>
</tr>
<tr>
<td>Employment/Occupation</td>
<td>:</td>
</tr>
</tbody>
</table>
REPORT OF INVESTIGATION

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

LEDFORD, KRIS ALLEN

April 9, 2009

DISTRIBUTION:
NARRATIVE

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

5. On September 2, 2008, the RA obtained a copy Ledford’s military personnel file from National Personnel Records Center.
6. On September 16, 2008 the reporting agent interviewed [redacted] who was the former [redacted] 1st Battalion, 36th Infantry Regiment. [redacted] stated he was the [redacted] 1st Battalion, 36th Infantry Regiment, during which time Ledford was assigned to the unit. [redacted] stated he remembered deploying to Bosnia with Ledford being assigned to this unit. [redacted] stated Ledford did not receive a Bronze Star or Purple Heart for action during the deployment. [redacted] specifically recalls Ledford due to [redacted].

7. On October 1, 2008, the RA obtained records from the U.S. Department of Veteran Affairs concerning Kris A. Ledford. [redacted]

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


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

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Kris Allen Ledford</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>None</td>
</tr>
<tr>
<td>Social Security Number</td>
<td>[Redacted]</td>
</tr>
<tr>
<td>Date/Place of Birth</td>
<td>April 9, 2009</td>
</tr>
<tr>
<td>Race</td>
<td>[Redacted]</td>
</tr>
<tr>
<td>Sex</td>
<td>[Redacted]</td>
</tr>
<tr>
<td>Residence</td>
<td>[Redacted]</td>
</tr>
<tr>
<td>Employment/Occupation</td>
<td>Police Officer</td>
</tr>
<tr>
<td></td>
<td>Muskogee Police Department</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>[Redacted]</td>
</tr>
<tr>
<td>Education</td>
<td>[Redacted]</td>
</tr>
</tbody>
</table>
REPORT OF INVESTIGATION

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

DEMOULIN, STANLEY P.
Odenton, MD

October 21, 2008

DISTRIBUTION

DCIS Headquarters (03SO)
NSA-OIG (S (b)(6)(c))
ICE-Baltimore (S (b)(6)(c))
NARRATIVE

1. This investigation was initiated based upon information derived from a DCIS Project, Operation Flicker, Case Control Number 200701199X. As background, on May 29, 2007, DCIS initiated Operation Flicker based on information provided by Assistant United States Attorney (AUSA) Gerald Smagala, United States Attorney's Office, Eastern District of Virginia, Alexandria Division. AUSA Smagala advised that Immigration and Customs Enforcement (ICE) was conducting a national investigation that identified over 5,000 individuals who subscribed to predicated child pornography websites. AUSA Smagala specifically requested that DCIS assist in identifying DoD affiliated individuals and provide investigative assistance. The reporting agent utilized information contained within the DoD Employee Interactive Data System and the Joint Personnel Adjudication Systems (JPAS to identify DoD affiliated individuals. Among those identified was Stanley P. Demoulin, a DoD contractor employee at the National Security Agency. A query of JPAS revealed that Demoulin made approximately four purchases of alleged pornographic material depicting children. Exhibit 1 is a copy of the DCIS Form 1, "Case Initiation", dated October 3, 2007.

2. On October 17, 2007, a search warrant was executed on DeMoulin's residence in Odenton, MD. Numerous computer-related and other items were seized from the residence. Exhibit 2 is a copy of the DCIS Form 1, "Significant Incident Report/Search Warrant", dated October 22, 2007.

3. Analysis of DeMoulin’s computer files indicated evidence of child pornography. After negotiations with DeMoulin and his attorney, on April 15, 2008, DeMoulin agreed to plead guilty to a Criminal Information charging him with Receipt of Child Pornography, Title 18 USC §2252A(a)(2)(A) & Title 18 USC §2256. Exhibit 3 is a copy of the DCIS Form 1, "Plea Agreement", dated May 29, 2008, and Exhibit 4 is a copy of the DCIS Form 1, "Criminal Information", dated May 29, 2008.

4. On July 11, 2008, DeMoulin pleaded guilty in U.S. District Court, Baltimore, MD, to violating one count of Receipt of Child Pornography, Title 18 USC §2252A(a)(2)(A) & Title 18 USC §2256. On August 28, 2008, DeMoulin was sentenced to 63 months in prison, a $100 assessment, sentenced to lifetime probation, and ordered to register as a sexual offender upon release from prison. Exhibit 5 is a copy of the DCIS Form 1, "Guilty Plea", dated July 11, 2008, and Exhibit 6 is a copy of the DCIS Form 1, "Sentencing", dated August 28, 2008.

5. No fraud vulnerability reports were completed during the course of this investigation. All investigative effort is now complete. This investigation is closed as “finished” with the submission of this report.
<table>
<thead>
<tr>
<th>Name</th>
<th>Stanley P. DeMoulin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td></td>
</tr>
<tr>
<td>Social Security Number</td>
<td>&lt;redacted&gt;</td>
</tr>
<tr>
<td>Date/Place of Birth</td>
<td></td>
</tr>
<tr>
<td>Race</td>
<td></td>
</tr>
<tr>
<td>Sex</td>
<td></td>
</tr>
<tr>
<td>Height</td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td></td>
</tr>
<tr>
<td>Hair</td>
<td></td>
</tr>
<tr>
<td>Eyes</td>
<td></td>
</tr>
<tr>
<td>Residence</td>
<td></td>
</tr>
<tr>
<td>Employment/Occupation</td>
<td></td>
</tr>
<tr>
<td>Telephone Number</td>
<td>Home: UNKNOWN</td>
</tr>
<tr>
<td></td>
<td>Office: UNKNOWN</td>
</tr>
<tr>
<td></td>
<td>[If appropriate] Cell: UNKNOWN</td>
</tr>
<tr>
<td>Driver’s License Number and Issuing State</td>
<td>UNKNOWN</td>
</tr>
<tr>
<td>Education</td>
<td>UNKNOWN</td>
</tr>
</tbody>
</table>

IDENTIFYING DATA
EXHIBITS


3 - DCIS Form 1, "Plea Agreement", dated May 29, 2008.

4 - DCIS Form 1, "Criminal Information", dated May 29, 2008.

5 - DCIS Form 1, "Guilty Plea", dated July 11, 2008.

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

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

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

C-1
On April 23, 2009, ICE and DCIS Criminal Investigative Service executed a search warrant at the personal residence of CbJe.cbx 7 7 (c). One computer was seized during the execution of the search warrant. During the forensic examination of the computer, approximately five thumbnail images were discovered from the Thumbs.db file of the media player. These images appeared to be the initial frame of deleted video files, which depicted the sexual abuse of minor children.

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

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

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

Attachment:
REPORT OF INVESTIGATION

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

February 4, 2005

DISTRIBUTION:
DCIS Headquarters, National Security Program (03NS)
DARPA (03NS,防务高级研究计划局)

CLASSIFICATION: OFFICIAL USE ONLY

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

1. This investigation was initiated based upon information received from Security and Intelligence Directorate, Defense Advanced Research Projects Agency (DARPA), Arlington, VA, concerning possible possession of child pornography by Program Manager, DARPA, Arlington, VA.

2. A contractor from DARPA’s Information Technology Division, Arlington, VA, discovered what appeared to be child pornography.

3. On June 24, 2003, who is the was interviewed by Special Agent (SA) Defense Criminal Investigative Service (DCIS), Mid-Atlantic Field Office (MAFO), and advised that on June 23, 2003, he was approached by a network engineer, who stated that he had found a large amount of pornography on computer during the process of reviewing the file system for a virus that had been reported by the network virus scanning software. called immediate supervisor, who came over to examine the images. While and were showing the images to they discovered images that appeared to be child pornography. and then directed to copy the portions of the file system from hard drive that contained the pornography. provided DCIS with a series of CD-ROMs containing the pornography copied from computer.

4. On July 15, 2003, SA DCIS-MAFO, began an analysis of the images provided by DARPA. Images that contained potential child pornography were identified and provided to the National Center for Missing and Exploited Children (NCMEC) to determine whether the individuals contained in the images could be identified as known victims. Routinely, in order to criminally prosecute child pornography cases through the Federal system, individuals in the images must be identified as known victims.

5. On October 31, 2003, the NCMEC reported that no known victims were found in the images provided for their review.

6. On November 3, 2003, Assistant United States Attorney (AUSA) U.S. Attorney’s Office, Eastern District of Virginia, Alexandria, VA, declined to criminally prosecute this matter given that there were no images of known victims.
7. On December 15, 2003, Criminal Investigator, Computer Crime Unit, Office of the Attorney General, Commonwealth of Virginia, Richmond, VA, was contacted and provided with a copy of the DCIS-MAFO media analysis report. [Redacted] stated that under Virginia statutes [Redacted] could be prosecuted by the Commonwealth under § 18.2-374.1:1, Possession of Child Pornography; which would be a class 5 felony. Virginia statute does not require that the individuals in the images be identified as known victims. [Redacted] stated his office would open an investigation and contact a Commonwealth’s Attorney to prosecute this matter.

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

9. On April 7, 2004, the media received from [Redacted] were provided to the Defense Computer Forensics Lab (DCFL) for analysis.

10. On September 22, 2004, the DCFL completed their analysis of the material received from [Redacted] A review of the report revealed a large amount of pornographic material that might meet the definition of child pornography. A copy of the DCFL report was provided to [Redacted] [Redacted]

11. This Report of Investigation is being provided to DARPA for information purposes and action as deemed appropriate. Should administrative action be taken, it is requested that [Redacted] be notified. [Redacted] can be contacted at [Redacted] or at the electronic mail address [Redacted].

12. Possible images of child pornography and other pornographic images obtained during the course of this investigation cannot be appended to this report due to their graphic nature and, in regards to the possible images of child pornography, their classification as contraband. Should additional information about the images be needed, please contact [Redacted].

13. Based on information obtained to date, the DCIS-MAFO will continue to work with the Commonwealth of Virginia in seeking possible criminal prosecution of [Redacted].

IDENTITY OF SUBJECTS:
IDENTIFYING DATA

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

Defense Advanced Research Projects Agency
Arlington, VA

EXHIBITS:

CLASSIFICATION:

WARNING
This document is the property of the Department of Defense Inspector General and is on loan to your agency. Contents may not be disclosed to any party under investigation nor may this document be distributed outside the receiving agency without the specific authorization of the Deputy Inspector General for Investigations.
1. DCIS Form 1 - Interview
2. Written Statement

Prepared by SA Mid-Atlantic Field Office

C-1
REPORT OF INVESTIGATION

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

March 17, 2009

DISTRIBUTION:

DCIS Headquarters, National Security Program (03NS)
Pentagon Force Protection Agency

CLASSIFICATION:

FOR OFFICIAL USE ONLY

LAW ENFORCEMENT SENSITIVE

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

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

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

3. created a “SQUID User Access Report” which captured every instance of internet access. provided the E-Policy report and the Squid report to Alex Benton, Network Security Manager, Dyncorp.

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

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

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

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

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

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

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

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

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

December 7, 2009

RONALD RICHARD SHANKEY, SSN: (b)(5)

ROBERT A MACCINI, SSN: (b)(5)

STEPHEN H. MCCONNAUGHAY, SSN: (b)(5)

RONALD E. ELMQUIST, SSN: (b)(5)

DISTRIBUTION

DCISHQ (03NS)

Central Field Office (40FO)
NARRATIVE

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

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

3. The FBI – Eau Claire developed information that child pornography was being stored at the Shankey residence. A search warrant was obtained and executed on September 7, 2006 which yielded numerous items of child pornography. On October 4, 2006, a grand jury for the Western District of Wisconsin, Madison, Wisconsin returned a two-count indictment with distributing a visual depiction of minors engaging in sexually explicit conduct, and possessing a computer hard drive containing such visual depictions.
4. On May 15, 2007, District Judge John C. Shabaz, for the Western District of Wisconsin, Madison, Wisconsin sentenced Shankey on one count of violating Title 18, United States Code Section 2252(a)(4)(B), Possession of Child Pornography; a Class C felony, a second count of distribution of child pornography was dismissed. Shankey was sentenced to a period of imprisonment of 108 months, followed by supervised release for life and to register as a sex offender. Additionally, he was required to pay a $100 criminal assessment.

5. Maccini was titled as a subject on December 5, 2006 in cooperation with the Massachusetts State Police. Maccini was indicted on December 20, 2006 on child pornography charges, including distribution based upon information provided by the DCIS Minneapolis Post of Duty. Maccini was sentenced on December 12, 2007 to 5 years probation in Massachusetts state court.

6. The Illinois Attorney General’s office has requested assistance for an e-mail associate of Shankey's going by the name _______. Information related to distribution of child pornography by this e-mail account was provided. On February 21, 2008, McConnaughay, aka. _______ was charged in Illinois with possession and dissemination of child pornography, class 3 and class 1 felony respectively. On May 29, 2009, McConnaughay was sentenced in McHenry County Illinois pursuant to a plea agreement on a Class 3 felony charge of possession of child pornography. He is to serve 4 months incarceration, 2 years probation, pay a $1,00 fine and register as a sex offender.

7. The FBI, Kansas City requested assistance with another associate of Shankey’s using the screen name _______. Information was retrieved from Shankey’s computer showing 13 messages between Shankey and _______. This information was provided to assist in their prosecution. AUSA Roseann Ketchmark, Western District of Missouri advised that on July 10, 2009, Ronald Elmquist _______ pled guilty to attempted possession of child pornography in violation of Title 18, United States Code Section 2252 (A)(4)(B) and (B)(2). On October 30, 2009, Elmquist was sentenced to 30 months incarceration, 5 yrs supervised release, 120 hours of community service, 12 months of home detention, participate in sex offender counseling, register under the Sex Offender registration and Notification Act, a $150,000 fine, and $100 special assessment.

8. All known subjects associated with this case have been sentenced. This case is therefore being closed as completed. Any evidence will be disposed of in accordance with DCIS policy.
EXHIBITS – Previously submitted.
REPORT OF INVESTIGATION

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

SWEENEY, DANIEL JOSEPH

DISTRIBUTION:

Defense Criminal Investigative Service Headquarters, National Security Program (03NS)
Immigration and Customs Enforcement, SAC Washington, D.C. (SAC WDC-WDC)
NARRATIVE:

1. On May 29, 2007, the DCIS, Arlington Resident Agency, initiated Project: Operation Flicker (CCN: 2007011199X) based on information provided by Assistant U.S. Attorney (AUSA) Gerald Smagala, U.S. Attorney’s Office (USAO), Eastern District of Virginia (EDVA), Alexandria Division. AUSA Smagala advised that the ICE was conducting a national investigation that identified over 5,000 individuals who subscribed to predatory child pornography websites. AUSA Smagala specifically requested DCIS assistance relative to any identified DoD personnel.

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

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

4. Information derived from Operation Flicker revealed that Sweeney, during a non-custodial interview of Sweeney, he stated that he was active duty U.S. Navy, E-6 and worked at the Navy Yard in Washington, D.C.

5. On June 21, 2007, a search warrant was executed on Sweeney’s residence located at...

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

7. During the search warrant, agents seized two laptop computers, one external hard disk drive, one thumb drive, two memory cards, and approximately 77 other media items from the...
residence. Computer forensics revealed child pornography on one of the laptop computers belonging to Sweeney.

9. The recovered images were submitted to the National Center for Missing and Exploited Children (NCMEC) in Alexandria, Virginia. The NCMEC reported that images recovered from Sweeney's residence included children previously identified by law enforcement as victims of sexual abuse.

10. On October 7, 2008, a warrant was issued for the arrest of Sweeney by the U.S. District Court (USDC), EDVA. On October 8, 2008, agents executed an arrest warrant on Sweeney in Norfolk, Virginia, where he was station aboard the U.S.S. Anzio.

11. On October 23, 2008, Sweeney was indicted in the Eastern District of Virginia on two counts of attempted receipt of child pornography and possession of child pornography, a violation of Title 18, U.S. Code (USC), Sections 2252A(a)(2) and 2252A(a)(5)(B).

13. On December 12, 2008, Sweeney appeared before the Honorable James C. Cacheris, District Judge, USDC, EDVA, Alexandria Division. Sweeney pled guilty to a single count of possession of child pornography, a violation of Title 18, USC, Section 2252A.

14. On March 13, 2009, Sweeney was sentenced to 41 months incarceration, 240 months supervised release, and a $100 penalty, for the possession of child pornography, a violation of Title 18, USC, Section 2252A.

15. No further criminal, civil or administrative activity by the DCIS will occur. This case is closed as “finished.”
**IDENTITY OF SUBJECTS:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Sweeney, Daniel Joseph</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>None</td>
</tr>
<tr>
<td>Social Security Number</td>
<td>(b)(6)(b)(7)(C)</td>
</tr>
<tr>
<td>Date/Place of Birth</td>
<td></td>
</tr>
<tr>
<td>Race</td>
<td></td>
</tr>
<tr>
<td>Sex</td>
<td></td>
</tr>
<tr>
<td>Height</td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td></td>
</tr>
<tr>
<td>Hair</td>
<td></td>
</tr>
<tr>
<td>Eyes</td>
<td></td>
</tr>
<tr>
<td>Residence</td>
<td></td>
</tr>
<tr>
<td>Employment/Occupation</td>
<td>Petty Officer Second Class (E-5), U.S. Navy</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>Unknown</td>
</tr>
<tr>
<td>Driver's License Number and Issuing State</td>
<td>Unknown</td>
</tr>
<tr>
<td>Education</td>
<td>Unknown</td>
</tr>
</tbody>
</table>

Prepared by Special Agent [Illegible] Arlington Resident Agency  APPR: [Illegible]

**WARNING**

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

B-1
REPORT OF INVESTIGATION

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

CAMPBELL, CAMERON MORRISON

November 23, 2009

DISTRIBUTION:

DCIS Headquarters, National Security Program (03NS)
NARRATIVE:

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

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

3. Cameron Morrison Campbell was identified as

4. On June 28, 2007, agents executed a search warrant on Campbell’s residence located at Subsequent to the execution of the search warrant, agents conducted a non-custodial interview of Campbell.

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

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

7. On November 20, 2009, Campbell appeared before the Honorable Gerald Bruce Lee, District Judge, U.S. District Court, Eastern District of Virginia, Alexandria, Virginia and was sentenced to 60 months in prison, 60 months supervised released, and a $100 penalty assessment.
<table>
<thead>
<tr>
<th>Identify of Subjects:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td></td>
</tr>
<tr>
<td>Alias</td>
<td></td>
</tr>
<tr>
<td>Social Security Number</td>
<td></td>
</tr>
<tr>
<td>Date/Place of Birth</td>
<td></td>
</tr>
<tr>
<td>Race</td>
<td></td>
</tr>
<tr>
<td>Sex</td>
<td></td>
</tr>
<tr>
<td>Height</td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td></td>
</tr>
<tr>
<td>Hair</td>
<td></td>
</tr>
<tr>
<td>Eyes</td>
<td></td>
</tr>
<tr>
<td>Residence</td>
<td></td>
</tr>
<tr>
<td>Employment/Occupation</td>
<td></td>
</tr>
<tr>
<td>Telephone Number</td>
<td>Unknown</td>
</tr>
<tr>
<td>Driver's License Number</td>
<td>Unknown</td>
</tr>
<tr>
<td>and Issuing State</td>
<td>Unknown</td>
</tr>
<tr>
<td>Education</td>
<td>Unknown</td>
</tr>
</tbody>
</table>

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

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

JONES, PAUL BURNELL

August 26, 2008
NARRATIVE

1. This investigation was initiated based on information derived from DCIS Project: Operation Flicker (Case Control Number 200701199X). Flicker was initiated based upon a national ICE investigation which identified over 5,000 individuals who subscribed to predicated child pornography websites. DCIS was requested to assist in the identification and investigation of DoD affiliated individuals.

2. DCIS, utilizing information contained within the DoD Employee Interactive Data System and the Joint Personnel Adjudication Systems (JPAS) to identify DoD employees who subscribed to the websites. Among those identified was Paul Burnell Jones, a Contract Specialist with the

3. Based on information obtained from ICE regarding Jones' subscriptions to known child pornography sites, agents from DCIS and ICE executed a search warrant on Jones' residence on July 25, 2007. Jones' residence was located at In addition a warrant was executed at Jones' office located at

4. Simultaneous to the executions of the search warrants, DCIS, and ICE, conducted a non-custodial interview of Jones. Jones admitted to further provided he regularly accessed child pornography from home. After establishing probable cause, Jones was arrested.

5. On July 25, 2007, a search warrant was executed on the home of

6. On October 11, 2007, Jones pled guilty to one count of Attempted Receipt of Child Pornography, a violation of Title 18 U.S.C 2252A(b)(1).

7. On January 11, 2008, Jones was sentenced to 60 months in prison and 120 months supervised release. Jones was also fined $2,000 in restitution and a $100 special assessment fee.

8. No fraud vulnerabilities were discovered during the course of this investigation. No further criminal, civil or administrative actions will be taken on this matter. The case is closed as "finished."
<table>
<thead>
<tr>
<th><strong>IDENTITY OF SUBJECTS</strong></th>
<th><strong>IDENTIFYING DATA</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Paul Burnell Jones</td>
</tr>
<tr>
<td>Alias</td>
<td>(b)(6),(b)(7)(C)</td>
</tr>
<tr>
<td>Social Security Number</td>
<td></td>
</tr>
<tr>
<td>Date/Place of Birth</td>
<td></td>
</tr>
<tr>
<td>Race</td>
<td></td>
</tr>
<tr>
<td>Sex</td>
<td></td>
</tr>
<tr>
<td>Height</td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td></td>
</tr>
<tr>
<td>Hair</td>
<td></td>
</tr>
<tr>
<td>Eyes</td>
<td></td>
</tr>
<tr>
<td>Residence</td>
<td></td>
</tr>
<tr>
<td>Employment/Occupation</td>
<td></td>
</tr>
<tr>
<td>Telephone Number</td>
<td></td>
</tr>
<tr>
<td>Driver’s License Number</td>
<td></td>
</tr>
<tr>
<td>and Issuing State</td>
<td></td>
</tr>
<tr>
<td>Education</td>
<td></td>
</tr>
</tbody>
</table>

Prepared by: SA Arlington Resident Agency

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

CLASSIFICATION: FOR OFFICIAL USE ONLY LAW ENFORCEMENT SENSITIVE
DEPARTMENT OF DEFENSE
OFFICE OF INSPECTOR GENERAL
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
ARLINGTON RESIDENT AGENCY
201 12TH STREET SOUTH, SUITE 712
ARLINGTON, VIRGINIA 22202-5408

REPORT OF INVESTIGATION

2007014031-09-JUL-2007-60DC-W1/D

April 29, 2009

DISTRIBUTION:

DCIS Headquarters, National Security Program (03NS)
Immigration and Customs Enforcement, SAC Washington, D.C.
NARRATIVE:

1. This case was initiated based on information derived from Defense Criminal Investigative Service (DCIS) Project: Operation Flicker (Case Control Number 200701199X). As background, on May 29, 2007, the DCIS, Mid-Atlantic Field Office (MAFO), initiated Operation Flicker based on information provided by Assistant United States Attorney (AUSA) Gerald Smagala, United States Attorney’s Office (USAO), Eastern District of Virginia, Alexandria Division. AUSA Smagala advised that the Immigration and Customs Enforcement (ICE) was conducting a national investigation that had identified over 5,000 individuals who subscribed to predicated child pornography websites. AUSA Smagala specifically requested that DCIS assist in identifying Department of Defense (DoD) affiliated individuals and provide investigative assistance.

2. SAl<bJ(e)J(S)J(C) 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 a civilian with an unknown DoD agency. A query of JPAS revealed that he was a civilian contract employee within the Office of the Secretary of Defense, and held a top secret clearance. Law enforcement database checks were conducted and no criminal history was located. A check of the Defense Central Index of Investigations (DCII) revealed one record for A. A query of the Investigative Data System revealed no open or closed investigations of SA(b)(B)(b)(J(c).

3. On July 10, 2007, SAl(b)(B)(b) and SA(J(c) met with (b)(B)(b) immediate supervisor to obtain work computer and advised a subpoena or search warrant was required for him to release the computer and that he would safeguard the computer in the interim.

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

5. On November 29, 2007, SAl(b)(B)(b) served a search warrant via facsimile to the . The search warrant was issued from the U.S. District Court, Eastern District of Virginia, Alexandria Division, by the Honorable Barry R. Portez, U.S. Magistrate Judge. The search warrant requested electronic mail.
(e-mail) subscriber information and e-mails sent and received from E-mail account.

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

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

8. On February 4, 2008, AUSA Smagala requested that the forensic examination of the home computer be completed by

9. On May 19, 2008, AUSA contacted and he verified that a search warrant was not needed to obtain work laptop computer.

10. On September 9, 2008, AUSA met with and obtained the original hard drive of the work laptop computer that was issued to also provided a forensic report on work laptop computer.

11. On September 15, 2008, AUSA reviewed the forensic report regarding work laptop and the results indicated there was no evidence of child pornography on work laptop computer.

12. On September 20, 2008, AUSA contacted ICE, and she requested all electronic media obtained from the residence search warrant be transferred back to ICE.

13. On September 25, 2008, AUSA returned all electronic media obtained from the residence search warrant to then forwarded all electronic media to for forensic analysis.

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

15. On March 26, 2009, AUSA met with and returned confiscated work laptop hard drive back to Lockheed Martin and stated he will update regarding AUSA Smagala’s decision not to prosecute.
16. A review of personal email and the results of the computer forensic reports of personal and work computers did not reveal evidence related to the receipt of child pornography. AUSA Smagala declined to criminally prosecute for violations relating to possession and/or receipt of child pornography, due to insufficient evidence. DCIS will take no further criminal, civil, or administrative actions on this matter. This case is closed as “declined.”
IDENTITY OF SUBJECTS:

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

[Redacted Information]
EXHIBIT: