CLASSIFIED

Exhibit(s) 94

Page(s) 000665 thru 000665a referred to:

Commander
INSCOM
ATTN: IAMG-C-FOIA
4552 Pike Road
Fort Meade, MD 20755-5995

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER 0028-10-CID221-10117

DETAILS

About 1010, 14 Jul 10, SA (b)(6)(b)(7)(C) coordinated with Ms. (b)(6)(b)(7)(C) Chief Executive Officer, IC Group, 1100 Vine St., Suite C8, Philadelphia, PA 19107, in regards to the Department of Defense, Office of Inspector General (DOD/IG) Subpoena 2010251-10468, issued for the records related to the account (b)(6)(b)(7)(C)@pobox.com.

Ms. (b)(6)(b)(7)(C) provided the following information regarding the account.

The account in question was registered to (b)(6)(b)(7)(C) This account was opened on 12 Sep 95, and is paid through 12 Dec 15. The Email account (b)(6)(b)(7)(C) pobox.com, (b)(6)(b)(7)(C)@pobox.com and (b)(6)(b)(7)(C)@pobox.com were all part of the same account and used since 1 Nov 09. The address (b)(6)(b)(7)(C)@pobox.com was also used with this account from 25 Mar 2008 until 15 Nov 2009. During the time frame specified in the subpoena, all pobox email was forwarded to the email address (b)(6)(b)(7)(C)@opensysadmin.com <mailto: (b)(6)(b)(7)(C)@opensysadmin.com> .

At no point during the requested period did (b)(6)(b)(7)(C)@pobox.com store mail at pobox.com. The user only logged in to pobox.com to make changes to the account.

Ms. (b)(6)(b)(7)(C) provided information on the last 6 logins to the account:
(The date format is yyyymmddhhmmss):

20091115180006 from IP: 18.214.0.239 (Registered to MIT.edu)

20091120121756 from IP: 66.92.78.210 (Registered to Speakeasy.net)

20091120174659 from IP: 18.214.0.239 (Registered to MIT.edu)

20100209230527 from IP: 71.184.178.120 (Registered to Verizon Internet Services)

20100304013807 from IP: 71.184.186.239 (Registered to Verizon Internet Services)

20100415173459 from IP: 18.214.0.239 (Registered to MIT.edu)

Ms. (b)(6)(b)(7)(C) stated that the account (b)(6)(b)(7)(C)@pobox.com received between 400 and 800 emails per day and it would take weeks to produce lists of all email received. ////LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION Washington Metro Resident Agency Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SA (b)(6)(b)(7)(C), (b) (7)(E)		
SIGNATURE SA (b)(6)(b)(7)(C)	DATE 14 JUL 10	EXHIBIT 95

Exhibit 96

Page(s) 000667 thru 000670 referred to:

Department of Defense

Office of Inspector General
DoD IG FOIA Requester Service Center
4800 Mark Center Drive – Suite 14L24
Alexandria, VA 22350-1500

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

About 1300, 16 Jul 10, this office received the results of the Department of Defense, Office of Inspector General (DoDIG) subpoena, 2010246-10456, from T-Mobile, for the cellular telephone number (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) previously identified as PFC MANNING's personal cellular telephone, via email. The results revealed the billing account name was Bradley Manning and that the account opened on 6 Dec 06 and closed on 12 Oct 09. (See Subpoena)

////LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060
SIGN (b)(6)(b)(7)(C)	DATE: 16 Jul 10 / EXHIBIT: 97

CID FORM 94
1 FEB 77

Exhibit 98

Page(s) 000672 thru 000675 referred to:

Department of Defense

Office of Inspector General
DoD IG FOIA Requester Service Center
4800 Mark Center Drive – Suite 14L24
Alexandria, VA 22350-1500

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

About 1005, 19 Jul 10, SA (b)(6)(b)(7)(C) received the results of Department of Defense Inspector General (DOD/IG) Subpoena 2010247-10461 served on Facebook for any records related to any account for (b)(6)(b)(7)(C) or the email account (b)(6)(b)(7)(C) @gmail.com.

Facebook security opened a case on this matter (Case #13640) and conducted a search of its records. Facebook reported to SA (b)(6)(b)(7)(C) that no such user/account was found. See response from Facebook Security for further details. ////LAST ENTRY///.

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION Washington Metro Resident Agency Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SA (b)(6)(b)(7)(C), (b) (7)(E)		
SIGNATURE SA (b)(6)(b)(7)(C)	DATE 19 JUL 10	EXHIBIT 99

Exhibit 100

Page(s) 000677 thru 000680 referred to:

Department of Defense

Office of Inspector General
DoD IG FOIA Requester Service Center
4800 Mark Center Drive – Suite 14L24
Alexandria, VA 22350-1500

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

About 0900, 20 Jul 10, SA (b)(6)(b)(7)(C) received the results of the Department of Defense Inspector General (DOD/IG) Subpoena 2010233-10429 issued to Google Inc, for subscriber information related to the account (b)(6)(b)(7)(C)@gmail.com". Google stated no account existed. ///LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060
SIGNATURE SA (b)(6)(b)(7)(C)	DATE 20 July 2010
	EXHIBIT 101

Exhibit 102

Page(s) 000682 thru 000685 referred to:

Department of Defense

Office of Inspector General
DoD IG FOIA Requester Service Center
4800 Mark Center Drive – Suite 14L24
Alexandria, VA 22350-1500

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

About 1130, 21 Jul 10, SA (b)(6)(b)(7)(C) received the results of the Department of Defense Inspector General (DOD/IG) Subpoena 2010247-10460 issued to Google, Inc, for subscriber information related to the account (b)(6)(b)(7)(C) @gmail.com.

The records showed the account was created on 25 May 10, at 11:04:32 UTC. The name used to create the account was (b)(6)(b)(7)(C) The account was created from IP address: 109.224.6.127 (Registered under (b)(6)(b)(7)(C) to EarthLink Ltd). In the response, Google stated there was no activity on the account, therefore no connection logs were available. See response from Google for further details. ///LAST ENTRY///.

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION Washington Metro Resident Agency Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SA (b)(6)(b)(7)(C), (b) (7)(E)		
SIGNATURE SA (b)(6)(b)(7)(C)	DATE 21 JUL 10	EXHIBIT 103

Exhibit 104

Page(s) 000687 thru 000691 referred to:

Department of Defense

Office of Inspector General
DoD IG FOIA Requester Service Center
4800 Mark Center Drive – Suite 14L24
Alexandria, VA 22350-1500

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

About 1240, 23 Jul 10, SA (b)(6)(b)(7)(C) and Mr. (b)(6)(b)(7)(C) Special Assistant U.S. Attorney, U.S. Attorney's Office, Eastern District of Virginia, 2100 Jamieson Avenue, Alexandria, VA 22314, met with the Honorable (b)(6)(b)(7)(C) U.S. Magistrate Judge, Eastern District of Virginia, 401 Courthouse Square, Alexandria, VA 22314, and obtained a Federal Magistrate Search Warrant, Search Warrant Number 1:10-SW-396, for the computer identified as an IBM ThinkCentre, Model 36U, desktop computer, Serial Number (SN): "KCZK85T"; which had been further identified as the property of PFC MANNING. The aforementioned computer had been previously collected as evidence by this office on 18 Jun 10, from the home of Ms. (b)(6)(b)(7)(C) located at (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) Ms. (b)(6)(b)(7)(C) had identified the IBM ThinkCentre computer as PFC MANNING's property, and had further provided investigators consent to collect this prorperty as potential evidence.

AGENT'S COMMENT: The facts and circumstances relating to the identification and collection of the property identified as belonging to PFC MANNING, were further documented in the Agent's Investigative Report report detailing the interview of Ms. (b)(6)(b)(7)(C)

About 1829, 23 Jul 10, SA (b)(6)(b)(7)(C) executed the abovementioned Search Warrant by sending a Request for Forensic Examination to the Digital Forensics and Research Branch (DFRB), Computer Crime Investigative Unit, U.S. Army CID, which included a copy of the Search Warrant, in order to conduct an examination of the IBM ThinkCentre computer for any evidence or information related to this investigation.

// **LAST ENTRY** //

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE (b)(6)(b)(7)(C)	DATE 23 Jul 10	EXHIBIT 105

FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE

Exhibit(s) 106

Page(s) 000693 thru 000696

Documents

SEALED

by the

U.S. District Court
for the Eastern District of Virginia

Exhibit 107

Page(s) 000697 thru 000861 referred to:

Office of the Judge Advocate General
ATTN: DAJA-ZX
Pentagon Room 2B514
2200 Army Pentagon
Washington, DC 20310-2200

CLASSIFIED

Exhibit(s) 108

Page(s) 000862 thru 000862b referred to:

Commander
INSCOM
ATTN: IAMG-C-FOIA
4552 Pike Road
Fort Meade, MD 20755-5995

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

On 27 Jul 10, SA (b)(6)(b)(7)(C) U.S. Immigration and Customs Enforcement (ICE), Joint Terrorism Task Force (JTTF), New York, NY, related the Treasury Enforcement Communication System (TECS) had reported that Mr. Jacob APPELBAUM, (b)(6)(b)(7)(C) a known WikiLeaks spokesperson, was returning to the United States from Amsterdam on board Continental flight 103, about 1130, 29 Jul 10, en route to a connecting flight to Las Vegas, NV.

About 1000, 29 Jul 10, SA (b)(6)(b)(7)(C), (b) (7)(E) and SA (b)(6)(b)(7)(C), (b) (7)(E) Washington Metro Resident Agency (WMRA), Computer Crime Investigative Unit (CCIU), U.S. Army Criminal Investigation Command, Fort Belvoir, VA, coordinated with SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) Diplomatic Security Service (DSS), U.S. Department of State (DoS), New York, NY, at B Terminal, Continental Arrivals, Newark International Airport. Upon Mr. APPELBAUM's arrival at 1130 at Newark International Airport, Officers of the U.S. Customs and Border Protection (CBP), Newark International Airport, escorted Mr. APPELBAUM to secondary screening, for Continental Arrivals, B Terminal.

About 1230, 29 Jul 10, SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) interviewed Mr. APPELBAUM under ICE's border search/detention authority, in a room located near the CBP Continental Arrivals secondary screening area. Mr. APPELBAUM related he was returning to the United States from a scientific convention in Amsterdam, and was traveling to Las Vegas, NV, to attend the DEFCON Hacking Conference. Mr. APPELBAUM related he was giving a presentation at DEFCON pertaining to the Power of Chinese Network Security. Mr. APPELBAUM related he worked for The Onion Router (TOR) network and indicated he was in Iceland earlier this year working on a TOR project for WikiLeaks. Mr. APPELBAUM related he had spoken with Mr. Julian ASSANGE about PFC MANNING. Mr. APPELBAUM believed PFC MANNING was a good person who will spend the rest of his life in jail. Mr. APPELBAUM related he normally deletes all phone logs, contact lists, and destroys his Subscriber Identity Module (SIM) card upon arrival from foreign travel, which he believed to be a normal practice. When questioned about classified material, including the material disclosed by PFC MANNING to WikiLeaks, Mr. APPELBAUM related it was not illegal to "state things in public that have already been stated in public", and Mr. APPELBAUM related he did not have any classified information, nor had he ever had any classified information in his possession. Mr. APPELBAUM added he did not know anything about WikiLeaks or any classified information, and he did not have access to any data of any kind. When confronted about his recent presentation for Mr. ASSANGE at the HOPE Conference in New York, Mr. APPELBAUM related he only spoke for Mr. ASSANGE because Mr. ASSANGE could not come to the United States and speak freely. Mr. APPELBAUM clarified his relationship with WikiLeaks relating he was a WikiLeaks spokesperson. When additional questions were asked pertaining to his extensive international travel, Mr. APPELBAUM related he hiked into Iraq in 2005, armed with two side arms and a rifle where he met people who picked him up and transported him into the Kurdish region of Iraq. When subsequently questioned about a tattoo on his left forearm, which depicted a peacock eating a snake that itself was eating it own tail, Mr. APPELBAUM expanded upon his travels in Iraq, relating he visited or stayed with a Kurdish tribe that worshiped animals, which inspired his tattoo. When asked about the snake, Mr. APPELBAUM commented about eating the snake as a last resort in a survival situation and referred to what he characterized as a

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
(b)(6)(b)(7)(C)	DATE 29 Jul 10	EXHIBIT 109

DETAILS

Special Forces statement, "eating the snake". When asked about why he traveled into Iraq and whether his travel pertained to WikiLeaks or to the reporting of a story, Mr. APPELBAUM related his father had been murdered, but Mr. APPELBAUM refused to delve any deeper into his father's death; however, Mr. APPELBAUM related his trip into Iraq was personally motivated. Additionally, Mr. APPELBAUM related while in Iraq, he spent time with an Iraqi sniper who stated he shot U.S. soldiers in the leg because the Iraqi sniper believed he was doing them a favor. When asked to clarify whether the wounding of U.S. soldiers was an attempt to remove the soldiers from the battlefield, Mr. APPELBAUM, related the Iraqi sniper believed soldiers in the U.S. were conscripted like the sniper; therefore, U.S. soldiers did not choose to invade Iraq, but instead they were forced to invade Iraq by the U.S. government. Additionally, Mr. APPELBAUM related the Iraqi sniper believed by wounding U.S. soldiers the U.S. government would be forced to return the wounded soldiers to their homes. Mr. APPELBAUM related if U.S. soldiers only realized the impact of the invasion of Iraq upon Iraqis, U.S. soldiers would not want to be in Iraq. Mr. APPELBAUM then asked what SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) would do if the U.S. was invaded, and added he would fight the invaders.

AGENT'S COMMENT: Mr. (b)(6)(b)(7)(C) was in possession of multiple unopened SIM cards, which CBP and ICE returned to him. SA (b)(6)(b)(7)(C) ICE, New York, NY, was able to image or detain the following property, which was collected from Mr. APPELBAUM: Three mobile telephones, from which one SIM card image was captured; images of two USB drives; and an image of a Micro Secure Digital (SD) card. Numerous receipts and papers were recovered and copied; in addition, Mr. APPELBAUM had an ultra violet mini black light in his possession, which SA (b)(6)(b)(7)(C) used to unsuccessfully search the aforementioned documents for hidden writings. CBP officers related during Mr. APPELBAUM's pat down, when CBP related to Mr. APPELBAUM that in the past, pat downs have facilitated the identification of large sums of contraband money, Mr. APPELBAUM stated if he had contraband he would have mailed it rather than attempt to cross the border with contraband in his possession. Further, Mr. APPELBAUM was in possession of a laptop computer that had no hard drive. Mr. APPELBAUM clarified that he used boot discs to run the computer; however, no boot discs were found in Mr. APPELBAUM's possession.

Between 1400 and 1500, 29 Jul 10, SA (b)(6)(b)(7)(C) assisted SA (b)(6)(b)(7)(C) Computer Forensic Agent, Immigrations and Customs Enforcement, by attempting extraction of data from three cellular phones utilizing the Cellebrite Universal Forensic Extraction Device (UFED).

Cellular Phone Make/Model:	HTC Google Nexus One
Cellular Phone Serial Number:	HT019P806305
Cellular Phone IMEI:	354957032526900
Cellular Phone Part Number:	99HKE002-00

SIM: 8907 2604 2002 2021 881

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE (b)(6)(b)(7)(C)	DATE 29 Jul 10	EXHIBIT 109

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

The phone contained a Kingston MicroSD 8GB card, which was provided to SA (b)(6)(b)(7)(C) for imaging. The phone was password protected and could not be extracted using the Cellebrite UFED. The SIM ID was cloned in an attempt to by-pass the password protection, which met with negative results. Data was extracted from the SIM using the Cellebrite UFED and provided to SA (b)(6)(b)(7)(C)

Cellular Phone Make/Model:	HTC Touch Viva
Cellular Phone Serial Number:	SZ845KC00597
Cellular Phone IMEI:	353443025456927
Cellular Phone Part Number:	99HHB011-00

The phone did not contain a SIM or memory card, and was password protected. Due to password protection, data could not be extracted using the Cellebrite UFED.

Cellular Phone Make/Model:	HTC Innovation
Cellular Phone Serial Number:	HT623F315989
Cellular Phone IMEI:	358167000321948
Cellular Phone Part Number:	99HBW009-00

The phone would not power-on, and a charger was not found. The phone was not supported by the Cellebrite UFED. There was not a SIM or memory card present in the phone.

About 1645, 29 Jul 10, ICE and CBP released Mr. APPELBAUM from secondary screening. ///LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SI (b)(6)(b)(7)(C)	DATE 29 Jul 10	EXHIBIT 109

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

About 1410, 27 Jul 10, SA (b)(6)(b)(7)(C) collected as evidence one Digital Versatile Disc (DVD) containing select contents of "http://www.nonrel.cie.centcom.smil.mil/sites/organization/specialstaff/JA /CentcomLegal/Forms/AllItems.aspx?RootFolder=%2fsites%2forganization%2fspecialstaff%2fJA%2fCentcomLegal%2fInvestigations%2fFarah&FolderCTID=&View={8E62FD94-A7D9-4436-9509-8B62FEB04A5E}" from the forensic computer, which was documented on Evidence/Property Custody Document (EPCD), Document Number (DN) 106-10.

AGENT's COMMENT: The content from the above mentioned site was gathered by SA (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) 310th MI Battalion, 9805 Lowen Road, Bldg 193, Fort Belvoir, VA, between about 1605, 21 Jul 10 and 1145, 27 Jul 10, utilizing WinHTTrack Website Copier 3.43-9. The content was gathered for comparison to suspected classified material found during forensic examinations of evidence collected in this investigation pertaining to the Gharani airstrike video and supporting documentation.

About 1615, 30 Jul 10, SA (b)(6)(b)(7)(C) received the results of the Department of Defense, Office of Inspector General (DODIG) subpoena, 2010265-10489, from Verizon Internet Services, for the customer information pertaining to IP address 71.190.140.39, via facsimile. The IP address, which was originally provided to this office in chat logs provided by RS221-0005 pertaining to an individual who claimed to have decrypted the Apache airstrike video, was leased by Ms. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) (See Subpoena)

//LAST ENTRY//

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE (b)(6)(b)(7)(C)	DATE 30 Jul 10	EXHIBIT 110

Exhibit 111

Page(s) 000867 thru 000871 referred to:

Department of Defense

Office of Inspector General
DoD IG FOIA Requester Service Center
4800 Mark Center Drive – Suite 14L24
Alexandria, VA 22350-1500

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER 0009-10-CID321

PAGE 1 OF 1 PAGES

DETAILS

About 0730, 2 Aug 10, SA (b)(6)(b)(7)(C) received a Request For Assistance (RFA) from the Washington Metro Resident Agency, Computer Crime Investigative Unit, Fort Belvoir, VA 22060 requesting this office coordinate with authorities at Fort Huachuca, AZ to determine if PFC Bradley E. MANNING, (b)(6)(b)(7)(C) the subject of CID Report of Investigation 0028-10-CID221-10117 had received Non-Judicial Punishment (NJP) while assigned to the 305th Military Intelligence (MI) Battalion (BN) for Advanced Individual Training (AIT) in 2008. The source of this information was an article on wired.com (http://www.wired.com/threatlevel/2010/07/manning_youtube/) indicating PFC MANNING had received NJP for uploading YouTube videos discussing classified facilities on Fort Huachuca while in a trainee status.

About 0915, 2 Aug 10, SA (b)(6)(b)(7)(C) coordinated with CPT (b)(6)(b)(7)(C) Chief Criminal Law, Staff Judge Advocate (SJA), Fort Huachuca, AZ and requested any information regarding any NJP received by PFC MANNING while assigned to Fort Huachuca, AZ.

About 1000, 2 Aug 10, SA (b)(6)(b)(7)(C) was contacted by CPT (b)(6)(b)(7)(C) who related there was no existing documentation for any NJP given to PFC MANNING while he was assigned to Fort Huachuca. Further coordination with the 305th MI BN which PFC MANNING was assigned to at the time of the incident revealed no documentation was maintained in their files as any record of Article 15 would have been destroyed upon Permanent Change of Station (PCS). LTC (b)(6)(b)(7)(C) Commander, 305th MI Battalion related to CPT (b)(6)(b)(7)(C) that no one in the unit was assigned to Fort Huachuca at the time of the alleged incident, but there was a previous NCO from the unit who related via conversations with current military members that PFC MANNING was given a verbal admonishment and told to provide a class to his fellow soldiers on proper OPSEC procedures. No further information was available.

//LAST ENTRY//

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
(b)(6)(b)(7)(C), (b) (7)(E)	Arizona Branch Office, Computer Crime Investigative Unit U.S. Army CID, Fort Huachuca, AZ 85613	
(b)(6)(b)(7)(C)	DATE 2 August 2010	EXHIBIT 112

CID FORM 94
1 FEB 77

FOR OFFICIAL USE ONLY
Law Enforcement Sensitive

Approved_____

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

About 1508, 2 Aug 10, SA (b)(6)(b)(7)(C), (b) (7)(E) this office, advised LTC (b)(6)(b)(7)(C) U.S. Army Element - Defense Intelligence Agency, The Pentagon, Washington, DC 20001, of his legal rights for the offense of Fraternization prior to attempting to conduct an interview. LTC (b)(6)(b)(7)(C) invoked his legal rights, indicating he did not wish to be questioned or say anything and requested an attorney.

AGENT'S COMMENT: LTC (b)(6)(b)(7)(C) was advised of his legal rights for the offense of Fraternization, which may be applicable under Uniform Code of Military Justice (UCMJ), Article 92 – Failure to Obey an Order or Regulation (for potential violations of command policy, specifically Army Regulation 600-20, Paragraph 4-14c, regarding 'Prohibited Relationships'), and/or UCMJ, Article 134 – Fraternization; as an analysis of email messages sent between the personal email accounts reportedly used by LTC (b)(6)(b)(7)(C) and PFC MANNING revealed what may have been an inappropriate relationship. During LTC (b)(6)(b)(7)(C) rights advisal, SA (b)(6)(b)(7)(C) was also present. Upon LTC (b)(6)(b)(7)(C) invoking his rights, SA (b)(6)(b)(7)(C) requested that LTC (b)(6)(b)(7)(C) obtain legal counsel and further requested him to have his attorney contact either SA (b)(6)(b)(7)(C) or SA (b)(6)(b)(7)(C) to discuss the nature of the questions related to PFC MANNING and this investigation this office wished to ask LTC (b)(6)(b)(7)(C)

// **LAST ENTRY** //

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit Fort Belvoir, VA 22060	
SIGNATU (b)(6)(b)(7)(C)	DATE 2 Aug 10	EXHIBIT 113

FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE

FOR OFFICIAL USE ONLY-LAW ENFORCEMENT SENSITIVE

RIGHTS WAIVER/NON-WAIVER CERTIFICATE AND STATEMENT PROCEDURE/WAIVER CERTIFICATE

For use of this form, see AR 190-30; the proponent agency is ODCSOPS

DATA REQUIRED BY THE PRIVACY ACT

AUTHORITY: Title 10, United States Code, Section 3012(g)
PRINCIPAL PURPOSE: To provide commanders and law enforcement officials with means by which information may be accurately identified.
ROUTINE USES: Your Social Security Number is used as an additional/alternate means of identification to facilitate filing and retrieval.
DISCLOSURE: Disclosure of your Social Security Number is voluntary.

1. LOCATION	2. DATE	3. TIME	FILE NO.
9805 Lowen Road, Fort Belvoir, VA 22060	2 Aug, 10	1508	0028-10-CID221-10117

5. NAME *(Last, First, MI)*	8. ORGANIZATION OR ADDRESS
(b)(6)(b)(7)(C)	US Army Element / DIA Pentagon, VA
6. SSN: (b)(6)(b)(7)(C)	7. GRADE/STATUS: LTC/O-5

PART I - RIGHTS WAIVER/NON-WAIVER CERTIFICATE

Section A. Rights

The investigator whose name appears below told me that he/she is with the United States Army Criminal Investigation Command, Computer Crime Investigative (b)(6)(b)(7)(C) and wanted to question me about the following offense(s) of which I am (b)(6)(b)(7)(C) cted/accus ternization.

e he/she asked me any questions about the offense(s), however, he/she made it clear to me that I have the following rights:

o not have to answer any questions or say anything.

ything I say or do can be used as evidence against me in a criminal trial.

or personnel subject to the UCMJ) I have the right to talk privately to a lawyer before, during, and after questioning and to have a lawyer present with me ring questioning. This lawyer can be a civilian lawyer I arrange for at no expense to the Government or a military lawyer detailed for me at no expense to me, both.

- or -

(b)(6)(b)(7)(C) *(For civilians not subject to the UCMJ)* I have the right to talk privately to a lawyer before, during, and after questioning and to have a lawyer present with me during questioning. I understand that this lawyer can be one that I arrange for at my own expense, or if I cannot afford a lawyer and want one, a lawyer will be appointed for me before any questioning begins.

If I am now willing to discuss the offense(s) under investigation, with or without a lawyer present, I have a right to stop answering questions at any time, or speak privately with a lawyer before answering further, even if I sign the waiver below.

5. COMMENTS (Continue on reverse side)

Section B. Waiver

I understand my rights as stated above. I am now willing to discuss the offense(s) under investigation and make a statement without talking to a lawyer first and without having a lawyer present with me.

WITNESSES *(If available)*	3. SIGNATURE OF INTERVIEWEE
1a. NAME *(Type or Print)* SA (b)(6)(b)(7)(C) (b)(6)(b)(7)(C)	
b. ORGANIZATION OR ADDRESS AND PHONE Computer Crime Investigative Unit Fort Belvoir, VA 22060	4. SIGNATURE OF INVESTIGATOR (b)(6)(b)(7)(C)
2a. NAME *(Type or Print)*	5. TYPED NAME OF INVESTIGATOR SA (b)(6)(b)(7)(C)
b. ORGANIZATION OR ADDRESS AND PHONE	6. ORGANIZATION OF INVESTIGATOR Computer Crime Investigative Unit Fort Belvoir, VA 22060

Sec (b)(6)(b)(7)(C)

1. (b)(6)(b)(7)(C) up my rights:

☑ I want a lawyer.

☑ I do not want to be questioned or say anything.

2. SIGNAT (b)(6)(b)(7)(C)

ATTACH T Y EXECUTED BY THE SUSPECT/ACCUSED.

DA FOR EDITION OF NOV 84 IS

EXHIBIT 114 000874

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER 0028-10-CID221-10117

DETAILS

About 0800, 2 Aug 10, SA (b)(6)(b)(7)(C) coordinated with Ms. (b)(6)(b)(7)(C) Chief Executive Officer at, IC Group, 1100 Vine St., Suite C8, Philadelphia, PA 19107, in regards to the Department of Defense, Office of Inspector General (DOD/IG) Subpoena 2010251-10468, issued for the records related to the account (b)(6)(b)(7)(C)@pobox.com.

Ms. (b)(6)(b)(7)(C) provided the following information regarding the account.

The account in question was registered to Mr. (b)(6)(b)(7)(C) This account was opened on 12 Sep 95, and paid through 12 Dec 15. (b)(6)(b)(7)(C) provided SA (b)(6)(b)(7)(C) with logs detailing the email addresses that passed through the pobox account. The logs represented 103,695 pieces of email handled for the dclark account since February 1, 2010 (as far back as the logs went). Ms. (b)(6)(b)(7)(C) stated that there were approximately 495 messages during this time period that were forwarded, but the sender's information was not logged. Ms. (b)(6)(b)(7)(C) explained that this is not uncommon. Ms. (b)(6)(b)(7)(C) stated that in order to keep the servers running as quickly as possible, if the log host was not able to accept a connection, write a log to disk, etc., the system would automatically drop the logs. The logs were sent to SA (b)(6)(b)(7)(C) in a compressed ZIP file. (b)(6)(b)(7)(C) also provided a text file listing all unique email addresses from the logs.

About 1300, 2 Aug 10, SA (b)(6)(b)(7)(C) transferred the following files from the email sent from Ms. (b)(6)(b)(7)(C) to a Compact Disk Recordable (CD-R); (b)(6)(b)(7)(C) tar.gz, (b)(6)(b)(7)(C) senders.txt, ATT565113.htm, and ATT56114.htm". The CD-R was collected as evidence and documented on Evidence Property Custody Document (EPCD), Document Number (DN): 108-10. ///LAST ENTRY///.

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION Washington Metro R.A. Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SA (b)(6)(b)(7)(C), (b) (7)(E)		
SIGNATURE (b)(6)(b)(7)(C) SA	DATE 3 AUG 10	EXHIBIT 115

Exhibit(s) 116 thru 119

Page(s) 000876 thru 000882 referred to:

Federal Bureau of Investigation
Record Information/Dissemination Section
170 Marcel Drive
Winchester, Virginia 22602-4843

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

About 0940, 5 Aug 10, SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) National Security Agency (NSA), 9800 Savage Road, Fort Meade, MD 20755, interviewed U.S. Air Force Senior Master Sergeant (SMSgt) (b)(6)(b)(7)(C) (NMN) (b)(6)(b)(7)(C) 32nd Intelligence Squadron, 9801 Love Road, Fort Meade, MD 20755, as he was identified as the Noncommissioned Officer in Charge (NCOIC) of Cryptological Support Team 5 (CST5) and worked in the same Sensitive Compartmented Information Facility (SCIF) where PFC MANNING worked between the time PFC MANNING arrived at FOB Hammer and 15 Jan 10, when SMSgt (b)(6)(b)(7)(C) returned to the United States at the completion of his Iraq assignment. SMSgt (b)(6)(b)(7)(C) related that he was assigned in Iraq for approximately 6 months, and that the first four months of his assignment at Forward Operating Base (FOB) Hammer were with the 3rd Brigade Combat Team (BCT) of the 82nd Airborne Division; while the remaining two months of his assignment were with PFC MANNING's unit, 2BCT, of the 10th Mountain Division. SMSgt (b)(6)(b)(7)(C) related the 3rd BCT soldiers he worked with were seasoned analysts, and many of them had multiple previous deployments. SMSgt (b)(6)(b)(7)(C) explained he noticed the difference when PFC MANNING's unit arrived, as he described them as being somewhat 'green' with a lot of junior personnel. SMSgt (b)(6)(b)(7)(C) stated he worked with PFC MANNING on the same shift, the midnight shift, and that there were approximately three other NSA assigned personnel also working in the SCIF on the night shift. SMSgt (b)(6)(b)(7)(C) identified these personnel as Senior Airman (SrA) (b)(6)(b)(7)(C) U.S. Air Force Technical Sergeant (TSgt) (b)(6)(b)(7)(C) and U.S. Marine Corporal (b)(6)(b)(7)(C) SMSgt (b)(6)(b)(7)(C) said due to the manner in which their office in the SCIF was set up, he and his fellow NSA assigned personnel were in a back room, which PFC MANNING would not have had uncontrolled access. SMSgt (b)(6)(b)(7)(C) explained if anyone had entered their area they would have had to announce themselves and why they were in the area. SMSgt (b)(6)(b)(7)(C) explained there wasn't any access to the Joint Worldwide Intelligence Communications System (JWICS) while he was at FOB Hammer, but mentioned that one of the personnel in PFC MANNING's unit was trying to get JWICS installed in the SCIF. SMSgt (b)(6)(b)(7)(C) could not provide any information as to whether that occurred or not after his departure. SMSgt (b)(6)(b)(7)(C) stated during the time he worked alongside PFC MANNING, he noticed that PFC MANNING's unit appeared to put undue stress on him. SMSgt (b)(6)(b)(7)(C) explained one instance in which PFC MANNING was conducting a briefing and froze up, and that the other personnel in the unit just allowed PFC MANNING to stand there for two to three minutes without saying anything. SMSgt (b)(6)(b)(7)(C) explained in another incident PFC MANNING was asked to do something and he became upset and threw a video monitor to the ground destroying it. SMSgt (b)(6)(b)(7)(C) said in regard to the broken video monitor incident, that two other unit members picked PFC MANNING up and physically carried him out of the SCIF. SMSgt (b)(6)(b)(7)(C) explained if that had happened with one of his subordinates, they would have not been allowed to return to the SCIF. SMSgt (b)(6)(b)(7)(C) related he felt PFC MANNING may have been mentally unstable. SMSgt (b)(6)(b)(7)(C) said he believed that PFC MANNING was assigned extra duty as a result of this incident, which he felt was uncalled for but perhaps just part of the Army culture. SMSgt (b)(6)(b)(7)(C) said as a senior Noncommissioned Officer (NCO), PFC MANNING's superiors should have recognized these issues with PFC MANNING. SMSgt (b)(6)(b)(7)(C) further stated the NCOIC in charge of PFC MANNING was MSG (b)(6)(b)(7)(C) who he described as not having any inter-personal skills and that MSG (b)(6)(b)(7)(C) would chastise PFC MANNING in front of groups of other personnel, such as in SCIF briefings. SMSgt (b)(6)(b)(7)(C) said he never heard anyone make any derogatory comments about

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE (b)(6)(b)(7)(C)	DATE 5 Aug 10	EXHIBIT 120

DETAILS

PFC MANNING in regard to his sexual preference and that he did not feel PFC MANNING was obvious about being homosexual. SMSgt (b)(6)(b)(7)(C) felt PFC MANNING was otherwise a good analyst and was surprised to hear about his apprehension by CID in the news media. SMSgt (b)(6)(b)(7)(C) later explained he felt PFC (b)(6)(b)(7)(C) would be someone of interest for CID to interview, based upon his apparent knowledge of computers, as well as issues PFC (b)(6)(b)(7)(C) had himself while assigned at FOB Hammer. SMSgt (b)(6)(b)(7)(C) further detailed it was his understanding that PFC (b)(6)(b)(7)(C) had threatened to commit suicide while assigned in Iraq, causing him to be released from duty for several days. SMSgt (b)(6)(b)(7)(C) said he knew of this situation as one of the personnel he supervised had to pick up PFC (b)(6)(b)(7)(C) duties as a result of this issue. SMSgt (b)(6)(b)(7)(C) stated he was surprised when PFC (b)(6)(b)(7)(C) was later allowed to return to his duties based on the circumstances. SMSgt (b)(6)(b)(7)(C) said he did not know much about the chat encryption application 'OTR', would not have mentioned information related to NSA and the iPhone device to PFC MANNING, as well as he did not know how PFC MANNING may have gained knowledge to make statements about data he recognized from an NSA database. SMSgt (b)(6)(b)(7)(C) said he felt many of the allegations which PFC MANNING was suspected to have committed likely occurred after his team of NSA assigned personnel left FOB Hammer in the middle of January 2010. SMSgt (b)(6)(b)(7)(C) said the NSA personnel that replaced him at FOB Hammer seemed to be less experienced and suggested these incidents could have occurred while the team that replaced his group were there in Iraq. SMSgt (b)(6)(b)(7)(C) could not explain the situation which was mentioned by PFC MANNING in regard to an incident that MANNING witnessed wherein Iraqi's allegedly handing out leaflets were arrested by Iraqi National Police. SMSgt (b)(6)(b)(7)(C) said PFC MANNING should have never gone 'outside the wire' of FOB Hammer to have been involved in something like that. SMSgt (b)(6)(b)(7)(C) further stated he could not explain when this incident involving the arrest of Iraqi civilians would have occurred and added this type of mission would have been conducted by Human Intelligence (HUMINT) personnel. SMSgt (b)(6)(b)(7)(C) related, when asked what the term "Reflection" meant, that this was terminology used by personnel in their section which means 'an indicator' or an event that has already happened, but could have also been used to refer to a document or report. SMSgt (b)(6)(b)(7)(C) identified several Signals Intelligence (SIGINT) personnel assigned with PFC MANNING as SSG (b)(6)(b)(7)(C) and/or SSG (b)(6)(b)(7)(C) SMSgt (b)(6)(b)(7)(C) could not immediately provide any additional information relevant to this investigation.

AGENTS COMMENT: SMSgt (b)(6)(b)(7)(C) mentioned after having read a news article related to this investigation of PFC MANNING, that PFC MANNING was alleged to have been lip-synching to the musical artist "Lady Gaga", specifically the song "Telephone", during one of the times he allegedly downloaded and transferred to a Compact Disc (CD) some of the Classified U.S. Government materials unlawfully disclosed in relation to this investigation. SMSgt (b)(6)(b)(7)(C) said he felt the incidents which PFC MANNING is suspected to be involved in occurred after his team had redeployed from Iraq about 15 Jan 10, based on the song "Telephone" having been released on 26 Jan 10. A further review by SA (b)(6)(b)(7)(C) of this information revealed SMSgt (b)(6)(b)(7)(C) appeared to be mistaken as the music album this song appears on, Lady Gaga's album "The Fame Monster", was originally released in the United States in November 2009. SA (b)(6)(b)(7)(C) did note that this album was reportedly released in various formats (CD,

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE (b)(6)(b)(7)(C)	DATE 5 Aug 10	EXHIBIT 120

DETAILS

DVD, digital download, etc.) on different dates in separate regions of the world between November 2009 and November 2010.

// **LAST ENTRY** //

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATU (b)(6)(b)(7)(C)	DATE 5 Aug 10	EXHIBIT 120

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

About 1750, 5 Aug 10, SA (b)(6)(b)(7)(C) received an e-mail from SA (b)(6)(b)(7)(C), (b) (7)(E) 62nd Military Police Detachment (CID), Fort Drum, NY (FDNY), who provided a scanned copy of DA Form 2062, Hand Receipt/Annex Number pertaining to PFC MANNING's belongings and a copy of DA Form 1594, Daily Staff Journal or Duty Officer's Log, containing the name (b)(6)(b)(7)(C) and telephone number '786-2601' both in the same circle. SA (b)(6)(b)(7)(C) stated it was reported Mr. (b)(6)(b)(7)(C) came and picked up the boxes with PFC MANNING's belongings sometime in the middle of the night in late Oct or early Nov09 (pre-deployment). SA (b)(6)(b)(7)(C) stated SSG (b)(6)(b)(7)(C), NCOIC, Rear Detachment, HHC, 2nd BCT, 10th MTN DIV, FDNY, did not know PFC MANNING's relationship to Mr. (b)(6)(b)(7)(C) or have Mr. (b)(6)(b)(7)(C) contact information.

//LAST ENTRY//

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060
(b)(6)(b)(7)(C), (b) (7)(E)	DATE: 5 Aug 10 / EXHIBIT: 121

Exhibit(s) 122 and 123

Page(s) 000887 thru 000888 referred to:

Directorate of Human Resources
Administrative Services Division
Attn: IMNE-DRM-HRR (FOIA-PA)
10720 Mt. Belvedere Blvd.
Fort Drum, New York 13602-5045

Exhibit(s) 124

Page(s) 000889 thru 000891 referred to:

Federal Bureau of Investigation
Record Information/Dissemination Section
170 Marcel Drive
Winchester, Virginia 22602-4843

Exhibit(s) 125

Page(s) 000892 and 000893 withheld.

5 U.S.C. § 552(b)(6) & (b)(7)(C)
Third Party Information
Not Reasonably Segregable

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

About 0800, 9 Aug 10, SA (b)(6)(b)(7)(C) received the results from the Department of Defense Inspector General (DOD/IG) Subpoena 2010247-10459, served on Twitter for the account "(b)(6)(b)(7)(C) or any account associated with the Email address (b)(6)(b)(7)(C) @gmail.com".

The following subscriber information was provided by Twitter:
User ID: 147937041
Account: bmanningfm
Created on: 25 May 10, 12:30:27 GMT
Updated on: 25 May 10, 12:46:22 GMT
Last login: 109.224.6.127 (Earthlink Telecommunications, Iraq)
Email account used: (b)(6)(b)(7)(C) @gmail.com.

It appeared that the account was created and last accessed on the same day.
////LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION Washington Metro R.A. Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SA (b)(6)(b)(7)(C), (b) (7)(E)		
SIGNA (b)(6)(b)(7)(C) S.A.	DATE 9 AUG 10	EXHIBIT 126

Exhibit 127

Page(s) 000895 thru 000899 referred to:

Department of Defense

Office of Inspector General
DoD IG FOIA Requester Service Center
4800 Mark Center Drive – Suite 14L24
Alexandria, VA 22350-1500

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

About 0940, 4 Aug 10, SA (b)(6)(b)(7)(C) SA (b)(6)(b)(7)(C) this office, and SA (b)(6)(b)(7)(C) U.S. Department of State, Boston Field Office, Boston, MA, received documentation pertaining to Mr. (b)(6)(b)(7)(C) from SA (b)(6)(b)(7)(C) FBI, Springfield, MA. SA (b)(6)(b)(7)(C) stated he had spoken to Mr. (b)(6)(b)(7)(C) about 3-4 times since 15 Jun 10, when he first had contact with Mr. (b)(6)(b)(7)(C)

About 1055, 4 Aug 10, SA (b)(6)(b)(7)(C) assisted SA (b)(6)(b)(7)(C) FBI, Springfield, MA, by attempting extraction of data from the cellular phone of Mr. (b)(6)(b)(7)(C) utilizing the Cellebrite Universal Forensic Extraction Device (UFED).

Cellular Phone Make/Model: LG CU720
Cellular Phone Serial Number: 812KPVH176263
Cellular Phone IMEI: 011783-00-176263-0
SIM: 89014103212383744655

The phone did not contain a MicroSD card. Data was extracted from the SIM using the Cellebrite UFED. Data could not be extracted from the phone, as the Cellebrite was unable to communicate with the phone. The contacts of the phone's data port appeared worn. The contacts were cleaned, however, the Cellebrite was still unable to communicate with the phone.

About 0845, 5 Aug 10, SA (b)(6)(b)(7)(C) reviewed the documents, inclusive of emails and chat logs, pertaining to Mr (b)(6)(b)(7)(C) that were provided by SA (b)(6)(b)(7)(C) on 4 Aug 10. Contained in the documents was a letter, which appeared to be from Mr. (b)(6)(b)(7)(C) to SA (b)(6)(b)(7)(C) Also contained within the documents were chat logs and emails. The email traffic included what appeared to be communication between "(b)(6)(b)(7)(C)@sunshinepress.org" (associated to name "Julian Assange") and "(b)(6)(b)(7)(C)@guardian.co.uk" (associated to name "(b)(6)(b)(7)(C) dated 29 Aug 08, that was forwarded to (b)(6)(b)(7)(C) @gmail.com" by "(b)(6)(b)(7)(C)@wikileaks.org". Within the traffic, the individual using the (b)(6)(b)(7)(C) account asked of the individual using the Julian Assange account if he was able to "get a buyer for the (b)(6)(b)(7)(C) stuff yet". The individual using the Julian Assange account responded that "Wikileaks is still negotiating terms and conditions with the prospective participants." The individual using the Julian Assange account also stated that "Wikileaks is experimenting with auction-type mechanisms". The Instant Messenger (IM) traffic included traffic between the usernames (b)(6)(b)(7)(C) and (b)(6)(b)(7)(C) Numerous IM sessions were provided which were dated 29 Aug 08. Between 0212 and 0230, the traffic referenced bidding on 430 megabytes (MB) of compressed email, and a total of 1-2 terabytes (TB) of data consisting of classified reports, and messages to (b)(6)(b)(7)(C) other diplomats, and agents. During IM exchange between 2005 and 2035, redbuixx disclosed he was from Houston, TX. Also, during the IM exchange in this timeframe, (b)(6)(b)(7)(C) solicits (b)(6)(b)(7)(C) for assistance in running a server, which would be hosting information related to corruption, ethics, arms, etc. Between 2302 and 2319, the traffic referenced auctions and "$500k USD".

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE (b)(6)(b)(7)(C)	DATE 9 Aug 10	EXHIBIT 128

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

About 1709, 6 Aug 10, SA (b)(6)(b)(7)(C) collected as evidence one hard drive, containing purported EnCase images pertaining to hard drives of Mr (b)(6)(b)(7)(C) which was documented on Evidence/Property Custody Document (EPCD), Document Number (DN) 113 -10.

AGENT's COMMENT: SA (b)(6)(b)(7)(C) FBI, provided photo copies of the hard drive labels from Mr. (b)(6)(b)(7)(C) computer.

About 1119, 9 Aug 10, SA (b)(6)(b)(7)(C) collected as evidence one CD, containing an EnCase Logical Evidence File of the SIM card data obtained with the Cellebrite UFED of SIM card 89014103212383744655, obtained from cellular phone LG CU720, serial number 812KPVH176263, property of Mr. (b)(6)(b)(7)(C) EPCD, DN 114-10.

//LAST ENTRY//

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION
SA (b)(6)(b)(7)(C), (b) (7)(E)	Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060
SIGNATURE (b)(6)(b)(7)(C)	DATE: 9 Aug 10 / EXHIBIT: 128

Exhibit(s) 129

Page(s) 000902 thru 000929 referred to:

Federal Bureau of Investigation
Record Information/Dissemination Section
170 Marcel Drive
Winchester, Virginia 22602-4843

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

About 1438, 9 Aug 10, SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) National Security Agency (NSA), 9800 Savage Road, Fort Meade, MD 20755, interviewed Senior Airman (SrA) (b)(6)(b)(7)(C) 29th Intelligence Squadron, 9801 Love Road, Fort Meade, MD 20755, as he was identified as having worked with PFC MANNING between Nov 09 and Jan 10, while assigned at Forward Operating Base (FOB) Hammer, Iraq. SrA (b)(6)(b)(7)(C) stated he was assigned in Iraq between Jul 09 and Jan 10, as part of an element known as Cryptological Support Team 5 (CST5). SrA (b)(6)(b)(7)(C) aid he was initially assigned at FOB Loyalty, but was later transferred to FOB Hammer. SrA (b)(6)(b)(7)(C) explained he originally worked with members of the 3rd Brigade Combat Team (BCT) of the 82nd Airborne Division, as part of an NSA support element embedded with the 3rd BCT organic intelligence unit assigned to FOB Hammer. SrA (b)(6)(b)(7)(C) said while working with the 3rd BCT he remarked at this unit's discipline and the noticeable difference when PFC MANNING's unit, 2nd BCT of the 10th Mountain Division arrived at FOB Hammer. SrA (b)(6)(b)(7)(C) provided several examples in which he related he heard and saw 2nd BCT personnel with iPods in the Fusion area of the Sensitive Compartmented Information Facility (SCIF), as well as personnel playing games on Secure Internet Protocol Router (SIPR) network computers. SrA (b)(6)(b)(7)(C) related a situation prior to the arrival of PFC MANNING's unit to Iraq, where members of the 3rd BCT were notified of the names of the soldiers from the 2nd BCT who would be replacing them. SrA (b)(6)(b)(7)(C) said two of the 3rd BCT personnel, which he remembered as SPC (b)(6)(b)(7)(C) (NFI) and/or SPC (b)(6)(b)(7)(C) (NFI), remarked they knew PFC MANNING and that PFC MANNING was reportedly involved in an incident either during Basic Training or Advanced Individual Training (AIT) where PFC MANNING reportedly stabbed or attempted to stab someone with a pencil. SrA (b)(6)(b)(7)(C) said he did not have any details of this incident and had only heard these comments second-hand from the aforementioned 82nd Airborne Division soldiers. SrA (b)(6)(b)(7)(C) also mentioned an incident that occurred while PFC MANNING was providing a briefing in front of other personnel who worked in the SCIF. SrA (b)(6)(b)(7)(C) said PFC MANNING apparently froze while talking and stood motionless for approximately two to three minutes while in front of the group he was briefing. SrA (b)(6)(b)(7)(C) remarked this was an unusual/odd thing to have witnessed, and that eventually someone in the briefing helped PFC MANNING continue with the presentation he was trying to give. SrA (b)(6)(b)(7)(C) related PFC MANNING's unit seemed to always put a Specialist (Pay Grade E-4) in charge during the night shift while there were four or five officers assigned to the day shift in the SCIF. SrA (b)(6)(b)(7)(C) explained he noted the 3rd BCT always seemed to have an officer assigned on the night shift which made things easier if problems occurred. SrA (b)(6)(b)(7)(C) related another incident where PFC MANNING allegedly kicked or threw a computer and/or computer monitor off of a desk after being asked to do something by another unit member. SrA (b)(6)(b)(7)(C) said he believed PFC MANNING was given two days of quarters after hurting his neck when personnel had to restrain him during this incident. SrA (b)(6)(b)(7)(C) stated he believed PFC (b)(6)(b)(7)(C) 10th Mountain Division, FOB Hammer, Iraq, APO AE 09308, who was a member of PFC MANNING's unit, was someone that should be interviewed based on some of PFC (b)(6)(b)(7)(C) own behavior. SrA (b)(6)(b)(7)(C) mentioned PFC (b)(6)(b)(7)(C) had been put on some type of suicide watch for approximately two or three weeks after PFC (b)(6)(b)(7)(C) unit arrived in Iraq. SrA (b)(6)(b)(7)(C) explained PFC (b)(6)(b)(7)(C) was allowed to return to work at some point, but PFC (b)(6)(b)(7)(C) didn't work in the SCIF. SrA (b)(6)(b)(7)(C) said he believed PFC (b)(6)(b)(7)(C) had also been

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SI (b)(6)(b)(7)(C)	DATE 9 Aug 10	EXHIBIT 130

FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE

DETAILS

involved in some type of incident at Fort Drum prior to his unit deploying to Iraq, and that PFC (b)(6)(b)(7)(C) was reportedly implicated in some type of computer hacking activity. SrA (b)(6)(b)(7)(C) said although PFC (b)(6)(b)(7)(C) did not work in the SCIF, he would come into the SCIF to participate in the daily change-over briefings which occurred between the day and night shift personnel. SrA (b)(6)(b)(7)(C) said PFC (b)(6)(b)(7)(C) also appeared to be working in the role of an Intelligence Analyst. SrA (b)(6)(b)(7)(C) related, when asked how PFC MANNING may know information about NSA systems, that PFC MANNING probably learned about this information from the information mentioned in the daily shift-change briefings. SrA (b)(6)(b)(7)(C) said he did not believe that anyone from CST5 really spoke with or was friends with PFC MANNING, and that CST5 personnel only interacted with PFC MANNING while working in the SCIF. SrA (b)(6)(b)(7)(C) said he did not know about the Internet chat encryption application called "OTR" or "Off The Record"; that he never had any conversations with PFC MANNING in which they discussed the NSA or the iPhone; and although he has knowledge of the Foreign Intelligence Surveillance Act (FISA) for his job, he did not hear or remember anyone discussing FISA information with PFC MANNING. SrA (b)(6)(b)(7)(C) could not immediately provide any additional information related to PFC MANNING.

AGENT'S COMMENT: SrA (b)(6)(b)(7)(C) was asked about the Internet chat application "OTR" also referred to as "Off The Record", certain NSA database systems, intelligence related discussions involving NSA's abilities to eaves drop on calls made from iPhone devices, and the topic of FISA – as these were all subjects which PFC MANNING mentioned in Internet chat conversations PFC MANNING had with Mr. (b)(6)(b)(7)(C) Further, PFC MANNING in his chat conversations with Mr. (b)(6)(b)(7)(C) referred to an unidentified individual associated with NSA, who was very talkative and gave the impression they may have mentioned some or all of this information to PFC MANNING. Based on a review of the Internet chat logs between PFC MANNING and Mr. (b)(6)(b)(7)(C) and the circumstances of NSA affiliate personnel being assigned in Iraq with PFC MANNING, a working theory was that PFC MANNING may have learned this knowledge of these subject areas from a member of CST5.

// **LAST ENTRY** //

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIG (b)(6)(b)(7)(C)	DATE 9 Aug 10	EXHIBIT 130

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID-10117

DETAILS

About 0930, 11 Aug 10, SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) coordinated with 1LT (b)(6)(b)(7)(C) Bravo Company (B Co), 2nd Brigade Special Troop Battalion (2BSTB), 10th Mountain Division (10th Mtn Div), Fort Drum, NY 13602 (FDNY), and identified the following soldiers as Prophet operators while deployed in Iraq and also conducted canvass interviews of the soldiers:

1. 1LT (b)(6)(b)(7)(C) B Co, 2 BSTB, 10th Mtn Div, FDNY;

2. SFC (b)(6)(b)(7)(C) B Co, 2 BSTB, 10th Mtn Div, FDNY;

3. SSG (b)(6)(b)(7)(C) B Co, 2 BSTB, 10th Mtn Div, FDNY

4. SSG (b)(6)(b)(7)(C) B Co, 2 BSTB, 10th Mtn Div, FDNY - SSG (b)(6)(b)(7)(C) stated he once saw PFC MANNING watching a video depicting gun camera footage taken what he thought from an helicopter on his government-issued Secure Internet Protocol Router (SIPR) laptop computer in the Sensitive Compartmented Information Facility (SCIF) in the early morning hours of an unknown date;

5. SSG (b)(6)(b)(7)(C) B Co, 2 BSTB, 10th Mtn Div, FDNY;

6. SGT (b)(6)(b)(7)(C) B Co, 2 BSTB, 10th Mtn Div, FDNY;

7. SGT (b)(6)(b)(7)(C) B Co, 2 BSTB, 10th Mtn Div, FDNY;

8. SGT (b)(6)(b)(7)(C) B Co, 2 BSTB, 10th Mtn Div, FDNY;

9. SPC (b)(6)(b)(7)(C) B Co, 2 BSTB, 10th Mtn Div, FDNY;

10. SPC (b)(6)(b)(7)(C) B Co, 2 BSTB, 10th Mtn Div, FDNY;

11. SGT (b)(6)(b)(7)(C) B Co, 2 BSTB, 10th Mtn Div, FDNY;

12. SPC (b)(6)(b)(7)(C) B Co, 2 BSTB, 10th Mtn Div, FDNY;

13. PFC (b)(6)(b)(7)(C) B Co, 2 BSTB, 10th Mtn Div, FDNY; and

14. SPC (b)(6)(b)(7)(C) B Co, 2 BSTB, 10th Mtn Div, FDNY.

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
(b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE (b)(6)(b)(7)(C), (b) (7)(E)	DATE 11 Aug 10	EXHIBIT 131

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID-10117

DETAILS

The majority of canvassed soldiers worked in the same SCIF as PFC MANNING, but in a different section – Signal Intelligence (SIGINT) shop, and would only interact with PFC MANNING on work-related business or during turn-over briefings. Some of those canvassed either heard or witnessed PFC MANNING losing his composure and military bearing and flipping tables while he was being counseled for arriving late at work and/or PFC MANNING assaulting SPC (b)(6)(b)(7)(C) S-2, Headquarters and Headquarters Company (HHC), 2 BCT, 10th Mtn Div. It was reported by those canvassed that there was no Joint Worldwide Intelligence Communications System (JWICS) present in SCIF during the majority of their deployment (Oct 09 – Aug 10); B Co's predecessor 3/82nd had a JWICS connection in the SCIF prior to 10th Mtn Div's arrival, but only for a short period of time during Relief in Place and Transfer of Authority (RIP TOA). ///LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE (b)(6)(b)(7)(C), (b) (7)(E)	DATE 11 Aug 10	EXHIBIT 131

DATE: 11 AUG 10 TIME: 0950

0028-10-CID221-10117
AGENT(S):

(b)(6)(b)(7)(C) CANVASS INTERVIEW WORKSHEET

NAME: (b)(6)(b)(7)(C) RANK: SGT SSN: (b)(6)(b)(7)(C)

UNIT/ADDRESS: B Co 2BSTB 2/10 MTN DIV

TELEPHONE: (b)(6)(b)(7)(C) AKO E-MAIL ADDRESS: (b)(6)(b)(7)(C)@us.army.mil

1. Do you know who PFC Bradley E. MANNING is?
   Yes. SPC (b)(6)(b)(7)(C) was @ 2 or 3 meetings I introduced @ the meeting.
2. Did you work with PFC MANNING?
   No.
3. When did you arrive in Iraq?
   around 15 Oct 09, that might be arrival in Kuwait.
4. When did PFC MANNING arrive in Iraq?
   I don't know.
5. Where did PFC MANNING work and what hours?
   In the fusion room of the main scif. I don't know the hours he worked
6. Where did you work and what hours?
   Hours varied by time of year.
   I worked in a language specific scif-annex in another building.
7. With whom did PFC MANNING work?
   I think brigade fusion.
8. Do you know or have you heard and/or witnessed of any incident involving PFC MANNING?
   Yes, I heard he punched a SPC (b)(6)(b)(7)(C)
9. Do you know who (b)(6)(b)(7)(C) is?
   Yes, I met him a couple times.
10. Do you know who (b)(6)(b)(7)(C) is?
    No.

11. Do you know who a U.S. Marine named (b)(6)(b)(7)(C) is?
He worked in the main scif.

12. Did you have access to JWICS or Prophet?
No.

13. Did PFC MANNING have access to JWICS or Prophet?
I don't know. He had no access to the language annex.

14. Do you know of anyone who tried to get JWICS installed in the SCIF?
No.

15. Can you identify any NSA personnel assigned to the SCIF between January 2010 and the end of your deployment?
No.

16. Did PFC MANNING have a friend, who worked for NSA?
I don't know.

17. Was there anyone, who was obviously outspoken about the war or openly expressed negative thoughts and opinions?
No.

18. Do you know who (b)(6)(b)(7)(C) is?
It could be the Army base of Nwachuca of HUMINT.

19. Did you ever witness PFC MANNING mention or watch any videos titled "Collateral Murder" and/or any other videos depicting gun camera footage taken by an Apache helicopter in Iraq?
No.

20. Have you received e-mails, attachments, digital media devices, packages from PFC MANNING and vice versa?
No.

21. Have you ever allowed PFC MANNING to use your personal and/or U.S. Government owned computer(s)?
No.

22. Is there anything else you would like to add?
No.

DATE: 11 AUG 2010 TIME: 0955

0028-10-CID221-10117
AGENT(S):

CANVASS INTERVIEW WORKSHEET

NAME: SGT (b)(6)(b)(7)(C) SGT SSN: (b)(6)(b)(7)(C)

UNIT/ADDRESS: (b)(6)(b)(7)(C)

TELEPHONE: (b)(6)(b)(7)(C) AKO E-MAIL ADDRESS: (b)(6)(b)(7)(C)@us.army.mil

1. Do you know who PFC Bradley E. MANNING is? Yes. (b)(6)(b)(7)(C), he worked in S2/in SCIF

2. Did you work with PFC MANNING? Loosely, but yes. (b)(6)(b)(7)(C) saw him pass & brief. Never worked directly.

3. When did you arrive in Iraq? 5 OCT 2009

4. When did PFC MANNING arrive in Iraq? OCT 2009?

5. Where did PFC MANNING work and what hours? S-2 And a variety of hours, mostly 12s (hours) later 9s

6. Where did you work and what hours? In the back room - with SIGINT - mostly day shift 0800 - 2200 from NOV 09 - APR 10 Then night shift 22-1000 from APR 2010 - JUL 2010

7. With whom did PFC MANNING work? SSG (NOW MSG) (b)(6)(b)(7)(C) → HHC

8. Do you know or have you heard and/or witnessed of any incident involving PFC MANNING? Yes, I have heard/witnessed 1 incident of him yelling/overturning a desk, heard of him attacking SPC (b)(6)(b)(7)(C) and heard of him passing SIPR stuff from NIPR

9. Do you know who (b)(6)(b)(7)(C) is? Yes. ACST Soldier/SrA

10. Do you know who (b)(6)(b)(7)(C) is? Yes. ACST TSGT → Maps person

DATE: TIME:

[redacted] 11 Aug 10 0955

0028-10-CID221-10117
AGENT(S):

11. Do you know who a U.S. Marine named [redacted] is?
Yes. A CST DNI soldier

12. Did you have access to JWICS or Prophet? Prophet

13. Did PFC MANNING have access to JWICS or Prophet? No

14. Do you know of anyone who tried to get JWICS installed in the SCIF? Yes. CW2 [redacted] was interested in installing JWICS

15. Can you identify any NSA personnel assigned to the SCIF between January 2010 and the end of your deployment? Yes, MS [redacted], SPC [redacted], SSGT [redacted] MSG. [redacted] SSG [redacted]

16. Did PFC MANNING have a friend, who worked for NSA? Not that I know of.

17. Was there anyone, who was obviously outspoken about the war or openly expressed negative thoughts and opinions? No.

18. Do you know who [redacted] is? Yes, a Humint soldier

19. Did you ever witness PFC MANNING mention or watch any videos titled "Collateral Murder" and/or any other videos depicting gun camera footage taken by an Apache helicopter in Iraq? No.

20. Have you received e-mails, attachments, digital media devices, packages from PFC MANNING and vice versa? I don't think so, but he might have sent out one of the morning update slides from S2

21. Have you ever allowed PFC MANNING to use your personal and/or U.S. Government owned computer(s)? Never

22. Is there anything else you would like to add? He was a loner, purposely didn't shower, and probably gay.

DATE: 11 AUG TIME: 1000

0028-10-CID221-10117
AGENT(S):

CANVASS INTERVIEW WORKSHEET

NAME: (b)(6)(b)(7)(C) RANK: SPC SSN: (b)(6)(b)(7)(C)

UNIT/ADDRESS: B Co 2BSTB 10DMTN DIV

TELEPHONE: (b)(6)(b)(7)(C) AKO E-MAIL ADDRESS: (b)(6)(b)(7)(C) @us.army.mil

1. Do you know who PFC Bradley E. MANNING is?

   YES ; Know of him / Saw a couple of times

2. Did you work with PFC M[redacted]?

   NO

3. When did you arrive in Iraq?

   OCT '09

4. When did PFC MANNING arrive in Iraq?

   DON'T KNOW

5. Where did PFC MANNING work and what hours?

   BRIGADE SCIF, DON'T KNOW HOURS

6. Where did you work and what hours?

   AT THE TIME PFC MANNING WAS THERE, I WAS AT JSS ROYALTY

7. With whom did PFC MANNING work?

   DON'T KNOW

8. Do you know or have you heard and/or witnessed of any incident involving PFC MANNING?

   I'VE HEARD ABOUT THE NEWS

9. Do you know who (b)(6)(b)(7)(C) is?

   NO

10. Do you know who (b)(6)(b)(7)(C) is?

    NO

11. Do you know who a U.S. Marine named (b)(6)(b)(7)(C) is?

No

12. Did you have access to JWICS or Prophet (b)(6)(b)(7)(C)

YES

13. Did PFC MANNING have access to JWICS or Prophet?

DON'T KNOW

14. Do you know of anyone who tried to get JWICS installed in the SCIF?

No

15. Can you identify any NSA personnel assigned to the SCIF between January 2010 and the end of your deployment? WO1 (b)(6)(b)(7)(C)
SPC (b)(6)(b)(7)(C)

16. Did PFC MANNING have a friend, who worked for NSA?

DON'T KNOW

17. Was there anyone, who was obviously outspoken about the war or openly expressed negative thoughts and opinions?

NO

18. Do you know who (b)(6)(b)(7)(C) is?
IF THIS IS (b)(6)(b)(7)(C) THEN YES; Same Room as Prophet SCIF

19. Did you ever witness PFC MANNING mention or watch any videos titled "Collateral Murder" and/or any other videos depicting gun camera footage taken by an Apache helicopter in Iraq?

No

20. Have you received e-mails, attachments, digital media devices, packages from PFC MANNING and vice versa?

No

21. Have you ever allowed PFC MANNING to use your personal and/or U.S. Government owned computer(s)?

No

22. Is there anything else you would like to add?

NO

DATE: TIME:

11AUG10 1003

0028-10-CID221-10117
AGENT(S):

CANVASS INTERVIEW WORKSHEET

NAME: (b)(6)(b)(7)(C) RANK: 1LT SSN: (b)(6)(b)(7)(C)

UNIT/ADDRESS: B Co. 2BSTB, 10 MTN DIV

TELEPHONE: (b)(6)(b)(7)(C)

AKO E-MAIL ADDRESS: (b)(6)(b)(7)(C)@us.army.mil

1. Do you know who PFC Bradley E. MANNING is?
   Yes, (b)(6)(b)(7)(C) professional acquaintance. - Not Personal / Never had Personal Conversation any work-related.
2. Did you work with PFC MANNING?
   Yes. (b)(6)(b)(7)(C) Same SCIF, but different section
3. When did you arrive in Iraq?
   October 2009
4. When did PFC MANNING arrive in Iraq?
   October 2009
5. Where did PFC MANNING work and what hours?
   BCT SCIF, night shift (2200-1000)
   (beginning of deployment was on dayshift)
6. Where did you work and what hours?
   BCT SCIF, SIGINT shop
7. With whom did PFC MANNING work?
   BCT S2 Analysts
8. Do you know (b)(6)(b)(7)(C) or have you heard and/or witnessed of any incident involving PFC MANNING?
   Yes (3) flipped table / flipped showman
9. Do you know who (b)(6)(b)(7)(C) is?
   Yes (b)(6)(b)(7)(C) e-mail
10. Do you know (b)(6)(b)(7)(C) is?
    Yes e-mail

11. Do you know who a U.S. Marine named [redacted] is?

Yes [redacted] e-mail [redacted]

12. Did you have access to JWICS or Prophet?

Yes (our BCT did not run JWICS) NSAnet

13. Did PFC MANNING have access to JWICS or Prophet?

No

14. Do you know of anyone who tried to get JWICS installed in the SCIF?

Yes; [redacted] CWS [redacted]

15. Can you identify any NSA personnel assigned to the SCIF between January 2010 and the end of your deployment?

Yes, they were assigned to support my platoon. [redacted] e-mail

16. Did PFC MANNING have a friend, who worked for NSA?

I do not know

17. Was there anyone, who was obviously outspoken about the war or openly expressed negative thoughts and opinions?

I don't know

18. Do you know who [redacted] is?

Yes; Human [redacted] 2BTSB

19. Did you ever witness PFC MANNING mention or watch any videos titled "Collateral Murder" and/or any other videos depicting gun camera footage taken by an Apache helicopter in Iraq?

I can't remember specifically

20. Have you received e-mails, attachments, digital media devices, packages from PFC MANNING and vice versa?

Yes, on SIPR during deployment [redacted] - Work Related / Mostly personal
- CIDNE Data

21. Have you ever allowed PFC MANNING to use your personal and/or U.S. Government owned computer(s)?

NO

22. Is there anything else you would like to add?

[redacted] No

DATE: 11 Aug 10 TIME: 1005 (b)(6)(b)(7)(C)

0028-10-CID221-10117
AGENT(S):

CANVASS INTERVIEW WORKSHEET

NAME: (b)(6)(b)(7)(C) RANK: SGT SSN: (b)(6)(b)(7)(C)

UNIT/ADDRESS: B Co 2BSTB 10 MTN

TELEPHONE: (b)(6)(b)(7)(C) AKO E-MAIL ADDRESS: (b)(6)(b)(7)(C) us.army.mil

1. Do you know who PFC Bradley E. MANNING is?
   Yes; heard thru Co-workers (b)(6)(b)(7)(C)
   Not a friend
2. Did you work with PFC MANNING?
   no
3. When did you arrive in Iraq?
   Oct 09
4. When did PFC MANNING arrive in Iraq?
   Oct 09
5. Where did PFC MANNING work and what hours? (b)(6)(b)(7)(C)
   S-2 shop
6. Where did you work and what hours?
   Language analyst daylight
7. With whom did PFC MANNING work?
   everyone in the front of the S-2 shop
8. Do you know or have you heard and/or witnessed of any incident involving PFC MANNING?
   Yes, just read on News (b)(6)(b)(7)(C)
9. Do you know who (b)(6)(b)(7)(C) is?
   no
10. Do you know who (b)(6)(b)(7)(C) is?
    no

11. Do you know who a U.S. Marine named (b)(6)(b)(7)(C) is?
no

12. Did you have access to JWICS or Prophet?
Yes (b)(6)(b)(7)(C)

13. Did PFC MANNING have access to JWICS or Prophet?
I don't know

14. Do you know of anyone who tried to get JWICS installed in the SCIF?
no

15. Can you identify any NSA personnel assigned to the SCIF between January 2010 and the end of your deployment? don't know names

16. Did PFC MANNING have a friend, who worked for NSA?
I don't know

17. Was there anyone, who was obviously outspoken about the war or openly expressed negative thoughts and opinions?
no

18. Do you know who (b)(6)(b)(7)(C) is?
no

19. Did you ever witness PFC MANNING mention or watch any videos titled "Collateral Murder" and/or any other videos depicting gun camera footage taken by an Apache helicopter in Iraq?
no

20. Have you received e-mails, attachments, digital media devices, packages from PFC MANNING and vice versa?
no

21. Have you ever allowed PFC MANNING to use your personal and/or U.S. Government owned computer(s)?
no

22. Is there anything else you would like to add? no

DATE: 11 Aug 2010 TIME: 1005

0028-10-CID221-10117
AGENT(S):

CANVASS INTERVIEW WORKSHEET

NAME: (b)(6)(b)(7)(C) RANK: SPC SSN (b)(6)(b)(7)(C)

UNIT/ADDRESS: B. Co., 2BSTB, 2BCT, 10121 North River Ridge Loop, Fort Drum, NY 13602

TELEPHONE: (b)(6)(b)(7)(C) AKO E-MAIL ADDRESS: (b)(6)(b)(7)(C) us.army.mil

1. Do you know wh(b)(6)(b)(7)(C)radley E. MANNING is?
Yes (b)(6)(b)(7)(C) - worked in Sare SCIF saw him once outside stood out; PFC (b)(6)(b)(7)(C) stated he would [illegible]
- Noe a personal friend

2. Did you work with PFC MANNING?
Yes

3. When did you arrive in Iraq?
October 14, 2009

4. When did PFC MANNING arrive in Iraq?
I dont remember

5. Where did PFC MANNING work and what hours?
He worked in the Brigade SCIF. At ~~first~~ first he worked nights (2200 - 1000). But because he seemed to be a problem his work scheduled changed to days (1000-2200).

6. Where did you work and what hours?
I worked in the second part of the Brigade SCIF. I worked nights (2200 - 1000) for most of the deployment.

7. With whom did PFC MANNING work?
MSG (b)(6)(b)(7)(C), SPC (b)(6)(b)(7)(C), 1LT (b)(6)(b)(7)(C), SFC (b)(6)(b)(7)(C), SPC (b)(6)(b)(7)(C)

8. Do you know or have you heard and/or witnessed of any incident involving PFC MANNING?
I only heard about his incidents with SPC (b)(6)(b)(7)(C) and SPC (b)(6)(b)(7)(C)

9. Do you know who (b)(6)(b)(7)(C) is?
Yes

10. Do you know who (b)(6)(b)(7)(C) is?
(b)(6)(b)(7)(C) Yes
W/ (b)(6)(b)(7)(C) @ 2200-100
with (b)(6)(b)(7)(C) /SPC (b)(6)(b)(7)(C) NCOIC

EXHIBIT 132
000944

11. Do you know who a U.S. Marine named (b)(6)(b)(7)(C) is?

Yes

12. Did you have access to JWICS or Prophet (b)(6)(b)(7)(C)

Yes, I'm not sure about JWICS access.

13. Did PFC MANNING have access to JWICS or Prophet?

No.

14. Do you know of anyone who tried to get JWICS installed in the SCIF?

Yes, CW1 (b)(6)(b)(7)(C) wanted 1LT (b)(6)(b)(7)(C) to give him and SPC (b)(6)(b)(7)(C) access, but 1LT (b)(6)(b)(7)(C) refused because they had OPSEC issues.

15. Can you identify any NSA personnel assigned to the SCIF between January 2010 and the end of your deployment? Yes, if you are asking about Sgt (b)(6)(b)(7)(C) or SrSgt (b)(6)(b)(7)(C)

16. Did PFC MANNING have a friend, who worked for NSA?

Not that I knew of.

17. Was there anyone, who was obviously outspoken about the war or openly expressed negative thoughts and opinions? No

18. Do you know who (b)(6)(b)(7)(C) is?

I know (b)(6)(b)(7)(C) who worked for SSA for a while.

19. Did you ever witness PFC MANNING mention or watch any videos titled "Collateral Murder" and/or any other videos depicting gun camera footage taken by an Apache helicopter in Iraq?

No

20. Have you received e-mails, attachments, digital media devices, packages from PFC MANNING and vice versa? In Iraq over SIPR. But it was all work related.

21. Have you ever allowed PFC MANNING to use your personal and/or U.S. Government owned computer(s)? No.

22. Is there anything else you would like to add? No.

(b)(6)(b)(7)(C) TE: 14 May 10 TIME: 1010

0028-10-CID221-10117
AGENT(S):

CANVASS INTERVIEW WORKSHEET

NAME: (b)(6)(b)(7)(C) RANK: SFC SSN: (b)(6)(b)(7)(C)

UNIT/ADDRESS: B Co 2BSTB

TELEPHONE: (b)(6)(b)(7)(C) AKO E-MAIL ADDRESS: (b)(6)(b)(7)(C) @us.army.mil

1. Do you know who PFC Bradley E. MANNING is? Former BDE analyst for 2-10 now charged with leaking classified information
2. Did you work with PFC MANNING? NO
3. When did you arrive in Iraq? 31 OCT 2009.
4. When did PFC MANNING arrive in Iraq? UNKNOWN
5. Where did PFC MANNING work and what hours? He worked in BDE S-2 and mostly worked nights as an Intel Analyst
6. Where did you work and what hours? I am the SIGNT/Prophet Platoon Sergeant and I worked in multiple locations and times to support the platoon
7. With whom did PFC MANNING work? CW2 (b)(6)(b)(7)(C), 1LT (b)(6)(b)(7)(C), MSG (b)(6)(b)(7)(C), SPC (b)(6)(b)(7)(C), SPC (b)(6)(b)(7)(C), SPC (b)(6)(b)(7)(C), SPC (b)(6)(b)(7)(C), SPC (b)(6)(b)(7)(C), CW2 (b)(6)(b)(7)(C)
8. Do you know or have you heard and/or witnessed of any incident involving PFC MANNING? I am only aware of an incident where PFC manning physically assaulted SPC (b)(6)(b)(7)(C)
9. Do you know who (b)(6)(b)(7)(C) is? SRA (Air Force) He was a NSA Cryptologic Support Augmentee who worked in the brigade SIGNT cell.
10. Do you know who (b)(6)(b)(7)(C) is? (TSGT)(USAF) He was a NSA Cryptologic Support Augmentee who worked in the SIGNT Cell

11. Do you know who a U.S. Marine named (b)(6)(b)(7)(C) is?
He was an NSA CSY Augmentee who worked as a DNI analyst

12. Did you have access to JWICS or Prophet? NO

13. Did PFC MANNING have access to JWICS or Prophet? NO

14. Do you know of anyone who tried to get JWICS installed in the SCIF? NO

15. Can you identify any NSA personnel assigned to the SCIF between January 2010 and the end of your deployment? WO1 (b)(6)(b)(7)(C), SPC (b)(6)(b)(7)(C)
SSgt (b)(6)(b)(7)(C) (USAF), SSgt (b)(6)(b)(7)(C) (USAF)

16. Did PFC MANNING have a friend, who worked for NSA? Not to my knowledge

17. Was there anyone, who was obviously outspoken about the war or openly expressed negative thoughts and opinions? NO

18. Do you know who (b)(6)(b)(7)(C)s? that is a nickname for
SPC (b)(6)(b)(7)(C)

19. Did you ever witness PFC MANNING mention or watch any videos titled "Collateral Murder" and/or any other videos depicting gun camera footage taken by an Apache helicopter in Iraq? NO

20. Have you received e-mails, attachments, digital media devices, packages from PFC MANNING and vice versa? NO

21. Have you ever allowed PFC MANNING to use your personal and/or U.S. Government owned computer(s)? NO

22. Is there anything else you would like to add? NO

DATE: 4 Aug 10 TIME: 1010

0028-10-CID221-10117
AGENT(S):

CANVASS INTERVIEW WORKSHEET

NAME: (b)(6)(b)(7)(C) RANK: SGT/E-5 SSN: (b)(6)(b)(7)(C)

UNIT/ADDRESS: B co 2BSTB

TELEPHONE (b)(6)(b)(7)(C) AKO E-MAIL ADDRESS: (b)(6)(b)(7)(C) @us.army.mil

1. Do you know who PFC Bradley E. MANNING is?

   Yes, but only by name and where he worked

2. Did you work with PFC MANNING?

   No

3. When did you arrive in Iraq?

   Oct 09

4. When did PFC MANNING arrive in Iraq?

   Not Sure

5. Where did PFC MANNING work and what hours?

   Not Sure

6. Where did you work and what hours?

   JSS loyalty 24-7

7. With whom did PFC MANNING work?

   Brigade S-2 shop

8. Do you know or have you heard and/or witnessed of any incident involving PFC MANNING?

   I know about the incident, but was not present for it. (b)(6)(b)(7)(C) told me about it.

9. Do you know who (b)(6)(b)(7)(C) is?

   Yes, I worked with him for a few days while I was at FOB Hammer

10. Do you know who (b)(6)(b)(7)(C) is?

    No

11. Do you know who a U.S. Marine named (b)(6)(b)(7)(C) is?

Yes, he worked in the SCIF

12. Did you have access to JWICS or Prophet?

No, No JWICS access through our equipment

13. Did PFC MANNING have access to JWICS or Prophet?

Not that I know of

14. Do you know of anyone who tried to get JWICS installed in the SCIF?

No

15. Can you identify any NSA personnel assigned to the SCIF between January 2010 and the end of your deployment?

A few, I never spent significant time in this office

16. Did PFC MANNING have a friend, who worked for NSA?

I do not know

17. Was there anyone, who was obviously outspoken about the war or openly expressed negative thoughts and opinions?

No

18. Do you know who (b)(6)(b)(7)(C) is?

No

19. Did you ever witness PFC MANNING mention or watch any videos titled "Collateral Murder" and/or any other videos depicting gun camera footage taken by an Apache helicopter in Iraq?

No

20. Have you received e-mails, attachments, digital media devices, packages from PFC MANNING and vice versa?

No

21. Have you ever allowed PFC MANNING to use your personal and/or U.S. Government owned computer(s)?

No

22. Is there anything else you would like to add?

No

(b)(6)(b)(7)(C) DATE: 11 Aug 10 TIME: 1015

0028-10-CID221-10117
AGENT(S):

CANVASS INTERVIEW WORKSHEET

NAME: (b)(6)(b)(7)(C) RANK: SSG SSN: (b)(6)(b)(7)(C)

UNIT/ADDRESS: bco, 2/10 MTN DIV

TELEPHONE: (b)(6)(b)(7)(C) AKO E-MAIL ADDRESS: (b)(6)(b)(7)(C)@us.army.mil

1. Do you know who PFC Bradley E. MANNING is?
   Yes (b)(6)(b)(7)(C) worked in the same SCIF worked in SIGINT side
2. Did you work with PFC MANNING?
   Yes Shift changes & processing setup.
3. When did you arrive in Iraq?
   OCT 09
4. When did PFC MANNING arrive in Iraq?
   OCT 09
5. Where did PFC MANNING work and what hours?
   BDE SCIF - at first he worked 2200-1000 shift but was switched back and forth between 1000-2200 & 2200-1000
6. Where did you work and what hours?
   BDE SCIF - 1000-2200
7. With whom did PFC MANNING work?
   with ~~35Es~~ analysts in the SCIF - ~~SPC Patsett, SPC Shannon, ILT~~
8. Do you know or have you heard and/or witnessed of any incident involving PFC MANNING?
   witnessed an incident when manning was being counseled for being late, he tried to overturn a table and had to be restrained
   yes- I heard of several other incidents
9. Do you know who (b)(6)(b)(7)(C) is?
   yes
10. Do you know who (b)(6)(b)(7)(C) is?
    yes

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

11. Do you know who a U.S. Marine named (b)(6)(b)(7)(C) is?
yes

12. Did you have access to JWICS or Prophet?
yes

13. Did PFC MANNING have access to JWICS or Prophet?
no

14. Do you know of anyone who tried to get JWICS installed in the SCIF?
yes

15. Can you identify any NSA personnel assigned to the SCIF between January 2010 and the end of your deployment? yes (b)(6)(b)(7)(C) CST folks Mr. (b)(6)(b)(7)(C) DIC / SPC (b)(6)(b)(7)(C) / (b)(6)(b)(7)(C)

16. Did PFC MANNING have a friend, who worked for NSA?
Probably - do not have direct knowledge of his connections

17. Was there anyone, who was obviously outspoken about the war or openly expressed negative thoughts and opinions? no

18. Do you know who (b)(6)(b)(7)(C) is?
yes

19. Did you ever witness PFC MANNING mention or watch any videos titled "Collateral Murder" and/or any other videos depicting gun camera footage taken by an Apache helicopter in Iraq?
no

20. Have you received e-mails, attachments, digital media devices, packages from PFC MANNING and vice versa?
no

21. Have you ever allowed PFC MANNING to use your personal and/or U.S. Government owned computer(s)?
no

22. Is there anything else you would like to add?
there was a 2-4 week period when there was a JWICS laptop in the SCIF. IT belonged to 3/82nd ~~that~~ We never activated our JWICS.
(b)(6)(b)(7)(C) During RIP / advanced party

DATE: 11 May 10 TIME: 1020

0028-10-CID221-10117
AGENT(S):

CANVASS INTERVIEW WORKSHEET

NAME: (b)(6)(b)(7)(C) RANK: SSG SSN: (b)(6)(b)(7)(C)

UNIT/ADDRESS: B/2 BSTB

TELEPHONE (b)(6)(b)(7)(C) AKO E-MAIL ADDRESS: (b)(6)(b)(7)(C) @ us.army.mil

1. Do you know who PFC Bradley E. MANNING is? Yes

(b)(6)(b)(7)(C): knew who he was, Not a friend

2. Did you work with PFC MANNING? No

3. When did you arrive in Iraq? Oct '09

4. When did PFC MANNING arrive in Iraq? I assume the same time

5. Where did PFC MANNING work and what hours? COS Hammer SCIF. Don't know his hours but I saw him regularly at the 2200 Change brief.

6. Where did you work and what hours? Oct - Dec COS Hammer Language Annex 1000-2200
Jan - June '10 - JSS Loyalty SCIF - 24/7

7. With whom did PFC MANNING work? I don't know what section he worked for.

8. Do you know or have you heard and/or witnessed of any incident involving PFC MANNING?
Yes He attacked + got beaten up by SPC (b)(6)(b)(7)(C)
(b)(6)(b)(7)(C) Heard the incident

9. Do you know who (b)(6)(b)(7)(C) is? NO.

10. Do you know who (b)(6)(b)(7)(C) is? No.

11. Do you know who a U.S. Marine named (b)(6)(b)(7)(C) is? I think he was our SCIF's DNI specialist.

12. Did you have access to JWICS or (b)(6)(b)(7)(C) Prophet? Yes

13. Did PFC MANNING have access to JWICS or Prophet? Not prophet – JWICS, maybe

14. Do you know of anyone who tried to get JWICS installed in the SCIF? No. I wasn't involved in SCIF operations. I reported info to the SCIF.

15. Can you identify any NSA personnel assigned to the SCIF between January 2010 and the end of your deployment? A lady named (b)(6)(b)(7)(C) and later on Mr. (b)(6)(b)(7)(C)

16. Did PFC MANNING have a friend, who worked for NSA? I don't know.

17. Was there anyone, who was obviously outspoken about the war or openly expressed negative thoughts and opinions? No.

18. Do you know who (b)(6)(b)(7)(C) is? Are you talking about (b)(6)(b)(7)(C)? If so, yes. (b)(6)(b)(7)(C) @ BCO

19. Did you ever witness PFC MANNING mention or watch any videos titled "Collateral Murder" and/or any other videos depicting gun camera footage taken by an Apache helicopter in Iraq? No.

20. Have you received e-mails, attachments, digital media devices, packages from PFC MANNING and vice versa? No.

21. Have you ever allowed PFC MANNING to use your personal and/or U.S. Government owned computer(s)? No - he seemed to keep to himself.

22. Is there anything else you would like to add? No.

DATE: 11 Aug 10 TIME: 1025

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

0028-10-CID221-10117
AGENT(S):

CANVASS INTERVIEW WORKSHEET

NAME: (b)(6)(b)(7)(C) RANK: PFC SSN: (b)(6)(b)(7)(C)

UNIT/ADDRESS: 2d BSTB Late Deployer (b)(6)(b)(7)(C)

TELEPHONE: (b)(6)(b)(7)(C) AKO E-MAIL ADDRESS: (b)(6)(b)(7)(C)@us.army.mil

1. Do you know who PFC Bradley E. MANNING is?
   Yes (b)(6)(b)(7)(C) SCIF
   But worked @ SIGINT
2. Did you work with PFC MANNING?
   Not directly
3. When did you arrive in Iraq?
   09 Feb 10
4. When did PFC MANNING arrive in Iraq?
   I don't Know
5. Where did PFC MANNING work and what hours?
   BDE SCIF Varying hours
6. Where did you work and what hours?
   BDE SCIF 1000-2200
7. With whom did PFC MANNING work?
   BDE S2
8. Do you know or have you heard and/or witnessed of any incident involving PFC MANNING?
   Yes - heard about the Assault
   - Saw News (b)(6)(b)(7)(C)
9. Do you know who (b)(6)(b)(7)(C)s?
   NO
10. Do you know who (b)(6)(b)(7)(C) is?
    NO

11. Do you know who a U.S. Marine named (b)(6)(b)(7)(C) is?

NO

12. Did you have access to JWICS or Prophet? (b)(6)(b)(7)(C)

YeS

13. Did PFC MANNING have access to JWICS or Prophet?

NO

14. Do you know of anyone who tried to get JWICS installed in the SCIF?

NO

15. Can you identify any NSA personnel assigned to the SCIF between January 2010 and the end of your deployment?

Petty officer (b)(6)(b)(7)(C) Spc (b)(6)(b)(7)(C) + Mr (b)(6)(b)(7)(C)
Sgt (b)(6)(b)(7)(C)

16. Did PFC MANNING have a friend, who worked for NSA?

I don't Know

17. Was there anyone, who was obviously outspoken about the war or openly expressed negative thoughts and opinions?

NONe I Knew of

18. Do you know who (b)(6)(b)(7)(C) is?

(b)(6)(b)(7)(C) Yes, HUMINT @ B Co

19. Did you ever witness PFC MANNING mention or watch any videos titled "Collateral Murder" and/or any other videos depicting gun camera footage taken by an Apache helicopter in Iraq?

NO

20. Have you received e-mails, attachments, digital media devices, packages from PFC MANNING and vice versa?

NO

21. Have you ever allowed PFC MANNING to use your personal and/or U.S. Government owned computer(s)?

NO

22. Is there anything else you would like to add?

NO

DATE: 11 May 10 TIME: 1030

0028-10-CID221-10117
AGENT(S):

CANVASS INTERVIEW WORKSHEET

NAME: (b)(6)(b)(7)(C) RANK: SSG SSN: (b)(6)(b)(7)(C)

UNIT/ADDRESS: B Co, 2BSTB

TELEPHONE: (b)(6)(b)(7)(C) AKO E-MAIL ADDRESS: (b)(6)(b)(7)(C)@us.army.mil

1. Do you know who PFC Bradley E. MANNING is? Yes
(b)(6)(b)(7)(C) Work together @ Nite Shift PFC (b)(6)(b)(7)(C) work front / SSG (b)(6)(b)(7)(C) work back
2. Did you work with PFC MANNING? Yes
(b)(6)(b)(7)(C) Would have RFI
Not Ops related info given
3. When did you arrive in Iraq? Oct 09
4. When did PFC MANNING arrive in Iraq? ?
5. Where did PFC MANNING work and what hours? BDE S2, night shift SPC (b)(6)(b)(7)(C) either NCO counterpart in charge
(b)(6)(b)(7)(C) Nite
Mannix, One or two other people; can't recall NCOIC /
6. Where did you work and what hours? BDE S2, night shift
7. With whom did PFC MANNING work? BDE S2 and SIGINT team
8. Do you know or have you heard and/or witnessed of any incident involving PFC MANNING? Yes
(b)(6)(b)(7)(C)
- Witness assaulting SM (b)(6)(b)(7)(C)
- Late for work; given Counseling by (b)(6)(b)(7)(C); flipped the table
9. Do you know who (b)(6)(b)(7)(C) is? Yes
(b)(6)(b)(7)(C) - Sjint NSA CSG (b)(6)(b)(7)(C) Cryptologic Support Group. 6 months augmentee NSA
10. Do you know who (b)(6)(b)(7)(C) is? Yes
(b)(6)(b)(7)(C) NSA Imint CSG (b)(6)(b)(7)(C)

11. Do you know who a U.S. Marine named (b)(6)(b)(7)(C) is? yes
(b)(6)(b)(7)(C) NSA/DHI (b)(6)(b)(7)(C)

12. Did you have access to JWICS or Prophet? yes
(b)(6)(b)(7)(C)

13. Did PFC MANNING have access to JWICS or Prophet? no

14. Do you know of anyone who tried to get JWICS installed in the SCIF? yes
(b)(6)(b)(7)(C) Chief (b)(6)(b)(7)(C) (tall)
@ BDE

15. Can you identify any NSA personnel assigned to the SCIF between January 2010 and the end of your deployment? yes
(b)(6)(b)(7)(C) ① SPC (b)(6)(b)(7)(C) PO (b)(6)(b)(7)(C) ; SGT (b)(6)(b)(7)(C)

16. Did PFC MANNING have a friend, who worked for NSA? not that I am aware of

17. Was there anyone, who was obviously outspoken about the war or openly expressed negative thoughts and opinions? no

18. Do you know who (b)(6)(b)(7)(C) is? yes
(b)(6)(b)(7)(C) HUMINT Tm B Co

19. Did you ever witness PFC MANNING mention or watch any videos titled "Collateral Murder" and/or any other videos depicting gun camera footage taken by an Apache helicopter in Iraq? yes
(b)(6)(b)(7)(C) pretty sure; It's the same video by people descriptor: He watching on a SIPR laptop in the front early in the morning 7-8 AM
No clue as to when/what warm

20. Have you received e-mails, attachments, digital media devices, packages from PFC MANNING and vice versa? no

21. Have you ever allowed PFC MANNING to use your personal and/or U.S. Government owned computer(s)? no

22. Is there anything else you would like to add? I saw him listening and singing to various CD's & I saw him watch the gun tape. I was there when he struck SPC

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

DATE: 11 May 10 TIME: 1030

0028-10-CID221-10117
AGENT(S):

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

CANVASS INTERVIEW WORKSHEET

NAME: (b)(6)(b)(7)(C) RANK: E-4 SSN: (b)(6)(b)(7)(C)

UNIT/ADDRESS: B Co 2BSTB

TELEPHONE: (b)(6)(b)(7)(C) AKO E-MAIL ADDRESS: (b)(6)(b)(7)(C)@us.army.mil

1. Do you know who PFC Bradley E. MANNING is?
   Yes, - during the change over brefg, Many would give briefing (b)(6)(b)(7)(C) (b)(6)(b)(7)(C)
2. Did you work with PFC MANNING? - Not work tyethe
   No
3. When did you arrive in Iraq?
   15 OCT 09
4. When did PFC MANNING arrive in Iraq?
   don't know
5. Where did PFC MANNING work and what hours?
   with fusion, at night, I believe.
6. Where did you work and what hours?
   In the language Annex, primarily late night, early morning
7. With whom did PFC MANNING work?
   the analysts
8. Do you know or have you heard and/or witnessed of any incident involving PFC MANNING?
   Yes (b)(6)(b)(7)(C) after the fact thru News.
9. Do you know who (b)(6)(b)(7)(C) is?
   Yes - (b)(6)(b)(7)(C) Senior Air ② other SCIF
10. Do you know who (b)(6)(b)(7)(C) is?
    No (b)(6)(b)(7)(C) the Similer as (b)(6)(b)(7)(C)

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

11. Do you know who a U.S. Marine named (b)(6)(b)(7)(C) is?

Yes, (b)(6)(b)(7)(C) DNI Worked w/ Networks @ other SCIF

12. Did you have access to JWICS or Prophet?

No

13. Did PFC MANNING have access to JWICS or Prophet?

I don't know

14. Do you know of anyone who tried to get JWICS installed in the SCIF?

No

15. Can you identify any NSA personnel assigned to the SCIF between January 2010 and the end of your deployment?

No

16. Did PFC MANNING have a friend, who worked for NSA?

I don't know

17. Was there anyone, who was obviously outspoken about the war or openly expressed negative thoughts and opinions?

No

18. Do you know who (b)(6)(b)(7)(C) is?

No

19. Did you ever witness PFC MANNING mention or watch any videos titled "Collateral Murder" and/or any other videos depicting gun camera footage taken by an Apache helicopter in Iraq?

No

20. Have you received e-mails, attachments, digital media devices, packages from PFC MANNING and vice versa?

No

21. Have you ever allowed PFC MANNING to use your personal and/or U.S. Government owned computer(s)?

No

22. Is there anything else you would like to add?

No

DATE: 11 Aug 10 TIME: 1107 (b)(6)(b)(7)(C)

0028-10-CID221-10117
AGENT(S):

CANVASS INTERVIEW WORKSHEET

NAME: (b)(6)(b)(7)(C) RANK: E4 SSN: (b)(6)(b)(7)(C)

UNIT/ADDRESS: B/2BSTB

TELEPHONE: (b)(6)(b)(7)(C) AKO E-MAIL ADDRESS: (b)(6)(b)(7)(C)@US.ARMY.MIL

1. Do you know who PFC Bradley E. MANNING is?
   YES.
2. Did you work with PFC MANNING?
   NO.
3. When did you arrive in Iraq?
   2009
4. When did PFC MANNING arrive in Iraq?
   I do not Know.
5. Where did PFC MANNING work and what hours?
   BDE SCIF, I do not Know.
6. Where did you work and what hours?
   BDE TOC, VARIOUS HOURS
7. With whom did PFC MANNING work?
   SPC (b)(6)(b)(7)(C) SPC (b)(6)(b)(7)(C) ~~SGT~~ (b)(6)(b)(7)(C)
8. Do you know or have you heard and/or witnessed of any incident involving PFC MANNING?
   I heard that he was introuble, found out what about on wikipedia/GOOGLE
9. Do you know who (b)(6)(b)(7)(C) is?
   NO.
10. Do you know who (b)(6)(b)(7)(C) is?
    NO.

11. Do you know who a U.S. Marine named (b)(6)(b)(7)(C) is?
NO.

12. Did you have access to JWICS or Prophet?
NO.

13. Did PFC MANNING have access to JWICS or Prophet?
He shouldn't have.

14. Do you know of anyone who tried to get JWICS installed in the SCIF?
No.

15. Can you identify any NSA personnel assigned to the SCIF between January 2010 and the end of your deployment? Yes.

16. Did PFC MANNING have a friend, who worked for NSA?
I do not know.

17. Was there anyone, who was obviously outspoken about the war or openly expressed negative thoughts and opinions?
NO.

18. Do you know who (b)(6)(b)(7)(C) is?
NO. UNLESS YOU ARE SPEAKING OF THE HUMINT SOLDIER.

19. Did you ever witness PFC MANNING mention or watch any videos titled "Collateral Murder" and/or any other videos depicting gun camera footage taken by an Apache helicopter in Iraq?
No.

20. Have you received e-mails, attachments, digital media devices, packages from PFC MANNING and vice versa? ONLY normal RFI from the BDE SCIF such as targeting or Analysis. Only Fouo.

21. Have you ever allowed PFC MANNING to use your personal and/or U.S. Government owned computer(s)? No.

22. Is there anything else you would like to add?
No.

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID-10117

DETAILS

About 1140,11 Aug 10, SA (b)(6)(b)(7)(C) re-interviewed SPC (b)(6)(b)(7)(C) S-2, Headquarters and Headquarters Company (HHC), 2 Brigade Combat Team (2BCT), 10th Mtn Div, Fort Drum, NY (FDNY), who stated there were only two Secret Internet Protocol Router (SIPR) computers inside of SCIF at FDNY, where she and PFC MANNING worked prior to the deployment. SPC (b)(6)(b)(7)(C) stated she once saw PFC MANNING inserting a classified CD into a unclassified stand-alone (not connected to network) computer and when she confronted PFC MANNING, he replied and told her that MSG (b)(6)(b)(7)(C) full ID had asked him to transfer files from one SIPR computer to the unclassified stand-alone computer prior to a rebuild of the SIPR computer. SPC (b)(6)(b)(7)(C) stated she later talked to MSG (b)(6)(b)(7)(C) about the incident and he confirmed that he had asked PFC MANNING to transfer the files. SPC (b)(6)(b)(7)(C) stated she did not know how many files were transferred from SIPR to unclassified computer.

SPC (b)(6)(b)(7)(C) stated PFC MANNING once told her that he knew a MAJ (NFI) in Washington, District of Columbia (D.C.) and also met a lot of people working at the Pentagon while he was working as a barista at a Starbucks coffee shop. SPC (b)(6)(b)(7)(C) stated PFC MANNING once boasted about how much he knew about the Pentagon security system ins and outs.

SPC (b)(6)(b)(7)(C) also added PFC MANNING told her he had a remote server set up somewhere in D.C. area, but did not provide any further information as to the purpose for or the location of the server. ///LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060
SIGNATURE (b)(6)(b)(7)(C), (b) (7)(E)	DATE: 11 Aug 10 / EXHIBIT: 133

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID-10117

DETAILS

About 1321,11 Aug 10, SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) re-interviewed SPC (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) Public Affairs Office (PAO), HHC, 2nd Brigade Combat Team, 10th Mtn Div, Fort Drum, NY. SPC (b)(6)(b)(7)(C) stated that when PFC MANNING asked her to check his Gmail account and stocks, she was not aware he was in custody, otherwise she would have not checked PFC MANNING's e-mail or stocks for him. SPC (b)(6)(b)(7)(C) stated that PFC MANNING handed her a small piece of paper with his Gmail account username and password along with some stock symbols and, using her own personal laptop computer, she logged onto the account and only saw maybe six e-mails in inbox and looked at "Subject" and "Sender" lines of those e-mails. SPC (b)(6)(b)(7)(C) thought it was weird of PFC MANNING to ask her to check his Gmail, but PFC MANNING was her friend and did not suspect him of any wrongdoing. SPC (b)(6)(b)(7)(C) stated she handed PFC MANNING back the paper and did not remember the password.

AGENT's COMMENTS: When SA (b)(6)(b)(7)(C) first identified himself as a Special Agent with the U. S. Army CID, SPC (b)(6)(b)(7)(C) immediately blurted out, "I have already told you guys everything....I don't know nothing." in an obviously agitated manner. SPC (b)(6)(b)(7)(C) stated she had already spoken with multiple investigators regarding PFC MANNING's Gmail and each time she would tell them the same thing. SPC (b)(6)(b)(7)(C) further added had she known checking PFC MANNING's Gmail was going to have caused her this much inconvenience and trouble, she would have not said anything in the first place. When SA (b)(6)(b)(7)(C) reminded her of the fact such acts could result in her committing unintended crimes such accessory after the fact, obstruction of justice, etc., to which SPC (b)(6)(b)(7)(C) remained unresponsive, but her body language suggested her obvious dislike of participating in this interview.///LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060
SIGNATURE (b)(6)(b)(7)(C), (b) (7)(E)	DATE: 11 Aug 10 / EXHIBIT: 134

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID-10117

DETAILS

About 1430, 11 Aug 10, SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) interviewed MSG (b)(6)(b)(7)(C) HHC, 2nd Brigade Combat Team, 10th Mtn Div, Fort Drum, NY (FDNY), who stated he was the S-2 Non-Commissioned Officer in Charge (NCOIC) at FDNY and also was at the SCIF, where PFC MANNING worked while deployed in Iraq.

MSG (b)(6)(b)(7)(C) stated when PFC MANNING first arrived at FDNY, he immediately noticed PFC MANNING was "tiny and shy" and did not socialize well with other Soldiers in his unit, but was otherwise very brilliant and intelligent.

(b)(6)(b)(7)(C) stated he first recognized PFC MANNING was having issues adjusting when PFC MANNING showed up late for formation. While being given an on-the-spot correction, PFC MANNING lost his composure and military bearing and started yelling unintelligibly and "freaking out." MSG (b)(6)(b)(7)(C) stated PFC MANNING had to be referred to the FDNY behavioral health clinic for evaluation.

MSG (b)(6)(b)(7)(C) recalled another incident, wherein PFC MANNING supposedly had gone to see a podiatrist and subsequently was referred to the behavioral health clinic as well (NFI).

MSG (b)(6)(b)(7)(C) added PFC MANNING was once again referred to the Combat Stress Team in Iraq after he "freaked out" and flipped over the table while being counseled for coming to work late.

MSG (b)(6)(b)(7)(C) stated that PFC MANNING once told him that he had no recollection of enlisting in the Army and finally realized that he was in the Army only 6 months after the fact.

MSG (b)(6)(b)(7)(C) stated when they first arrived in Iraq, when PFC MANNING would give a presentation of his work product during turn-over briefings, he would often freeze and just stand there for a minute or two.

MSG (b)(6)(b)(7)(C) stated he thought PFC MANNING was not performing satisfactorily and maybe under stress and decided to move him to the night shift, during which he could be more productive and have less human interactions.

MSG (b)(6)(b)(7)(C) was questioned about the data transfer from SIPR to unclassified stand-alone computer, to which he replied and stated he had no recollection. MSG (b)(6)(b)(7)(C) stated this was possibly due to past and current neuro-psychological problems he had been dealing with and for which had been evaluated at Walter Reed Army Medical Center.

MSG (b)(6)(b)(7)(C) further confirmed while deployed in Iraq, PFC MANNING had never gone outside the camp on a mission nor did he interact with local or foreign nationals outside the camp.///LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE (b)(6)(b)(7)(C), (b) (7)(E)	DATE 11 Aug 10	EXHIBIT 135

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID-10117

DETAILS

About 0945, 12 Aug 10, SA (b)(6)(b)(7)(C) interviewed CPL (b)(6)(b)(7)(C) Supply Clerk, HHC, 2nd Brigade Combat Team (2 BCT), 10th Mountain Division (10 Mtn Div), Fort Drum, NY (FDNY), to obtain information concerning her interactions with PFC MANNING and the personal laptop of SSG (b)(6)(b)(7)(C) S-4, HHC, 2 BCT, 10th Mtn Div, FDNY . CPL (b)(6)(b)(7)(C) advised that while the unit was deployed to Forward Operating Base Hammer, she worked with PFC MANNING for a short time in the S-2 Section and also when he was briefly assigned to work in Supply. CPL (b)(6)(b)(7)(C) advised that she used SSG (b)(6)(b)(7)(C) personal laptop on occasion to check her Yahoo! Mail and Facebook when PFC MANNING was not there. She denied any knowledge of (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) or WikiLeaks. She denied any use of FriendFeed.com, Twitter, or Gmail. CPL (b)(6)(b)(7)(C) stated SPC (b)(6)(b)(7)(C) S-1, HHC, 2 BCT, 10th Mtn Div, FDNY, would occasionally use the laptop to access Yahoo! Instant Messenger. ///LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
(b)(6)(b)(7)(C), (b) (7)(E)	DATE 12 Aug 10	EXHIBIT 136

Approved (b)(6)(b)(7)(C)

DATE: 8-12-10 TIME: 1040 [redacted] 0028-10-CID221-10117
AGENT(S):
Page 1 of 2

CANVASS INTERVIEW WORKSHEET

NAME: [redacted] RANK: [redacted] SSN [redacted]

UNIT/ADDRESS: HHC, 2nd BCT Supply room

TELEPHONE: [redacted] AKO E-MAIL ADDRESS: [redacted]@us.army.mil

1. Do you know who PFC Bradley E. MANNING is?
   Yes. I worked with him in supply and when in S-2
2. Did you work with PFC MANNING?
   Yes
3. When did you arrive in Iraq?
   Nov 2009
4. When did PFC MANNING arrive in Iraq?
   No he was there before I was
5. Where did PFC MANNING work and what hours?
   He worked in S-2 but not sure what hours-
   saw him in cooking area at night
6. Where did you work and what hours?
   Supply from 1000-1800 normally
7. With whom did PFC MANNING work?
   He worked with SPC [redacted] PFC [redacted] SPC [redacted]
   SGT [redacted] MSGT [redacted]
8. Do you know or have you heard and/or witnessed of any incident involving PFC MANNING?
   Heard when he punched SPC [redacted]
   Before he was arrested, said he "did something wrong" but not what
9. Do you know who [redacted]?
   No
10. Do you know who [redacted]?
    No

11. Do you know who a U.S. Marine named (b)(6)(b)(7)(C) is?

No

12. Did you have access to JWICS or Prophet?

No

13. Did PFC MANNING have access to JWICS or Prophet?

I have no idea

14. Do you know of anyone who tried to get JWICS installed in the SCIF?

No

15. Can you identify any NSA personnel assigned to the SCIF between January 2010 and the end of your deployment?

No

16. Did PFC MANNING have a friend, who worked for NSA?

No

17. Was there anyone, who was obviously outspoken about the war or openly expressed negative thoughts and opinions?

Only MANNING - when the subject came up

18. Do you know who (b)(6)(b)(7)(C) is?

No

19. Did you ever witness PFC MANNING mention or watch any videos titled "Collateral Murder" and/or any other videos depicting gun camera footage taken by an Apache helicopter in Iraq?

No Downloading / listening to music

20. Have you received e-mails, attachments, digital media devices, packages from PFC MANNING and vice versa?

No

21. Have you ever allowed PFC MANNING to use your personal and/or U.S. Government owned computer(s)?

NO

22. Is there anything else you would like to add?

used when MANNING was off, but not every day i.e. yahoo mail & fb

UU28 10 CID221 10117

1.) Do you know or have you ever had any communication with anyone by the last name of (b)(6)(b)(7)(C)

No

2.) Do you know or have you ever had any communication with anyone by the last name of (b)(6)(b)(7)(C)

No

3.) You have ever searched for and/or viewed on ~~your personal~~ SSG (b)(6)(b)(7)(C) laptop any videos titled "Collateral Murder" and/or any other videos depicting gun camera footage taken by an Apache helicopter in Iraq?

No

4.) Have you ever visited the website "WikiLeaks.org" or any websites related to or mentioning WikiLeaks?

No

5.) Do you know or have you ever had any communication with anyone by the last name of (b)(6)(b)(7)(C)

No

6.) Do you know or have you ever had any communication with anyone by the first name of (b)(6)(b)(7)(C)

NO

~~7.) On your personal computer the "Registered Owner" identified in the operating system was named (b)(6)(b)(7)(C) this would have likely been established when the Windows Vista operating system was installed. Did you provide this Registered Owner name or would someone else have provided this?~~

8.) Have you ever created any Twitter accounts using ~~your personal~~ SGT (b)(6)(b)(7)(C) laptop computer?

No don't use Twitter

~~9.) Was your personal laptop computer set to require anyone using it to have a password (i.e., was your laptop password protected)?~~

10.) Have you ever used, searched for, or were otherwise aware of the domain name "FriendFeed.com"?

No

11.) Do you use the email service provided by Google called "Gmail", if yes, what is your email address there?

No

12.) Have you recently (in the past year) been in contact with anyone who lives in the Boston, MA area?

No

13.) Have you ever let anyone borrow your ~~personal laptop~~ government computer, if yes, who and what were the approximate dates/times they borrowed it?

No personal computer then

No, only a few work-related times, nothing personal

14.) If someone did borrow your personal laptop computer, can you provide any of the circumstances as to why they would have needed to use it and/or why you allowed them to use your computer?

N/A

15.) Could someone have used your personal laptop computer without your knowledge?

N/A

16.) Is there anything else I did not specifically ask in the questions or your use of SSG (b)(6)(b)(7)(C) above in relation to your personal laptop computer and anyone who may have borrowed or used it in the past several months that you'd like to mention?

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

Sic [redacted] used it to

Yahoo! Messenger No one else used it.

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER 0028-10-CID221-10117

PAGE 1 OF 1 PAGES

DETAILS

About 0945, 12 Aug 10, SA (b)(6)(b)(7)(C) coordinated with CWO4 (b)(6)(b)(7)(C) Commanding Officer, Marine Corps Brig (MCB)– Quantico, Quantico, VA, concerning inmate PFC MANNING.

CWO4 (b)(6)(b)(7)(C) produced the inventory sheet pertaining to PFC MANNING which listed a wallet, a few debit/credit cards, a certain amount of cash, and some U.S. Government issued items which were in-processed with PFC MANNING. The inventory sheet reflected that no personal papers in-processed with PFC MANNING. CWO4 (b)(6)(b)(7)(C) confirmed that no personal papers were transferred with PFC MANNING.

CWO4 (b)(6)(b)(7)(C) related that PFC MANNING was only allowed to receive mail and visits from specific persons from a list he created. Included on PFC MANNING's list of persons he could receive mail/visits from were: (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) (Friend, (b)(6)(b)(7)(C) , (b)(6)(b)(7)(C) Friend, (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) (Friend, (b)(6)(b)(7)(C) (Prospective Attorney, (b)(6)(b)(7)(C) , (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) , (b)(6)(b)(7)(C) Friend, (b)(6)(b)(7)(C) , and (b)(6)(b)(7)(C) (Friend, (b)(6)(b)(7)(C)

Since his arrival at MCB - Quantico, PFC MANNING had been visited by mental health personnel, his chain of command, defense counsel (military), and his aunt. CWO4 (b)(6)(b)(7)(C) further related that the telephone calls of inmates were not recorded as a manner of practice, however, could be recorded upon official request from the investigative organization.

CWO4 (b)(6)(b)(7)(C) related that PFC MANNING had been re-assigned to the Fort Myer Military Community. His chain of command included CPT (b)(6)(b)(7)(C) 1SG (b)(6)(b)(7)(C) and CSM (b)(6)(b)(7)(C) , all of Headquarters and Headquarters Company (HHC), U.S. Army Garrison (USAG), Fort Myer, VA.

AGENT's COMMENT: Due to the fact that the conversation with CWO4 (b)(6)(b)(7)(C) concerned PFC MANNING, I had to sign the guest book as a visitor would to see PFC MANNING. At no point while at the Quantico Brig, did I make contact with PFC MANNING or see PFC MANNING.

//LAST ENTRY//

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION Washington Metro Resident Agency Computer Crime Investigative Unit U.S. Army CID. Fort Belvoir. VA 22060	
SA (b)(6)(b)(7)(C), (b) (7)(E)		
SIGNATURE (b)(6)(b)(7)(C)	DATE 12 Aug 10	EXHIBIT 138

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID-10117

DETAILS

About 1000, 12 Aug 10, SA (b)(6)(b)(7)(C) interviewed SPC (b)(6)(b)(7)(C), B Co, 2nd Brigade Combat Team, 10th Mtn Div, Fort Drum, NY, who stated the "Shared SIPR Server" at Forward Operating Base Hammer was located on a global network drive and anyone with SIPR account could easily map it and gain access. SPC (b)(6)(b)(7)(C) however, cautioned that just because one had access to the server and its contents, he or she should not be doing so. SPC (b)(6)(b)(7)(C) stated he had always been vocal and adamant about a strong network defense and prevention of sensitive information spillage. SPC (b)(6)(b)(7)(C) stated that since he was more computer and network savvy than the assigned S-6 personnel, he would often "be volunteered" to scan the network for viruses and patch updates using Retina and Norton Anti-Virus software.

SPC (b)(6)(b)(7)(C) recalled his conversation with PFC MANNING about hash table software and stated that PFC MANNING seemed more interested in marketing and profiting aspects of the software, rather than for his personal use.

SPC (b)(6)(b)(7)(C) theorized about how PFC MANNING transmitted classified materials: SPC (b)(6)(b)(7)(C) stated that PFC MANNING could have copied the data onto CD-RW's and sent the data either using his own personnel computer via wireless internet at his room or using one of the Morale, Welfare, and Recreation (MWR) computers at Forward Operating Base (FOB) Hammer, Iraq. SPC (b)(6)(b)(7)(C) stated the Non-classified Internet Protocol Router Network (NIPRNet) in the SCIF was extremely slow and doubted PFC MANNING used it to transmit a large volume of data. SPC (b)(6)(b)(7)(C) stated MWR computers required no username or password and were always available for anyone to use at their pleasure.

SPC (b)(6)(b)(7)(C) escribed PFC MANNING as a brilliant individual, who would read a lot of literature to self-educate, but not "innate".

SPC (b)(6)(b)(7)(C) clarified that in his previous statement when he mentioned the weak network computer security in the housing units, he was talking about the local commercial "Haji" Internet. SPC (b)(6)(b)(7)(C) stated the local service provider would take first 3 letters of Soldier's last name, plus room numbers and use the combination as one's username. SPC (b)(6)(b)(7)(C) stated password would usually be 3 to 4 numbers in length. SPC (b)(6)(b)(7)(C) stated the local service provider would input everyone's username and password on a spreadsheet, and one could easily look over the provider's shoulder and see others' usernames and passwords. SPC (b)(6)(b)(7)(C) stated due to the simplicity of the user name naming convention, one could easily guess others' usernames and passwords and gain access to the local internet service. SPC (b)(6)(b)(7)(C) stated he did not know after how many failed attempts, the account would be locked, but he was speculating that it was unlimited. SPC (b)(6)(b)(7)(C) stated Soldiers were given wireless connection, but if one was already connected, others could not use the same username and password.

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060
SIGNATURE (b)(6)(b)(7)(C), (b) (7)(E)	DATE: 12 Aug 10 / EXHIBIT: 139

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID-10117

DETAILS

SPC (b)(6)(b)(7)(C) further added that, to the best of his knowledge, while PFC MANNING was stationed at FOB HAMMER, Iraq, he had never gone outside the wire.

SPC (b)(6)(b)(7)(C) mentioned PFC MANNING became upset after he had found out several foreign journalists were apprehended by Iraqi police for distributing what they believed to be anti government of Iraq literature///LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNAT (b)(6)(b)(7)(C), (b) (7)(E)	DATE 12 Aug 10	EXHIBIT 139

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID-10117

DETAILS

About 1351, 12 Aug 10, SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) interviewed 1LT (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) S-2, Headquarters and Headquarters Company (HHC), 2 Brigade Combat Team (BCT), 10th Mountain Division (Mtn Div), who stated in preparation for the upcoming deployment to Iraq, he had asked SPC (b)(6)(b)(7)(C) to scan the Prophet operating system with Retina and Norton Anti-virus software.

1LT (b)(6)(b)(7)(C) said that PFC MANNING was highly motivated before they left for Iraq because he thought he would jump right into action and do great things in Iraq; however, once he realized he would sit in front of a computer all day and not go outside the wire, he was disappointed and down. 1LT (b)(6)(b)(7)(C) stated he would often attempt to motivate PFC MANNING by giving him words of encouragement and motivational speeches, but PFC MANNING remained "disinterested and not willing". 1LT (b)(6)(b)(7)(C) recalled that when PFC MANNING first started working in SCIF, he seemed to spend a long time surfing the Internet on a NIPR laptop computer and he was fascinated by the recent volcano eruption in Iceland.///LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE (b)(6)(b)(7)(C), (b) (7)(E)	DATE 12 Aug 10	EXHIBIT 140

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

About 1330, 13 Aug 10, SA (b)(6)(b)(7)(C) reviewed the Internet Protocol (IP) addresses that accessed the Gmail account "bradly.e.manning@Gmail.com". The following IP addresses were obtained from Google Inc, after SA (b)(6)(b)(7)(C), (b) (7)(E) this office, served a search warrant on Google Inc. for the information. SA (b)(6)(b)(7)(C) performed a IP whois query for each of the recorded IP addresses and received the following results:

IP: 82.205.133.8
Resolved to: Horizon Satellite Services FZ LLC, LIR
P.O. Box 502343, Building No.14
Dubai Internet City, United Arab Emirates
Phone: +971 4 391 5122
Fax-no: +971 4 391 2906
Open source searches showed Horizon was a satellite communications provider throughout the Middle East.

~~~~~

IP: 82.205.133.9
Resolved to: Horizon Satellite Services FZ LLC, LIR
P.O. Box 502343, Building No.14
Dubai Internet City
United Arab Emirates
Phone: +971 4 391 5122
Fax-no: +971 4 391 2906
Open source searches showed Horizon was a satellite communications provider throughout the Middle East.

~~~~

IP: 82.205.133.10
Resolved to: Horizon Satellite Services FZ LLC, LIR
P.O. Box 502343, Building No.14
Dubai Internet City
United Arab Emirates
Phone: +971 4 391 5122
Fax-no: +971 4 391 2906
Open source searches showed Horizon was a satellite communications provider throughout the Middle East.

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION Washington Metro Resident Agency Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SA (b)(6)(b)(7)(C), (b) (7)(E)		
SIGNATURE SA. (b)(6)(b)(7)(C)	DATE 13 AUG 10	EXHIBIT 141

DETAILS

~~~

IP: 82.205.133.20
Resolved to: Horizon Satellite Services FZ LLC, LIR
P.O. Box 502343, Building No.14
Dubai Internet City
United Arab Emirates
Phone: +971 4 391 5122
Fax-no: +971 4 391 2906
Open source searches showed Horizon was a satellite communications provider throughout the Middle East.

~~~~

IP: 82.205.133.30
Resolved to: Horizon Satellite Services FZ LLC, LIR
P.O. Box 502343, Building No.14
Dubai Internet City
United Arab Emirates
Phone: +971 4 391 5122
Fax-no: +971 4 391 2906
Open source searches showed Horizon was a satellite communications provider throughout the Middle East.

~~~~

IP: 109.224.1.70
Resolves to: EarthLink Ltd. Communications & Internet Services
Phone: + 964 790 1946348

~~~~

IP: 109.224.6.127
Resolves to: EarthLink Ltd. Communications & Internet Services
Phone: + 964 790 1946348

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION Washington Metro Resident Agency Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SA (b)(6)(b)(7)(C), (b) (7)(E)		
SIGNATURE SA (b)(6)(b)(7)(C)	DATE 13 AUG 10	EXHIBIT 141

DETAILS

~~~~

IP: 84.11.147.4
Resolves to: IABG Satellite Internet Services
Einsteinstrasse 20
85521 Ottobrunn
Germany
Phone +49 89 6088-0
Fax +49 89 6088-4000
info@iabg.de

Open source searches show IABG offers complete end-to-end communications solutions via satellite, for services such as the Internet, voice, data and images to customers worldwide.

~~~~

IP: 214.13.232.180
Resolves to: DoD Network Information Center
DNIC
3990 E. Broad Street
Columbus, OH, 43218

Agents note: All of the above listed IP addresses repeatedly accessed the bradly.e.manning@Gmail.com account, with the exception of the DoD network IP, which only appeared one time in the logs. ///LAST ENTRY///.

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION Washington Metro Resident Agency Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SA (b)(6)(b)(7)(C), (b) (7)(E)		
SIGNATURE SA. (b)(6)(b)(7)(C)	DATE 13 AUG 10	EXHIBIT 141

GOOGLE SUBSCRIBER INFORMATION

Name: Bradley Manning
e-Mail: bradleyemanning@gmail.com
Status: Enabled
Services: Data summary, Docs, Gmail, Google wave, Mobile, News, Search history, Talk, Toolbar, Transliteration, Web history promo, Youtube
Secondary e-Mail: bradley.manning@earthlink.net
Created on: 2009/09/09-00:14:38-UTC
IP: 96.231.145.214 on 2009/09/09-00:14:38-UTC
Language Code: en
Other Usernames: bradley.e.manning@gmail.com

Date/Time	Event	IP
2010/05/28-19:03:13-UTC	Logout	82.205.133.9
2010/05/28-18:52:21-UTC	Login	82.205.133.9
2010/05/28-07:53:15-UTC	Login	109.224.1.70
2010/05/28-07:51:41-UTC	Login	109.224.1.70
2010/05/27-09:58:10-UTC	Login	82.205.133.9
2010/05/27-03:19:47-UTC	Login	82.205.133.9
2010/05/26-23:31:38-UTC	Login	82.205.133.9
2010/05/26-20:35:54-UTC	Login	82.205.133.9
2010/05/26-20:33:58-UTC	Login	82.205.133.9
2010/05/26-13:32:30-UTC	Login	82.205.133.9
2010/05/26-13:22:49-UTC	Login	82.205.133.9
2010/05/26-08:23:25-UTC	Login	82.205.133.9
2010/05/26-08:20:51-UTC	Login	82.205.133.9
2010/05/26-04:43:25-UTC	Login	82.205.133.9
2010/05/26-04:39:32-UTC	Login	82.205.133.9
2010/05/26-03:53:29-UTC	Login	82.205.133.9
2010/05/25-20:35:02-UTC	Login	82.205.133.9
2010/05/25-20:28:08-UTC	Login	82.205.133.9
2010/05/25-20:04:48-UTC	Login	82.205.133.9
2010/05/25-19:54:17-UTC	Login	82.205.133.9
2010/05/25-19:05:02-UTC	Login	82.205.133.9
2010/05/25-18:32:44-UTC	Login	82.205.133.9
2010/05/25-17:39:02-UTC	Login	82.205.133.9
2010/05/25-17:27:53-UTC	Login	82.205.133.9
2010/05/25-16:31:42-UTC	Login	82.205.133.9
2010/05/25-15:24:41-UTC	Login	82.205.133.9
2010/05/25-14:56:25-UTC	Login	82.205.133.9
2010/05/25-14:37:37-UTC	Login	82.205.133.9
2010/05/25-14:24:18-UTC	Login	82.205.133.9
2010/05/25-14:22:19-UTC	Login	82.205.133.9
2010/05/25-14:21:59-UTC	Login	82.205.133.9
2010/05/25-14:21:04-UTC	Login	82.205.133.9
2010/05/25-08:40:45-UTC	Login	82.205.133.9
2010/05/25-08:40:29-UTC	Login	82.205.133.9
2010/05/25-08:39:48-UTC	Login	82.205.133.9
2010/05/25-08:39:43-UTC	Login	82.205.133.9
2010/05/25-08:36:58-UTC	Login	82.205.133.9
2010/05/24-23:30:44-UTC	Login	82.205.133.9
2010/05/24-23:16:18-UTC	Login	82.205.133.9
2010/05/24-20:48:08-UTC	Login	82.205.133.9
2010/05/24-20:46:51-UTC	Login	82.205.133.9
2010/05/24-19:43:20-UTC	Login	82.205.133.9
2010/05/24-19:28:50-UTC	Login	82.205.133.9

2010/05/24-19:23:10-UTC	Login	82.205.133.9
2010/05/24-19:23:08-UTC	Login	82.205.133.9
2010/05/24-17:20:01-UTC	Logout	109.224.6.127
2010/05/24-16:23:20-UTC	Login	109.224.6.127
2010/05/24-15:07:28-UTC	Login	82.205.133.9
2010/05/24-14:58:13-UTC	Login	82.205.133.9
2010/05/24-14:52:52-UTC	Login	82.205.133.9
2010/05/24-14:51:41-UTC	Login	82.205.133.9
2010/05/24-14:35:36-UTC	Login	82.205.133.9
2010/05/24-14:31:36-UTC	Login	82.205.133.9
2010/05/24-07:28:15-UTC	Logout	109.224.6.127
2010/05/24-07:20:28-UTC	Login	109.224.6.127

Subscriber Information bradley.e.manning

Email:	bradley.e.manning@gmail.com
Status:	Enabled
Services:	MOBILE, Docs, Gmail, Talk, Search History, TRANSLITERATION, YOUTUBE, DATA_SUMMARY, News, Google Wave, WEB_HISTORY_PROMO, Toolbar
Name:	Bradley Manning
Secondary email:	bradley.manning@earthlink.net
Created on:	09-Sep-2009 12:14:38am GMT
Lang:	en
IP:	96.231.145.214 on 09-Sep-2009 12:14:38am GMT

Logs
All times are displayed in UTC/GMT.
bradley.e.manning@gmail.com

Date/Time	Event	IP
28-May-2010 07:03:13 pm GMT	Logout	82.205.133.9
28-May-2010 06:52:21 pm GMT	Login Success	82.205.133.9
28-May-2010 06:52:20 pm GMT	Login Attempt	82.205.133.9
28-May-2010 06:49:49 pm GMT	LOGIN_ATTEMPT_AND_FAILURE	82.205.133.9
28-May-2010 06:47:42 pm GMT	LOGIN_ATTEMPT_AND_FAILURE	82.205.133.9
28-May-2010 06:46:38 pm GMT	Login Failure	82.205.133.9
28-May-2010 06:46:37 pm GMT	Login Attempt	82.205.133.9
28-May-2010 07:53:15 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	109.224.1.70
28-May-2010 07:51:41 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	109.224.1.70
27-May-2010 09:58:10 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
27-May-2010 03:19:47 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
26-May-2010 11:31:38 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
26-May-2010 08:35:54 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
26-May-2010 08:33:58 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
26-May-2010 01:32:30 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
26-May-2010 01:22:49 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
26-May-2010 08:23:25 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
26-May-2010 08:20:51 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
26-May-2010 04:43:25 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
26-May-2010 04:39:32 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
26-May-2010 03:53:29 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
25-May-2010 08:35:02 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
25-May-2010 08:28:08 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
25-May-2010 08:04:48 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
25-May-2010 07:54:17 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
25-May-2010 07:05:02 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
25-May-2010 06:32:44 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
25-May-2010 05:39:02 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
25-May-2010 05:27:53 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
25-May-2010 05:24:07 pm GMT	Login Attempt	82.205.133.9
25-May-2010 04:31:42 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
25-May-2010 03:24:41 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
25-May-2010 02:56:25 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
25-May-2010 02:37:37 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
25-May-2010 02:24:18 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9

EXHIBIT 142

25-May-2010 02:22:19 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
25-May-2010 02:21:59 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
25-May-2010 02:21:04 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
25-May-2010 08:40:45 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
25-May-2010 08:40:29 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
25-May-2010 08:39:48 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
25-May-2010 08:39:43 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
25-May-2010 08:36:58 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
24-May-2010 11:30:44 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
24-May-2010 11:16:18 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
24-May-2010 08:48:08 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
24-May-2010 08:46:51 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
24-May-2010 07:43:20 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
24-May-2010 07:28:50 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
24-May-2010 07:23:10 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
24-May-2010 07:23:08 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
24-May-2010 05:20:01 pm GMT	Logout	109.224.6.127
24-May-2010 04:23:20 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	109.224.6.127
24-May-2010 04:22:30 pm GMT	LOGIN_ATTEMPT_AND_FAILURE	109.224.6.127
24-May-2010 03:07:28 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
24-May-2010 02:58:13 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
24-May-2010 02:52:52 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
24-May-2010 02:51:41 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
24-May-2010 02:35:36 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
24-May-2010 02:31:36 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
24-May-2010 07:28:15 am GMT	Logout	109.224.6.127
24-May-2010 07:20:28 am GMT	Login Success	109.224.6.127
24-May-2010 07:20:27 am GMT	Login Attempt	109.224.6.127
24-May-2010 07:20:18 am GMT	LOGIN_ATTEMPT_AND_FAILURE	109.224.6.127
24-May-2010 06:20:46 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
24-May-2010 06:14:07 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
23-May-2010 07:37:55 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
23-May-2010 07:29:48 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
23-May-2010 07:12:54 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
23-May-2010 07:12:26 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
23-May-2010 07:02:55 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
23-May-2010 06:32:06 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
23-May-2010 05:21:26 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
22-May-2010 11:16:16 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
22-May-2010 08:16:53 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
22-May-2010 05:21:32 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
22-May-2010 03:34:07 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	214.13.232.180
22-May-2010 10:13:54 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
22-May-2010 10:12:59 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
22-May-2010 10:12:48 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
22-May-2010 10:11:00 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
22-May-2010 10:09:43 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
22-May-2010 05:34:24 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
21-May-2010 08:34:48 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
21-May-2010 08:34:41 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8

EXHIBIT 142

21-May-2010 08:04:31 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
21-May-2010 07:58:12 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
21-May-2010 07:54:22 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
21-May-2010 07:46:36 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
21-May-2010 06:39:17 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
21-May-2010 06:38:40 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
21-May-2010 06:26:47 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
21-May-2010 06:24:12 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
21-May-2010 05:07:01 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
21-May-2010 05:04:42 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
21-May-2010 04:01:42 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	214.13.232.180
21-May-2010 04:01:31 pm GMT	LOGIN_ATTEMPT_AND_FAILURE	214.13.232.180
21-May-2010 02:14:52 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
21-May-2010 02:14:48 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
21-May-2010 12:31:42 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	214.13.232.180
21-May-2010 11:54:56 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
21-May-2010 11:47:59 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
21-May-2010 11:33:47 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	214.13.232.180
21-May-2010 11:06:02 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	214.13.232.180
21-May-2010 10:27:31 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	214.13.232.180
21-May-2010 09:49:18 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	214.13.232.180
21-May-2010 09:14:28 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
21-May-2010 09:09:32 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
21-May-2010 09:08:51 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
21-May-2010 08:56:10 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
21-May-2010 08:55:17 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
21-May-2010 08:55:10 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
21-May-2010 08:55:03 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
21-May-2010 08:54:58 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
21-May-2010 08:54:20 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
21-May-2010 08:50:47 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
21-May-2010 08:50:29 am GMT	LOGIN_ATTEMPT_AND_FAILURE	82.205.133.20
21-May-2010 08:50:06 am GMT	LOGIN_ATTEMPT_AND_FAILURE	82.205.133.20
21-May-2010 08:49:49 am GMT	Login Attempt	82.205.133.20
21-May-2010 08:31:32 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
21-May-2010 08:31:06 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
21-May-2010 08:30:58 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
21-May-2010 07:45:04 am GMT	Logout	214.13.232.180
21-May-2010 07:38:15 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	214.13.232.180
21-May-2010 07:38:06 am GMT	Login Failure	214.13.232.180
21-May-2010 07:38:05 am GMT	Login Attempt	214.13.232.180
21-May-2010 05:22:10 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
21-May-2010 05:22:03 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
21-May-2010 05:21:55 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
21-May-2010 05:21:50 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
21-May-2010 12:06:40 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
20-May-2010 11:06:50 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
20-May-2010 10:37:42 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
20-May-2010 10:05:22 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
20-May-2010 10:01:22 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20

EXHIBIT 142

20-May-2010 09:34:23 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
20-May-2010 09:31:11 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
20-May-2010 09:20:24 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
20-May-2010 09:06:55 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
20-May-2010 08:59:17 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
20-May-2010 08:32:52 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
20-May-2010 08:31:39 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
20-May-2010 08:31:22 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
20-May-2010 07:59:08 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
20-May-2010 07:58:59 pm GMT	Login Success	82.205.133.20
20-May-2010 07:58:58 pm GMT	Login Attempt	82.205.133.20
20-May-2010 07:38:54 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
20-May-2010 07:36:31 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.20
20-May-2010 07:27:13 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
20-May-2010 07:21:42 pm GMT	Login Success	82.205.133.8
20-May-2010 07:21:41 pm GMT	Login Attempt	82.205.133.8
20-May-2010 06:48:28 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.30
20-May-2010 06:47:39 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.30
20-May-2010 06:05:26 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
20-May-2010 05:57:15 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
20-May-2010 03:26:39 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
20-May-2010 03:23:22 pm GMT	Login Success	82.205.133.8
20-May-2010 03:23:21 pm GMT	Login Attempt	82.205.133.8
20-May-2010 02:53:29 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
20-May-2010 02:48:42 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
20-May-2010 02:46:38 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
20-May-2010 02:25:00 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
20-May-2010 02:24:54 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
20-May-2010 02:24:48 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
20-May-2010 02:24:33 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
20-May-2010 09:01:06 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
20-May-2010 09:00:49 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
20-May-2010 09:00:41 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
20-May-2010 09:00:39 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
20-May-2010 09:00:38 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
20-May-2010 09:00:36 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
20-May-2010 03:26:22 am GMT	Login Success	82.205.133.8
20-May-2010 03:26:21 am GMT	Login Attempt	82.205.133.8
20-May-2010 12:17:09 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 11:30:35 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 11:13:32 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 11:04:13 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 10:52:25 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 10:49:37 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 10:20:12 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 09:59:54 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 09:48:42 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 09:48:30 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 09:44:05 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 09:38:59 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8

EXHIBIT 142

19-May-2010 09:36:25 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 09:34:06 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 09:31:56 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 09:28:46 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 09:26:46 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 09:24:07 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 08:58:11 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 08:45:45 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 08:08:08 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 06:53:12 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 06:14:23 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 06:11:30 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 06:06:59 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 05:57:21 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 03:09:59 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 03:04:44 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 02:40:03 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 02:32:10 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 02:31:02 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 01:00:07 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 10:14:06 am GMT	Login Success	82.205.133.8
19-May-2010 10:14:05 am GMT	Login Attempt	82.205.133.8
19-May-2010 10:12:55 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 10:01:04 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.10
19-May-2010 09:53:43 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.10
19-May-2010 09:12:15 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 07:49:44 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 07:49:12 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 07:44:29 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
19-May-2010 02:31:14 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
18-May-2010 11:44:25 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
18-May-2010 11:29:57 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
18-May-2010 11:22:55 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
18-May-2010 10:59:23 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
18-May-2010 10:54:10 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
18-May-2010 10:21:30 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
18-May-2010 10:21:26 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
18-May-2010 09:56:13 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
18-May-2010 09:46:43 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
18-May-2010 07:17:51 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
18-May-2010 07:14:43 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
18-May-2010 07:13:13 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
18-May-2010 02:46:08 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
18-May-2010 02:40:52 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
18-May-2010 09:10:32 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
18-May-2010 09:03:34 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
18-May-2010 09:03:29 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
18-May-2010 08:09:43 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
17-May-2010 10:18:23 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
17-May-2010 03:37:06 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8

EXHIBIT 142

17-May-2010 02:55:58 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
17-May-2010 02:45:31 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
17-May-2010 02:45:18 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
17-May-2010 02:45:13 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
17-May-2010 01:26:09 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
17-May-2010 01:01:55 pm GMT	Logout	214.13.232.180
17-May-2010 12:51:55 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	214.13.232.180
17-May-2010 12:51:39 pm GMT	LOGIN_ATTEMPT_AND_FAILURE	214.13.232.180
17-May-2010 09:20:32 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
17-May-2010 09:20:25 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
17-May-2010 09:16:30 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
17-May-2010 09:00:17 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.10
17-May-2010 08:59:46 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.10
17-May-2010 08:59:42 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.10
17-May-2010 08:55:34 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.10
17-May-2010 08:55:22 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.10
17-May-2010 08:49:21 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.10
17-May-2010 08:38:01 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
17-May-2010 08:37:52 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
17-May-2010 08:37:48 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
17-May-2010 08:37:40 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
17-May-2010 08:33:15 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
17-May-2010 08:16:52 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
17-May-2010 08:12:05 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
17-May-2010 08:00:27 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
17-May-2010 07:50:25 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
17-May-2010 07:46:33 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.8
17-May-2010 07:43:50 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.10
17-May-2010 07:36:45 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.10
17-May-2010 06:46:34 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.10
17-May-2010 06:35:00 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.10
17-May-2010 06:29:10 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.10
17-May-2010 06:28:37 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.10
17-May-2010 06:19:11 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.10
17-May-2010 06:19:01 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.10
17-May-2010 06:06:46 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.10
17-May-2010 06:03:45 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.10
17-May-2010 06:00:31 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.10
17-May-2010 05:55:18 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.10
16-May-2010 10:17:01 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.10
16-May-2010 10:16:43 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.10
16-May-2010 10:05:45 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.10
16-May-2010 10:05:19 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.10
16-May-2010 09:42:32 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
16-May-2010 09:42:11 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
16-May-2010 09:42:09 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
16-May-2010 08:33:28 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
16-May-2010 08:33:16 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
16-May-2010 08:32:59 pm GMT	Login Success	82.205.133.9
16-May-2010 08:32:59 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9

EXHIBIT 142
000984

16-May-2010 08:32:59 pm GMT	Login Attempt	82.205.133.9
16-May-2010 08:07:42 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
16-May-2010 07:44:50 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
16-May-2010 07:44:12 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
16-May-2010 07:43:35 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
16-May-2010 07:42:46 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
16-May-2010 07:42:16 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
16-May-2010 07:41:47 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
16-May-2010 06:47:44 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
16-May-2010 06:47:14 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
16-May-2010 05:31:33 pm GMT	Login Attempt	82.205.133.9
15-May-2010 05:45:10 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
15-May-2010 04:38:18 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
15-May-2010 04:02:28 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
15-May-2010 10:48:58 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
14-May-2010 06:49:17 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
14-May-2010 12:31:08 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
13-May-2010 07:42:46 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
13-May-2010 07:34:22 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
13-May-2010 07:23:05 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
13-May-2010 07:18:39 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
13-May-2010 07:18:32 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
13-May-2010 07:18:22 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
13-May-2010 07:18:17 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
13-May-2010 05:46:54 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
13-May-2010 05:24:39 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	214.13.232.180
13-May-2010 05:24:34 pm GMT	LOGIN_ATTEMPT_AND_FAILURE	214.13.232.180
13-May-2010 05:15:52 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	214.13.232.180
13-May-2010 05:15:47 pm GMT	LOGIN_ATTEMPT_AND_FAILURE	214.13.232.180
13-May-2010 04:00:02 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
13-May-2010 06:49:32 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
13-May-2010 06:46:01 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
12-May-2010 08:37:35 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
12-May-2010 08:37:28 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
12-May-2010 08:37:24 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
12-May-2010 08:37:15 pm GMT	Login Success	82.205.133.9
12-May-2010 08:37:14 pm GMT	Login Attempt	82.205.133.9
12-May-2010 08:36:38 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
12-May-2010 07:32:37 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
11-May-2010 08:15:24 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
10-May-2010 04:28:32 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
10-May-2010 12:24:55 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
10-May-2010 12:24:45 am GMT	Login Attempt	82.205.133.9
09-May-2010 04:56:48 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
09-May-2010 04:11:40 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
09-May-2010 02:42:21 pm GMT	Login Success	82.205.133.9
09-May-2010 02:42:20 pm GMT	Login Attempt	82.205.133.9
09-May-2010 02:42:15 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
09-May-2010 02:41:56 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
09-May-2010 01:37:36 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9

EXHIBIT 142

09-May-2010 08:47:27 am GMT	Login Success	82.205.133.9
09-May-2010 08:47:26 am GMT	Login Attempt	82.205.133.9
09-May-2010 08:47:21 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
09-May-2010 06:22:58 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
08-May-2010 04:30:48 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
08-May-2010 04:30:28 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
08-May-2010 04:30:20 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
08-May-2010 04:24:55 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
08-May-2010 01:54:13 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
07-May-2010 12:16:57 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
07-May-2010 10:23:29 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
07-May-2010 10:23:22 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
07-May-2010 10:23:18 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
07-May-2010 10:23:10 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
06-May-2010 10:34:16 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
06-May-2010 02:41:47 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
06-May-2010 10:00:51 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
05-May-2010 10:50:01 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
05-May-2010 10:49:56 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
05-May-2010 10:49:49 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
05-May-2010 10:49:44 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
05-May-2010 10:49:09 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	82.205.133.9
05-May-2010 11:58:09 am GMT	Login Success	84.11.147.4
05-May-2010 11:58:08 am GMT	Login Attempt	84.11.147.4
05-May-2010 11:50:07 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	84.11.147.4
05-May-2010 04:34:37 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	84.11.147.4
05-May-2010 01:58:51 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	84.11.147.4
05-May-2010 01:57:40 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	84.11.147.4
04-May-2010 10:29:46 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	84.11.147.4
04-May-2010 10:29:43 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	84.11.147.4
04-May-2010 10:29:14 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	84.11.147.4
04-May-2010 10:23:09 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	84.11.147.4
04-May-2010 02:29:50 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	84.11.147.4
04-May-2010 12:39:40 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	84.11.147.4
04-May-2010 12:29:14 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	84.11.147.4
04-May-2010 10:33:54 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	84.11.147.4
04-May-2010 10:30:28 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	84.11.147.4
04-May-2010 10:29:25 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	84.11.147.4
04-May-2010 10:20:29 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	84.11.147.4
04-May-2010 10:18:45 am GMT	LOGIN_ATTEMPT_AND_SUCCESS	84.11.147.4

EXHIBIT 142

Exhibit(s) 143 thru 147

Page(s) 000987 thru 000996 referred to:

Federal Bureau of Investigation
Record Information/Dissemination Section
170 Marcel Drive
Winchester, Virginia 22602-4843

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID-10117

DETAILS

About 1140, 9 Aug 10, SA (b)(6)(b)(7)(C), (b) (7)(E) and SA (b)(6)(b)(7)(C), (b) (7)(E) both assigned to Washington Metro Resident Agency (WMRA), Computer Crime Investigative Unit (CCIU), Fort Belvoir, VA 22060, interviewed Mr. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) who described PFC MANNING as a "friend, who is stationed at Fort Drum."

Mr. (b)(6)(b)(7)(C) stated he first met PFC MANNING when a mutual friend, Mr. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) brought PFC MANNING to his cottage near Fort Drum, NY, located at (b)(6)(b)(7)(C) sometime between the Memorial Day and the Independence Day holidays in 2009. Mr (b)(6)(b)(7)(C) stated PFC MANNING and Mr. (b)(6)(b)(7)(C) visited him two more times, once with a young white male named (b)(6)(b)(7)(C) (NFI), before PFC MANNING left for Iraq in 2009. Mr. (b)(6)(b)(7)(C) stated while PFC MANNING stayed at the cottage, he would often attempt to engage in conversations involving political issues, but each time Mr. (b)(6)(b)(7)(C) stopped PFC MANNING and told him not to bother him (Mr. (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) stated he and Mr. (b)(6)(b)(7)(C) had been friends for several years and Mr. (b)(6)(b)(7)(C) knew him well enough to know that he (Mr. (b)(6)(b)(7)(C) was a "race car nut" and not someone who was interested in political issues.

Mr. (b)(6)(b)(7)(C) stated before PFC MANNING left for Iraq, PFC MANNING told him that he had left two boxes full of his personal property that he did not want to leave at Fort Drum, NY while he was deployed, but to have sent to his aunt in Potomac, MD. Mr. (b)(6)(b)(7)(C) stated shortly after PFC MANNING departed for Iraq, he was able to make it to Fort Drum, NY and retrieve the aforementioned boxes. Mr. (b)(6)(b)(7)(C) described the boxes as full and heavy, one of which had broken open and the other of which remained sealed.

Mr. (b)(6)(b)(7)(C) stated after he transported the boxes to his residence, he looked into the opened box and observed several items of military clothing, boots, books, and other miscellaneous items. Mr. (b)(6)(b)(7)(C) said he attempted to mail the boxes to PFC MANNING's aunt's residence per PFC MANNING's original request, but when he found out the shipping and handling would cost him a lot of money out of pocket, he decided not to and later communicated with PFC MANNING and told him that he would just safeguard the boxes for him instead.

Mr. Mr. (b)(6)(b)(7)(C) stated he would chat with PFC MANNING via AOL Instant Messenger (AIM) (Username: (b)(6)(b)(7)(C)), but discussed nothing out of ordinary or topics involving the war or classified materials; Mr. (b)(6)(b)(7)(C) would ask PFC MANNING how he was doing and PFC MANNING in return would tell him that he was doing well and nothing related to his work or amounting to anything serious. Mr. (b)(6)(b)(7)(C) stated the last time he chatted with PFC MANNING was prior to his apprehension in late May 2010. Mr. (b)(6)(b)(7)(C) stated during the last chat, PFC MANNING seemed upset because he had not been able to contact Mr. (b)(6)(b)(7)(C) for several days and asked him to get in touch with Mr. (b)(6)(b)(7)(C) on behalf of him. Mr. (b)(6)(b)(7)(C) said his primary method of communication with PFC MANNING was

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060
SIG (b)(6)(b)(7)(C), (b) (7)(E)	DATE: 16 Aug 10 / EXHIBIT: 148

DETAILS

through AIM and he had never received an e-mail, digital media in any form, or a package from PFC MANNING during his deployment in Iraq. Mr. (b)(6)(b)(7)(C) further added he did not think PFC MANNING knew the address to his residence in Rochester or to the cottage in Worth.

(b)(6)(b)(7)(C) added he still had the boxes in his house and invited SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) to his residence at (b)(6)(b)(7)(C)

Mr (b)(6)(b)(7)(C) stated he had heard of wikileaks.org, but had no interest because he was a "race car nut" and not interested in political issues. Furthermore, Mr. (b)(6)(b)(7)(C) stated he had never heard of or met anyone named (b)(6)(b)(7)(C) full ID Julian ASSANGE, full ID or persons affiliated with the WikiLeaks.

Mr. (b)(6)(b)(7)(C) consented to let SA (b)(6)(b)(7)(C) mage the internal hard drive of his laptop computer, which he had used to chat with PFC MANNING. Mr. (b)(6)(b)(7)(C) also mentioned PFC MANNING never used any of his computers nor did he give PFC MANNING permission to do so.

About 1230, 9 Aug 10, SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) located the boxes, purportedly containing PFC MANNING's property on the floor of Guest Room upstairs of Mr. (b)(6)(b)(7)(C) residence, located at (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) permitted SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) to look through the contents of the open box in his presence and gave them his consent to take the other sealed box into custody. With Mr. (b)(6)(b)(7)(C) consent, SA (b)(6)(b)(7)(C) nd SA (b)(6)(b)(7)(C) N looked through the contents of the open box in the presence of Mr. (b)(6)(b)(7)(C) The following items were found and were documented by exposing several photographs using Canon PowerShot SD 1300IS: Class "A" Jacket with PFC MANNING's name tag, rank, and unit patch, several books, hand-written notes, games, movies, CDs, and DVDs.

A cursory look at the CDs andDVDs did not indicate any items of evidentiary value or contraband; however, SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) located one CD-RW labeled "PFC Manning," which had been formatted and showed approximately 512MB free space out of 700MB. SA (b)(6)(b)(7)(C) also discovered three classification labels ((1) Secret and (2) Top Secret) in a book titled, "More than a Carpenter" by Josh McDOWELL. SA (b)(6)(b)(7)(C) collected the CD-RW, the classification labels and the sealed box of PFC MANNING's property as evidence on Evidence/Property Custody Document (EPCD), Document Number (DN) 117-10.

About 1200, 10 Aug, SA (b)(6)(b)(7)(C) coordinated with Mr. (b)(6)(b)(7)(C) to obtain an image of his personally-owned laptop computer which was utilized in chat sessions with PFC MANNING.

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE (b)(6)(b)(7)(C), (b) (7)(E)	DATE 16 Aug 10	EXHIBIT 148

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID-10117

DETAILS

AGENT's COMMENT: An attempt to image the hard drive on 9 Aug 10 was unsuccessful because of a forensic hardware failure and SA (b)(6)(b)(7)(C) purchased a new internal drive for the forensic laptop to fix the problem.

Between 1218 and 1308, 10 Aug 10, SA (b)(6)(b)(7)(C) obtained a forensic image of the laptop computer belonging to Mr (b)(6)(b)(7)(C)

Computer Make/Model:	Toshiba Satellite A015
Computer Serial Number:	66232209Q
Hard drive make/model/capacity	Hitachi Travelstar, Model HTS541080G9SA00, 80 GB
Hard drive serial number:	XKGYRDKG
Method of imaging:	ICS ImageMasster Solo III Forensic device
Type of Image:	DD
Make and model of write block:	ICS ImageMasster Solo III Forensic device

The image was verified to be an exact, bit-for-bit copy of the hard drive through a comparison of MD5 message-digest algorithm (i.e., hash) values with no errors.

Acquisition Hash:	c1850b76c36ae5c3e5b13be8f19d8120
Verify Hash:	c1850b76c36ae5c3e5b13be8f19d8120

Between 1930 and 2300, 10 Aug 10, SA (b)(6)(b)(7)(C) conducted a conversion from .dd to Encase file format (compressed) on the image taken from Mr. (b)(6)(b)(7)(C) laptop hard drive, and a hash verification. Conversion and compression successfully completed with a matching MD5 hash value. A SHA1 hash value was obtained during this operation: 593c39ff4544e0e0a152615521777638a438a2d6.

Encase image successfully loaded into Encase with a verification of matching MD5 and SHA1 hash values.

About 0815, 16 Aug 10, SA (b)(6)(b)(7)(C) transferred the Encase image of the (b)(6)(b)(7)(C) laptop hard drive to a Western Digital 74.3 GB Hard Drive, SN WMAKE1914292. A copy of the image was placed on the Image Server for examination. The collection of the WD 74.3 GB drive as evidence was documented on DA 4137, EPCD, DN 118-10///LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE (b)(6)(b)(7)(C), (b) (7)(E)	DATE 16 Aug 10	EXHIBIT 148

0028 10 CID221 10117

DEPARTMENT OF THE ARMY
UNITED STATES ARMY CRIMINAL INVESTIGATION COMMAND
COMPUTER CRIME INVESTIGATIVE UNIT
9805 LOWEN ROAD, BUILDING 193
FORT BELVOIR, VIRGINIA 22060-5598

CONSENT TO SEARCH COMPUTER/ELECTRONIC EQUIPMENT

I, (b)(6)(b)(7)(C) _____, have been asked to give my consent to the seizure and subsequent search of my computer/electronic equipment. I have been informed by the undersigned U.S. Army Criminal Investigation Command (USACIDC) Special Agent that an inquiry is being conducted in connection with the following possible violation(s) of law: Article 106a, UCMJ - Espionage
18 USC § 1030 Unauthorized access to a US Government computer

I have also been informed of my right to refuse to consent to such a search. I hereby authorize Special Agent (b)(6)(b)(7)(C) _____ and any other person(s) designated by U.S. Army Criminal Investigation Command (USACIDC), to conduct at any time a complete search of:

All computer/electronic equipment located at Davenport Machine, Inc.
167 Ames Streeet
Rochester, NY 14611

These persons are also authorized by me to enter and to take from the above location: any computer hardware and storage media, including internal hard disk drive(s), floppy diskettes, compact disks, scanners, printers, other computer/electronic hardware or software and related manuals; any other electronic storage devices, including but not limited to, personal digital assistants, cellular telephones, and electronic pagers; and any other media or materials necessary to assist in accessing the stored electronic data.

[Description of computers, data storage devices, cellular telephone, or other devices (makes, models, and serial numbers, if available)]

Hard drive, Hitachi Travelstar, Model HTS541080G9SA00, Serial Number XKGYRDKG, from a Toshiba Satellite A015 laptop, Model PSAA5U-01P00P, Serial Number 66232209Q, property of Mr. (b)(6)(b)(7)(C)

I certify that I own, possess, control, and/or have a right of access to these devices and all information found in them. I understand that any contraband or evidence on these devices may be used against me in a court of law.

I relinquish any constitutional right to privacy in these electronic devices and any information stored on them. I authorize USACIDC to make and keep a copy of any information stored on these devices. I understand that any copy made by USACIDC will become the property of USACIDC and that I will have no privacy or possessory interest in the copy.

This written permission is given by me voluntarily. I have not been threatened, placed under duress, or promised anything in exchange for my consent. I have read this form; it has been read to me; and I understand it. I understand the English _____ language and have been able to communicate with the agents/officers.

I understand that I may withdraw my consent at any time. I may also ask for a receipt for all things turned over.

Signed: (b)(6)(b)(7)(C) _____ Signature of Witnesses: (b)(6)(b)(7)(C) _____

Name: (b)(6)(b)(7)(C) _____ Name: Special Agent (b)(6)(b)(7)(C) _____

Date and Time: AUG 10 2010 Date and Time: 8/10/10 12:10 Pm

For Official Use Only
Law Enforcement Sensitive

EXHIBIT 149
001000

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID-10117

DETAILS

About 1220, 11 Aug 10, SA (b)(6)(b)(7)(C) re-interviewed SSG (b)(6)(b)(7)(C), S-4, HHC, 2nd Brigade Combat Team, 10th Mtn Div, Fort Drum, NY, who stated he did not know anyone with the names of (b)(6)(b)(7)(C) and had not had any communication with them.

SSG (b)(6)(b)(7)(C) stated he had never searched for or viewed on his personal laptop computer any videos titled "Collateral Murder" or any other videos depicting gun camera footage taken by an Apache helicopter in Iraq.

SSG (b)(6)(b)(7)(C) stated he had never visited the website "WikiLeaks.org" or any other websites related to or mentioning WikiLeaks.

SSG (b)(6)(b)(7)(C) mentioned he had never used his personal laptop computer to create any Twitter accounts or used, searched for, or was otherwise aware of the domain name "FriendFee.com".

SSG (b)(6)(b)(7)(C) stated he had a "Gmail" account, which was (b)(6)(b)(7)(C)@gmail.com, and further stated he rarely used it and had last accessed it during his last deployment in December 08-January 09.

SSG (b)(6)(b)(7)(C) stated his personal laptop computer was not password-protected and remained in his office during the deployment. SSG (b)(6)(b)(7)(C) stated to the best of his knowledge, CPL (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) Supply Clerk, HHC, 2nd Brigade Combat Team, 10TH Mtn Div, Fort Drum, NY and PFC MANNING were the only ones to use the laptop computer besides him; however, PFC MANNING used it the most. SSG (b)(6)(b)(7)(C) stated that CPL (b)(6)(b)(7)(C) had an Internet connection in her room and would only use his laptop computer to go online occasionally. SSG (b)(6)(b)(7)(C) stated the only way someone else could have used his personal laptop computer without his knowledge would be if CPL (b)(6)(b)(7)(C) let someone use it. SSG (b)(6)(b)(7)(C) stated PFC MANNING was most likely the one who used his laptop computer during the 22-24 May timeframe and further added he had not been in contact with anyone recently (in the past year), who lived in the Boston, MA area///LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE (b)(6)(b)(7)(C), (b) (7)(E)	DATE 16 Aug 10	EXHIBIT 150

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID-10117

DETAILS

About 1326, 12 Aug 10, SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C), (b) (7)(E) this office, interviewed SPC (b)(6)(b)(7)(C) (NMN) (b)(6)(b)(7)(C) S-2, HHC, 2nd Brigade Combat Team, 10th Mtn Div, Fort Drum, NY, who stated Soldiers at Forward Operating Base Hammer would chat in MIRC, an Internet Relay Chat (IRC) client for Microsoft Windows, on SIPRNet to communicate with one another and often discuss their personal issues and sometimes blatantly hit on one another, and supervisory Soldiers were not happy about it. SPC (b)(6)(b)(7)(C) stated PFC MANNING told her in passing that she should be careful with what she said because some of the chat was being logged and kept on the "T" server. SPC (b)(6)(b)(7)(C) stated PFC MANNING's warning was not without basis, given the fact that several NCO's and officers gave the same warning.

SPC (b)(6)(b)(7)(C) stated she and PFC MANNING were "Fobbits" and had never gone outside the wire.
///LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro Resident Agency Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE (b)(6)(b)(7)(C), (b) (7)(E)	DATE 16 Aug 10	EXHIBIT 151

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

About 1430, 13 Aug 10, SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C), (b) (7)(E) this office, interviewed LTC (b)(6)(b)(7)(C) U.S. Army Element - Defense Intelligence Agency, The Pentagon, Washington, DC 20001, as he was identified from emails found within PFC MANNING's Gmail email account which were discovered as the result of a forensic examination of PFC MANNING's personal laptop computer collected as evidence by CID at Forward Operating Base (FOB) Hammer, Iraq. LTC (b)(6)(b)(7)(C) who was interviewed in the presence of his assigned Trial Defense Service (TDS) Attorney, CPT (b)(6)(b)(7)(C) U.S. Army Trial Defense Service, 9910 Lowen Road, Building 702, Fort Belvoir, VA 22060, provided a verbal statement in which he related he met PFC MANNING about October 2008, but he only had in-person contact with PFC MANNING approximately five times since that time. LTC (b)(6)(b)(7)(C) stated the last time he had contact with PFC MANNING was April 2010, and that PFC MANNING did not say or give LTC (b)(6)(b)(7)(C) the impression anything was wrong. LTC (b)(6)(b)(7)(C) explained he did not notice PFC MANNING having any behavioral issues during the time he had known him, with the exception of talking with PFC MANNING on the phone wherein LTC (b)(6)(b)(7)(C) described PFC MANNING as being "flighty" shortly after PFC MANNING arrived in the U.S. from his mid-tour leave from Iraq. LTC (b)(6)(b)(7)(C) stated he knew PFC MANNING traveled to Boston, MA during his mid-tour leave in January/February 2010. LTC (b)(6)(b)(7)(C) related PFC MANNING had told him previously that he had planned to take his mid-tour leave from Iraq in the U.K.; however, LTC (b)(6)(b)(7)(C) said for an unknown reason PFC MANNING changed his mind. LTC (b)(6)(b)(7)(C) mentioned PFC MANNING apparently was going to Boston, MA on his mid-tour leave to visit a friend, which LTC (b)(6)(b)(7)(C) only knew as (b)(6)(b)(7)(C) NFI). LTC (b)(6)(b)(7)(C) further related he believed (b)(6)(b)(7)(C) attended Brandeis University. LTC (b)(6)(b)(7)(C) explained PFC MANNING arrived in the Washington, D.C. area from Iraq, spent a short time at his aunt's home, and then went to Boston, MA shortly thereafter, for what LTC (b)(6)(b)(7)(C) described as a long-weekend. LTC (b)(6)(b)(7)(C) said by the manner in which PFC MANNING talked about Boston, LTC (b)(6)(b)(7)(C) got the impression PFC MANNING had traveled to Boston, MA several times previously. LTC (b)(6)(b)(7)(C) said PFC MANNING only mentioned that he had hung around with (b)(6)(b)(7)(C) and some of (b)(6)(b)(7)(C) friends who were associated with the Massachusetts Institute of Technology (MIT). LTC (b)(6)(b)(7)(C) said he did not know anything else about any the friends of (b)(6)(b)(7)(C) that PFC MANNING mentioned. LTC (b)(6)(b)(7)(C) stated PFC MANNING had never sent him anything by U.S. Mail or similar type of parcel service while PFC MANNING was assigned in Iraq. LTC (b)(6)(b)(7)(C) explained PFC MANNING had not left any digital media or any other personal items with LTC (b)(6)(b)(7)(C) nor had PFC MANNING ever sent LTC (b)(6)(b)(7)(C) any encrypted emails. LTC (b)(6)(b)(7)(C) related PFC MANNING never mentioned the website WikiLeaks.org or any videos or documents of combat operations in Iraq and/or Afghanistan. LTC (b)(6)(b)(7)(C) said PFC MANNING did not express any political or social viewpoints which PFC MANNING seemed passionate about. LTC (b)(6)(b)(7)(C) related one incident in which PFC MANNING was in the Washington, D.C. area for training prior to his deployment to Iraq. LTC (b)(6)(b)(7)(C) further explained while PFC MANNING was in the Washington, D.C. area for training, an unidentified Staff Sergeant in PFC MANNING's training group wanted to go to a restaurant for lunch which was not reasonably accessible within the time-frame the soldiers were given for their lunch break. LTC (b)(6)(b)(7)(C) said PFC MANNING, who was familiar with the local area, reportedly told the Staff Sergeant the restaurant was too far away, causing the Staff Sergeant

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE (b)(6)(b)(7)(C)	DATE 16 Aug 10	EXHIBIT 152

FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE

DETAILS

to contact PFC MANNING's supervisor at Fort Drum to complain about PFC MANNING. LTC [redacted]was not able to elaborate as to what the result of this reported incident was. LTC [redacted] said he did not know of any other disciplinary issues involving PFC MANNING, and stated he did not know PFC MANNING had received an Article 15 while deployed to Iraq. LTC [redacted] when asked about 'Annex B' which was a term that appeared in emails between LTC [redacted]nd PFC MANNING, said Annex B most likely refers to an Intelligence Annex to a military Operations Order which PFC MANNING may have been working on as a project within his unit. LTC [redacted]related he did not have any indication PFC MANNING had any large debts or had come into any money which was unexplained. LTC [redacted]aid he knew PFC MANNING's mother was a citizen of the United Kingdom, but that he did not know of any other friends, associates, or relatives of PFC MANNING that were non-U.S. Citizens. LTC [redacted]elated he did not have any contact with anyone associated with the website WikiLeaks.org nor did he have any knowledge or participation in PFC MANNING's alleged disclosure of classified information. LTC [redacted]ould not immediately provide any additional information related to PFC MANNING.

AGENT'S COMMENT: LTC[redacted]was interviewed in the presence and with the consent of his assigned TDS attorney, CPT [redacted]who had advised LTC [redacted]f his rights in regard to being interviewed by CID in relation to this investigation. CPT [redacted]elated she would prepare a written memorandum documenting having advised LTC[redacted] of his rights and would forward this memorandum to SA [redacted] SA [redacted]noted during the initial interview of LTC [redacted]on 2 Aug 10, he was advised of his legal rights in regard to Uniform Code of Military Justice (UCMJ) Article 134 – Fraternization, as the nature of the content in emails sent between LTC [redacted] and PFC MANNING gave the appearance of a potential inappropriate relationship between a Commissioned Officer and an Enlisted member. LTC [redacted]ubsequently invoked his legal rights during the interview on 2 Aug 10, requesting to speak with legal counsel before making any statements to CID. The individual identified as [redacted]by LTC [redacted] during his interview, was previously identified as Mr. [redacted]

About 1428, 16 Aug 10, SA [redacted]received an email message from CPT [redacted]which contained an attached Memorandum related to LTC [redacted]as having been advised of his legal rights previously and having understood his rights to remain silent and to stop questioning at any time. The Memorandum further related LTC [redacted] voluntarily waived those rights in CPT [redacted] presence and fully cooperated in the interview with CID on 13 Aug 10.

// LAST ENTRY //

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA [redacted]	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE [redacted]	DATE 16 Aug 10	EXHIBIT ~~153~~ 152

Exhibit(s) 153

Page(s) 001005 referred to:

Federal Bureau of Investigation
Record Information/Dissemination Section
170 Marcel Drive
Winchester, Virginia 22602-4843

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

PAGE 1 OF 1 PAGES

DETAILS

About 1205, 17 Aug 10, SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) National Security Agency (NSA), 9800 Savage Road, Fort Meade, MD 20755, interviewed SPC (b)(6)(b)(7)(C) A Company, 741st Military Intelligence Battalion, 9802 Love Road, Fort Meade, MD 20755, as he was identified as a having been assigned with PFC MANNING while at Forward Operating Base (FOB) Hammer, Iraq. SPC (b)(6)(b)(7)(C) stated he did not know PFC MANNING very well and did not speak with him much during the time they were both assigned at FOB Hammer. SPC (b)(6)(b)(7)(C) ated he was deployed to Iraq from 15 Jan 10 through 13 Jul 10, and was assigned to FOB Hammer as part of a Cryptological Support Team that provided support to the soldiers assigned as Intelligence Analysts to the 2nd Brigade Combat Team (BCT), 10th Mountain Division. SPC (b)(6)(b)(7)(C) further referred to the 2nd BCT personnel working in the Sensitive Compartmented Information Facility (SCIF) on FOB Hammer as 'organic' personnel. SPC (b)(6)(b)(7)(C) elated he felt PFC MANNING was odd as he noticed PFC MANNING always seemed to distance himself from other personnel in his unit and/or that worked in the SCIF. SPC (b)(6)(b)(7)(C) explained he would occasionally leave the SCIF to go outside and smoke a cigarette and noticed when PFC MANNING was also outside, PFC MANNING appeared to make a point of avoiding others who were also in the area smoking, by standing by himself in a nearby bunker. SPC (b)(6)(b)(7)(C) aid he generally tried to avoid PFC MANNING while at FOB Hammer due to what he felt was odd behavior by PFC MANNING. SPC (b)(6)(b)(7)(C) elated he had heard of the incidents related to PFC MANNING having damaged a computer when told to perform some type of duty by SPC (b)(6)(b)(7)(C) who was assigned to PFC MANNING's unit. He also knew of the incident in which PFC MANNING assaulted SPC (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) also assigned to PFC MANNING's unit, while both PFC MANNING and SPC (b)(6)(b)(7)(C) were on duty in the SCIF. SPC (b)(6)(b)(7)(C) related he did not witness these incidents, but felt PFC MANNING should not have been working in the SCIF based on these events. SPC (b)(6)(b)(7)(C) provided a list of other personnel who worked in the SCIF during the time he was assigned at FOB Hammer, but could not immediately provide any additional information related to PFC MANNING or this investigation.

// **LAST ENTRY** //

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE (b)(6)(b)(7)(C)	DATE 17 Aug 10	EXHIBIT 154

FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE

Approved (b)(6)(b)(7)(C)

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

About 1120, 18 Aug 10, SA (b)(6)(b)(7)(C) SA (b)(6)(b)(7)(C) this office, and SA (b)(6)(b)(7)(C) National Security Agency (NSA), 9800 Savage Road, Fort Meade, MD 20755, interviewed U.S. Marine CPL (b)(6)(b)(7)(C) B Company, Marine Cryptological Support Battalion, 9803 Love Road, Fort Meade, MD 20755, as he was identified as an NSA assigned service member who was stationed with PFC MANNING at Forward Operating Base (FOB) Hammer, Iraq. CPL (b)(6)(b)(7)(C) stated he was assigned in Iraq from July 2009 through January 2010. CPL (b)(6)(b)(7)(C) explained he was aware of the recent disclosure of U.S. Government Classified materials to the website WikiLeaks.org, but was unaware PFC MANNING was involved; however, CPL (b)(6)(b)(7)(C) further remarked that he was not surprised by these circumstances. CPL (b)(6)(b)(7)(C) explained he was initially assigned to FOB Loyalty, Iraq for the first month or two of his tour in Iraq, before being reassigned to FOB Hammer. CPL (b)(6)(b)(7)(C) said when assigned to FOB Hammer he initially worked with members of the 3rd Brigade Combat Team (BCT) of the 82nd Airborne Division. CPL (b)(6)(b)(7)(C) related PFC MANNING's unit, the 2nd BCT, of the 10th Mountain Division, arrived in Iraq sometime in November 2009 and that he worked in the same Sensitive Compartmented Information Facility (SCIF) as PFC MANNING during his assignment there. CPL (b)(6)(b)(7)(C) said he assignment in Iraq ended in January 2010. CPL (b)(6)(b)(7)(C) explained because he was the only Digital Network Intelligence (DNI) Analyst supporting FOB Hammer, he worked a schedule which covered both of the 12-hour shifts worked by the 10th Mountain Division soldiers. CPL (b)(6)(b)(7)(C) related the shift he worked was generally 1400 to 0200, each day. CPL (b)(6)(b)(7)(C) remarked that PFC MANNING seemed to be what he described as 'bi-polar', in that PFC MANNING's moods each day would seem to vary between being fairly happy; to being sad or angry. CPL (b)(6)(b)(7)(C) related PFC MANNING had issues in getting along with other unit members and knew of at least one incident in which PFC MANNING allegedly got into some type of physical altercation with another soldier, SPC (b)(6)(b)(7)(C), who was assigned to PFC MANNING's unit. CPL (b)(6)(b)(7)(C) said he was not a witness to this incident where PFC MANNING apparently damaged some government property by flipping a table containing computer equipment, but knew about this incident second-hand. CPL (b)(6)(b)(7)(C) explained SPC (b)(6)(b)(7)(C) was formerly a U.S. Marine who had transferred into the U.S. Army and had mentioned the incident involving PFC MANNING. CPL (b)(6)(b)(7)(C) said he was surprised that PFC MANNING was allowed to continue working in the SCIF after this incident, as behavior like this could be grounds for eliminating personnel from further access to a SCIF facility. CPL (b)(6)(b)(7)(C) said he believed PFC MANNING would have talked with Senior Airman (SrA) (b)(6)(b)(7)(C) also formerly assigned to Cryptological Support Team 5 (CST5), or himself the most out of any of the CST5 assigned personnel at FOB Hammer. CPL (b)(6)(b)(7)(C) stated he did not feel SrA (b)(6)(b)(7)(C) or himself spoke with PFC MANNING aside from day-to-day greetings and casual passing conversation. CPL (b)(6)(b)(7)(C) said he generally did not have any direct interaction with PFC MANNING while working in the SCIF based on the level of classified information a DNI Analyst works with, which few personnel assigned to FOB Hammer were authorized to view. CPL (b)(6)(b)(7)(C) related he could not remember a time in which PFC MANNING asked him any hypothetical questions which may have been related to PFC MANNING's own alleged unlawful activities; he was unaware of any computer applications known as 'OTR' or 'Off-The-Record'; had not heard any discussions relating to NSA's activities associated with the iPhone device; and did not know about any naturalized U.S. Citizens being tracked by NSA personnel while at FOB Hammer which PFC MANNING may have been involved with. CPL (b)(6)(b)(7)(C) aid he is knowledgeable about the Foreign Intelligence

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNAT (b)(6)(b)(7)(C)	DATE 18 Aug 10	EXHIBIT 155

FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE

Approved_____

DETAILS

Surveillance Act (FISA), but would have never discussed this type of information with PFC MANNING. CPL (b)(6)(b)(7)(C) related, when asked about comments PFC MANNING made during Internet chat conversations with Mr. (b)(6)(b)(7)(C) in regard to recognizing data he saw as '9/11 Pager Messages', he believed something like what PFC MANNING described may have come from an NSA system which he provided the name for. CPL (b)(6)(b)(7)(C) aid he would not have disclosed this information to PFC MANNING, but was only making a guess as to where PFC MANNING may have learned of this information. CPL (b)(6)(b)(7)(C) ated he could not remember any additional personnel he was assigned within Iraq that he would have described as a friend of PFC MANNING or someone PFC MANNING would have associated with. CPL (b)(6)(b)(7)(C) could not immediately provide any additional information relevant to this investigation.

AGENT'S COMMENT: The NSA system from which CPL (b)(6)(b)(7)(C) said PFC MANNING may have learned about the '9/11 Pager Messages' mentioned in PFC MANNING Internet chat conversations with Mr. (b)(6)(b)(7)(C) was not listed here as this system name may itself be classified.

// **LAST ENTRY** //

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060
SIGN (b)(6)(b)(7)(C)	DATE: 18 Aug 10 / EXHIBIT: 155

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

About 1459, 13 Aug 10, SA (b)(6)(b)(7)(C) received an email from Mr. (b)(6)(b)(7)(C) Army Knowledge Online (AKO), Security, 10119 Beach Road, Fort Belvoir, VA 22060-5801, containing an Excel spreadsheet purportedly containing the To and From header information for the AKO account of LTC (b)(6)(b)(7)(C)

About 1233, 16 Aug 10, SA (b)(6)(b)(7)(C) copied the header data to a compact disc (CD) for preservation and analysis. SA (b)(6)(b)(7)(C) reviewed LTC (b)(6)(b)(7)(C) AKO account To and From header information and ascertained the dates provided were from 7 Aug 01 - 10 May 05. SA (b)(6)(b)(7)(C) reviewed the email addresses of those who sent or received email from LTC (b)(6)(b)(7)(C), none of which match the email address of PFC MANNING.

About 1049, 18 Aug 10, SA (b)(6)(b)(7)(C) received an email from Mr. (b)(6)(b)(7)(C) AKO Security, containing the AKO logs of PFC Bradley MANNING's AKO account. SA (b)(6)(b)(7)(C) copied the message and files to CD and collected the CD as evidence. SA (b)(6)(b)(7)(C) annotated the collection on a DA Form 4137, Evidence/Property Custody Document (EPCD), DN 120-10.

//LAST ENTRY//

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE (b)(6)(b)(7)(C)	DATE 18 Aug 10	EXHIBIT 156

Exhibit(s) 157

Page(s) 001010 withheld.

5 U.S.C. § 552(b)(6) & (b)(7)(C)
Third Party Information
Not Reasonably Segregable

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

About 1527, 25 Aug 10, SA (b)(6)(b)(7)(C) conducted a telephonic re-interview of MSG (b)(6)(b)(7)(C) Headquarters and Headquarters Company (HHC), 2nd Brigade Combat Team (2 BCT), 10th Mountain Division (10 Mtn Div), 10112 4th Armored Division Drive, Fort Drum, NY 13602 (FDNY), who stated SIPR computers used in SCIF at Forward Operating Base (FOB) Hammer, Iraq (IZ), would often "crash" due to the environmental causes and frequently needed to be either replaced or re-imaged/base-lined; however, MSG (b)(6)(b)(7)(C) could not recall whether or not PFC MANNING's computer(s) was crashed and had to be replaced or re-imaged/base-lined or otherwise repaired. MSG (b)(6)(b)(7)(C) stated he believed US Army CID agents had collected a total of three computers reportedly used by PFC MANNING; two of which were the property of 2 BCT while the other one was Theatre Provided Equipment (TPE). MSG (b)(6)(b)(7)(C) stated he believed he had originally signed for approximately 12 TPE computers at FOB Hammer, IZ. MSG (b)(6)(b)(7)(C) described the re-deployment process and stated all of the hard drives from SIPR computers were removed and stored in a Pelican-type case and the case placed in a SECRET-accredited CONEX. MSG (b)(6)(b)(7)(C) stated NIPR and SIPR computers without internal hard drives were then placed in another CONEX. MSG (b)(6)(b)(7)(C) stated none of the hard drives should have been wiped, altered, over-written, and/or modified.

About 1624, 25 Aug 10, SA (b)(6)(b)(7)(C) conducted a telephonic interview of CPT (b)(6)(b)(7)(C) Officer on Charge (OIC), S-2, HHC, 2 BCT, 10 Mtn Div, FDNY, who stated SIPR computers used in SCIF at FOB Hammer, IZ, would frequently "crash" and, as a matter of fact, his computer had to be repaired three different times while he was at FOB Hammer, IZ. CPT (b)(6)(b)(7)(C) stated Mr. (b)(6)(b)(7)(C) (later fully identified as Mr. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) was the System Administrator of the Distributed Common Ground System - Army (DCGS-A) systems at FOB Hammer and was in charge of the system maintenance, operations, and all of its hardware and peripherals. CPT (b)(6)(b)(7)(C) stated he believed each time his computer crashed, Mr. (b)(6)(b)(7)(C) would either wipe the hard drive and rebuild it or replace the unit. CPT (b)(6)(b)(7)(C) stated DCGS-A computers were highly temperamental and sensitive to the harsh environment. CPT (b)(6)(b)(7)(C) stated the DCGS-A computers were strictly maintained by Mr. (b)(6)(b)(7)(C) and no soldiers from the unit S-6 shop were allowed to have administrator-level privileges to the system and its hardware and peripherals. CPT (b)(6)(b)(7)(C) stated he believed there were about 10 to 12 DCGS-A computers used in the SCIF at FOB Hammer and all were stay-behind TPEs and would more than likely have been re-imaged/based-lined and re-distributed through IZ. CPT (b)(6)(b)(7)(C) further stated only two or three 2 BCT owned SIPR computers were used in the SCIF and they should been all backed up on the SIPR server and then wiped cleaned. CPT (b)(6)(b)(7)(C) stated in preparation for re-deployment, all SIPR had drives were backed-up on the SIPR server and wiped clean and only a few SIPR computers were hand-carried back because the sensitive item CONEX had already been sealed and shipped. CPT (b)(6)(b)(7)(C) stated the hand-carried back computers should have been secured in the SECRET vault of each perspective unit. CPT (b)(6)(b)(7)(C) further mentioned it was the mission of the S-2, HHC, 2 BCT, 10th Mtn Div, while at FOB Hammer, IZ, to enable Iraqi Security Forces through the Foreign Disclosure process by providing them with the most timely, accurate, and objective intelligence so that the Iraqi Security Forces could be successful in their mission.

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE (b)(6)(b)(7)(C), (b) (7)(E)	DATE 18 Aug 10	EXHIBIT 158

DETAILS

About 1700, 26 Aug 10, SA [redacted] conducted a telephonic interview of Mr. [redacted] Contractor, DCGS-A System Administrator, Camp Ramadi, IZ, who stated he was the DCGS-A system Administrator for S-2, HHC, 2 BCT, 10th Mtn Div at FOB HAMMER, IZ, for the duration of their deployment and he specifically recalled PFC MANNING's DCGS-A SIPR computer "crashed" at least twice from the time PFC MANNING started working in the SCIF to the time he was apprehended in May 2010. Mr. [redacted] stated Windows Explorer on his computer would frequently lock up and applications on the computer would not open. Mr. [redacted] stated that on one occasion, he asked PFC MANNING if he was "messing around" on the computer, to which PFC MANNING replied that he used to work at a computer repair shop (NFI) and was somewhat computer savvy, but denied having altered and/or modified his computer. Mr. [redacted] stated that when he re-imaged "crashed computers", he would use software to restore current settings and should it fail, he would base-line by overwriting all previously imaged settings. Mr. [redacted] stated there were only 10 to 12 DCGS-A SIPR computers used in SCIF at FOB Hammer, IZ, and when S-2, HHC, 2 BCT, 10 Mtn Div redeployed, the computers were more than likely wiped clean and redistributed through IZ. Mr. [redacted] further mentioned he believed Mr. [redacted] (NFI) would be able to provide further information pertaining to the current whereabouts of the DCGS-A computers.

About 1835, 31 Aug 10, SA [redacted] conducted a telephonic interview of SPC [redacted] Provost Marshal's Office (PMO), 2 BCT, 10 Mtn Div, FDNY who stated while he was giving SA [redacted] (US Army CID Agent) a ride to the FOB Hammer Landing Zone (LZ), he heard SA [redacted] mention that she had not been able to locate SPC [redacted] and still needed to talk to her and further take a look at her computer. SPC [redacted] stated he told SA [redacted] that he knew where SPC [redacted] lived and drove SA [redacted] to SPC [redacted] Place of Dwelling (POD). SPC [redacted] stated he walked up to SPC [redacted] POD and knocked on her door and was greeted by SPC [redacted] SPC [redacted] stated when he told SPC [redacted] there was a CID agent looking for her, her face turned red and she told him, "I only checked his (PFC MANNING's) emails...I was just being his friend." SPC [redacted] recalled SPC [redacted] was obviously nervous and concerned, but he did not think she was lying or trying to hide something. SPC [redacted] stated that shortly thereafter SPC [redacted] was interviewed by SA [redacted] and since that day he and SPC [redacted] had not had any discussion pertaining to PFC MANNING or that encounter. SPC [redacted] stated at no time SPC [redacted] told him that she had mailed any package or had done anything else other than checking PFC MANNING's e-mails nor did he tell anyone that SPC [redacted] had sent and/or received any package for PFC MANNING.

//LAST ENTRY//

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION
SA [redacted]	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060
SIGNATURE [redacted]	DATE: 18 Aug 10 / EXHIBIT: 158

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

About 1604, 23 Aug 10, SA [redacted] coordinated with SA [redacted] For Drum CID Office, 10705 South Riva Ridge Loop, Fort Drum, NY 13602, in regard to classified material nondisclosure agreements PFC MANNING signed which should have been on file with PFC MANNING's unit. SA [redacted] received from SA [redacted] the DD Form 1847-1, Sensitive Compartmented Information Nondisclosure Statement, dated 22 Jan 09, signed by PFC MANNING; and the Standard Form 312, Classified information Nondisclosure Agreement, dated 17 Sep 08, signed by PFC MANNING.

AGENT'S COMMENT: The aforementioned documents spell out the obligations to protect classified information and the potential penalties for wrongful disclosure of classified information. PFC MANNING was noted to have signed both of these documents prior to his deployment to Iraq.

//LAST ENTRY//

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION
SA [redacted]	Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060
SIGNATURE FOR [redacted]	DATE: 23 Aug 10 / EXHIBIT: ~~158~~ 159

0028 10 CID22 10117

SENSITIVE COMPARTMENTED INFORMATION NONDISCLOSURE STATEMENT

0172-10-CID452-

PRIVACY ACT STATEMENT

0172-10-CID452-

AUTHORITY: EO 9397, November 1943 (SSN).

PRINCIPAL PURPOSE(S): The information contained herein will be used to precisely identify individuals when it is necessary to certify their access to sensitive compartmented information.

ROUTINE USE(S): Blanket routine uses, as published by Defense Intelligence Agency in the Federal Register.

DISCLOSURE: Voluntary; however, failure to provide requested information may result in delaying the processing of your certification.

SECTION A

An Agreement Between MANNING, BRADLEY EDWARD and the United States.

(Printed or Typed Name)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to information or material protected within Special Access Programs, hereinafter referred to in this Agreement as Sensitive Compartmented Information (SCI). I have been advised that SCI involves or derives from intelligence sources or methods and is classified or in the process of a classification determination under the standards of Executive Order 12356 or other Executive order or statute. I understand and accept that by being granted access to SCI, special confidence and trust shall be placed in me by the United States Government. (b)(6)(b)(7)(C)

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of SCI, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and I understand these procedures. I understand that I may be required to sign subsequent agreements upon being granted access to different categories of SCI. I further understand that all my obligations under this Agreement continue to exist whether or not I am required to sign such subsequent agreements. (b)(6)(b)(7)(C)

3. I have been advised that unauthorized disclosure, unauthorized retention, or negligent handling of SCI by me could cause irreparable injury to the United States or be used to advantage by a foreign nation. I hereby agree that I will never divulge anything marked as SCI or that I know to be SCI to anyone who is not authorized to receive it without prior written authorization from the United States Government department or agency (hereinafter Department or Agency) that last authorized my access to SCI. I understand that it is my responsibility to consult with appropriate management authorities in the Department or Agency that last authorized my access to SCI, whether or not I am still employed by or associated with that Department or Agency or a contractor thereof, in order to ensure that I know whether information or material within my knowledge or control that I have reason to believe might be SCI, or related to or derived from SCI, is considered by such Department or Agency to be SCI. I further understand that I am also obligated by law and regulation not to disclose any classified information or material in an unauthorized fashion. (b)(6)(b)(7)(C)

4. In consideration of being granted access to SCI and of being assigned or retained in a position of special confidence and trust requiring access to SCI, I hereby agree to submit for security review by the Department or Agency that last authorized my access to such information or material, any writing or other preparation in any form, including a work of fiction, that contains or purports to contain any SCI or description of activities that produce or relate to SCI or that I (b)(6)(b)(7)(C)

4. *(Continued)* have reason to believe are derived from SCI, that I contemplate disclosing to any person not authorized to have access to SCI or that I have prepared for public disclosure. I understand and agree that my obligation to submit such preparations for review applies during the course of my access to SCI and thereafter, and I agree to make any required submissions prior to discussing the preparation with, or showing it to, anyone who is not authorized to have access to SCI. I further agree that I will not disclose the contents of such preparation to any person not authorized to have access to SCI until I have received written authorization from the Department or Agency that last authorized my access to SCI that such disclosure is permitted. (b)(6)(b)(7)(C)

5. I understand that the purpose of the review described in paragraph 4 is to give the United States a reasonable opportunity to determine whether the preparation submitted pursuant to paragraph 4 set forth any SCI. I further understand that the Department or Agency to which I have made a submission will act upon them, coordinating within the Intelligence Community when appropriate, and make a response to me within a reasonable time, not to exceed 30 working days from date of receipt. (b)(6)(b)(7)(C)

6. I have been advised that any breach of this Agreement may result in the termination of my access to SCI and removal from a position of special confidence and trust requiring such access, as well as the termination of my employment or other relationships with any Department or Agency that provides me with access to SCI. In addition, I have been advised that any unauthorized disclosure of SCI by me may constitute violations of United States criminal laws, including the provisions of Sections 793, 794, 798, and 952, Title 18, United States Code, and of Section 783(b), Title 50, United States Code. Nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation. (b)(6)(b)(7)(C)

7. I understand that the United States Government may seek any remedy available to it to enforce this Agreement, including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. I have been advised that the action can be brought against me in any of the several appropriate United States District Courts where the United States Government may elect to file the action. Court costs and reasonable attorneys' fees incurred by the United States Government may be assessed against me if I lose such action. (b)(6)(b)(7)(C)

8. I understand that all information to which I may obtain access by signing this Agreement is now and will remain the property of the United States Government unless and until otherwise determined by an appropriate official or final ruling of a

EXHIBIT encl 3

001014

EXHIBIT 160

8. *(Continued)* court of law. Subject to this determination, I do not now, nor will I ever, possess any right, interest, title or claim whatsoever to such information. I agree that I shall return all materials that may have come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the United States Government entity providing me access to such materials. If I do not return such materials upon request, I understand this may be a violation of Section 793, Title 18, United States Code. (b)(6)(b)(7)(C)

9. Unless and until I am released in writing by an authorized representative of the Department or Agency that last provided me with access to SCI, I understand that all the conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to SCI, and at all times thereafter. (b)(6)(b)(7)(C)

10. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect. This Agreement concerns SCI and does not set forth such other conditions and obligations not related to SCI as may now or hereafter pertain to my employment by or assignment or relationship with the Department or Agency. (b)(6)(b)(7)(C)

11. These restrictions are consistent with and do not supersede conflict with or otherwise alter the employee obligations, rights, or liabilities created by Executive Order 12356; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act

11. *(Continued)* (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 USC 421 et seq.) (governing disclosures that could expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Section 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 USC Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling. (b)(6)(b)(7)(C)

12. I have read this Agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available Sections 793, 794, 798, and 952 of Title 18, United States Code, and Section 783(b) of Title 50, United States Code, and Executive Order 12356, as amended, so that I may read them at this time, if I so choose. (b)(6)(b)(7)(C)

13. I hereby assign to the United States Government all rights, title and interest, and all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation not consistent with the terms of this Agreement. (b)(6)(b)(7)(C)

14. This Agreement shall be interpreted under and in conformance with the laws of the United States. (b)(6)(b)(7)(C)

15. I make this Agreement without any mental reservation or purpose of evasion. (b)(6)(b)(7)(C)

16. TYPED OR PRINTED NAME *(Last, First, Middle Initial)*	17. GRADE/RANK/SVC	18. SOCIAL SECURITY NO.	19. BILLET NO. *(Optional)*
MANNING, BRADLEY E	E3/PFC	(b)(6)(b)(7)(C)	
20. ORGANIZATION	**21. SIGNATURE**	**22. DATE SIGNED** *(YYMMDD)*	
HHC, S2 2 BCT 10TH MTN DIV	(b)(6)(b)(7)(C) redacted	090122	

FOR USE BY MILITARY AND GOVERNMENT CIVILIAN PERSONNEL

SECTION B

The execution of this Agreement was witnessed by the undersigned, who accepted it on behalf of the United States Government as a prior condition of access to Sensitive Compartmented Information.

23. TYPED OR PRINTED NAME *(Last, First, Middle Initial)*	24. ORGANIZATION	
(b)(6)(b)(7)(C) redacted	HHC 2BCT 10TH MTN DIV (CIV)	
25. SIGNATURE		**26. DATE SIGNED** *(YYMMDD)*
(b)(6)(b)(7)(C) redacted		090124

FOR USE BY CONTRACTORS/CONSULTANTS/NON-GOVERNMENT PERSONNEL

SECTION C

The execution of this Agreement was witnessed by the undersigned.

27. TYPED OR PRINTED NAME *(Last, First, Middle Initial)*	28. ORGANIZATION	
29. SIGNATURE		**30. DATE SIGNED** *(YYMMDD)*

SECTION D

This Agreement was accepted by the undersigned on behalf of the United States Government as a prior condition of access to Sensitive Compartmented Information.

31. TYPED OR PRINTED NAME *(Last, First, Middle Initial)*	32. ORGANIZATION	
33. SIGNATURE		**34. DATE SIGNED** *(YYMMDD)*

DD FORM 1847-1, DEC 91 (BACK)

002R 10 CID221 10117

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN MANNING, Bradley AND THE UNITED STATES

(Name of Individual - Printed or typed)

0172-10-CID452-

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12958, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.2, 1.3, and 14(e) of Executive Order 12958, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of the information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, *952 and 1924, Title 18, United States Code, * the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Section 793 and/or 1924, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

(Continue on reverse.)

EXHIBIT 10010

10. These restrictions are consistent with and supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12356; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, 952 and 1924 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this Agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER (See Notice below)
(b)(6)(b)(7)(C)	17 SEP 08	(b)(6)(b)(7)(C)

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) *(Type or Print)*

Manning, Bradley Edward
10100 N. Riva Ridge LP
Ft Drum, NY 13602

WITNESS		ACCEPTANCE	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.	
(b)(6)(b)(7)(C)	DATE 17 Sep 08	SIGNATURE	DATE
(b)(6)(b)(7)(C) 10100 N. Riva Ridge Loop FT. Drum, NY 13601		NAME AND ADDRESS *(Type or print)* (b)(6)(b)(7)(C) 10100 N. Riva Ridge Loop FT. Drum, NY 13601	

SECURITY DEBRIEFING ACKNOWLEDGMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE

NAME OF WITNESS *(Type or print)*	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

* NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

Exhibit(s) 162 and 163

Page(s) 001018 thru 001024 referred to:

Federal Bureau of Investigation
Record Information/Dissemination Section
170 Marcel Drive
Winchester, Virginia 22602-4843

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

About 1100, 17 Aug 10, SA (b)(6)(b)(7)(C), (b) (7)(E) and SA (b)(6)(b)(7)(C), (b) (7)(E) both assigned to Washington Metro Resident Agency (WMRA), Computer Crime Investigative Unit (CCIU), Fort Belvoir, VA 22060, traveled to the United States Central Command (CENTCOM), MacDill Air Force Base, FL 33621 (MAFBFL) to image a server reportedly containing some of the files which were allegedly downloaded by PFC Bradley E. MANNING. SA (b)(6)(b)(7)(C) Special Agent-in-Charge (SAC), Digital Forensics and Research Branch (DFRB), CCIU, requested that this agent obtain an EnCase image of the folder "FARAH", reportedly located in the files belonging to the Staff Judge Advocate (SJA). SA (b)(6)(b)(7)(C) also requested agents from this office obtain the server data connection logs from December 2009 through the present, containing the IP addresses of computers accessing the folder "FARAH" on the CENTCOM server.

About 0930, 18 Aug 10, SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) coordinated with Mrs. (b)(6)(b)(7)(C) GS-13 equivalent, Branch Chief, Information Assurance (IA) Branch, J6, CENTCOM, MAFBFL, and briefed her on what information this office was seeking and needed to locate and image. Mrs. (b)(6)(b)(7)(C) stated MG (b)(6)(b)(7)(C) Chief of Staff, CENTCOM, MAFBFL, needed to approve the request before agents from this office could conduct aforementioned investigative activities. Shortly thereafter, Mrs. (b)(6)(b)(7)(C) and Mrs. (b)(6)(b)(7)(C) Senior Watch Officer, Network Operations, J6, CENTCOM, MAFBFL, prepared a briefing packet for MG (b)(6)(b)(7)(C) About 1500, 18 Aug 10, Mrs. (b)(6)(b)(7)(C) stated she hand-carried the packet to her supervisor COL (b)(6)(b)(7)(C) J6, CENTCOM, MAFBFL for his review.

About 1100, 19 Aug 10, Mrs. (b)(6)(b)(7)(C) assigned Mr. (b)(6)(b)(7)(C), Senior INFOSEC Analyst, IA Branch, J6, CENTCOM, MAFBFL, to assist agents from this office. As per CENTCOM policy, the two CCIU SATA hard drives SA (b)(6)(b)(7)(C) brought to collect evidence were scanned by Mr. (b)(6)(b)(7)(C) who found no signs of malware or viruses on the drives and subsequently approved the drives for evidence collection.

Between 1300 and 1450, 19 Aug 10, Mr. (b)(6)(b)(7)(C) conducted searches for "Farah", "Gharani", "Strike2" and "BE22" on the CENTCOM web servers and was able to locate the file BE22.zip in a folder belonging to the CENTCOM Public Affairs Office (PAO). Further investigation revealed that the PAO had been given copies of the Gharani videos in zip file format in preparation for possible release by the website WikiLeaks. It was therefore determined that the PAO folder was not the location from which PFC MANNING had allegedly downloaded the files.

About 1500, 19 Aug 10, SA (b)(6)(b)(7)(C) consulted with SA (b)(6)(b)(7)(C) on the location of the "FARAH" folder. SA (b)(6)(b)(7)(C) provided the Uniform Resource Locator (URL)

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION Washington Metro Resident Agency Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SA (b)(6)(b)(7)(C), (b) (7)(E)		
SIGNATURE SA (b)(6)(b)(7)(C)	DATE 23 Aug 10	EXHIBIT 164

DETAILS

www.nonrel.cie.centcom.smil.mil/JADocumentspage/investigations/FARAH. Mr. (b)(6)(b)(7)(C) reviewed the URL and determined that the files were not stored on a traditional web server, but were stored in a Microsoft SharePoint, Structured Query Language (SQL) Server database, which was enabled to be accessible using a web-based portal. The SharePoint servers were identified by the IP addresses 131.240.47.33 (the SharePoint database cluster), 131.240.47.6 and 131.240.47.7 (web portal front end). It was determined that the folder structure a user saw when accessing the portal was symbolic and did not actually exist as traditional folders would on a standard Microsoft server.

About 1510, 19 Aug 10, SA (b)(6)(b)(7)(C) inquired about the size of the SharePoint SQL database, to which Mr (b)(6)(b)(7)(C) replied and stated he did not know the exact size, but at a minimum it was several terabytes in size. SA (b)(6)(b)(7)(C) so coordinated with Mr (b)(6)(b)(7)(C) Principle IA/Computer Network Defense (CND) Manager, IA Branch, J6, MAFBFL, in order to determine if the entire database could be imaged. Mr. (b)(6)(b)(7)(C) stated imaging the database would require taking the SharePoint system off-line, therefore rendering the entire CENTCOM document library inaccessible by field personnel and for the imaged database to be meaningful and forensically sound, the image would have to be reconstituted in a SQL Server database.

About 1600, 19 Aug, 10, SA (b)(6)(b)(7)(C) and Mr. (b)(6)(b)(7)(C) attempted to copy the entire "FARAH" folder and move it out of SharePoint onto the local machine; however, because the folders were symbolic, all attempts to download or save a group of files or an entire folder met with negative results. It was determined the best course of action, and the most forensically sound method of collection, would be downloading and saving each individual file and a corresponding screen shot. SA (b)(6)(b)(7)(C) further coordinated with SA (b)(6)(b)(7)(C) who concurred with the aforementioned collection method and further opined it would be the mostly forensically sound image available.

About 1704, 19 Aug 10, Mrs. (b)(6)(b)(7)(C) and Mrs. (b)(6)(b)(7)(C) Senior Watch Officer, Network Operations, J6, CENTCOM, MAFBFL, notified agents from this office MG (b)(6)(b)(7)(C) Chief of Staff, CENTCOM, MAFBFL, had finally approved the request to image and search the server and further authorized the release of the data. [AGENT'S COMMENTS: CCIU had forwarded a formal, written request through the OSJA to the CENTCOM G-6 requesting release of this information on 9 Aug 10.]

About 1730, 19 Aug 10, Mr. (b)(6)(b)(7)(C) prepared a laptop computer for SA (b)(6)(b)(7)(C) use. Mr. (b)(6)(b)(7)(C) wiped the laptop's hard drive and re-installed Windows XP with Service Pack 3. The laptop was identified as a Dell Latitude, Model D820, Host Name: C058077, IP Address: 131.240.22.118, Subnet:

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION Washington Metro Resident Agency Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SA (b)(6)(b)(7)(C), (b) (7)(E)		
SIGNATURE SA (b)(6)(b)(7)(C)	DATE 23 Aug 10	EXHIBIT 164

DETAILS

255.255.255.224, Mac Address: 00-19-B9-66-5D-47, Serial Number: CN-OJF240-48643-738-0236. The laptop was then connected to the SIPR network.

About 1031, 20 Aug, 10, SA (b)(6)(b)(7)(C) connected a CCIU-issued Voyager drive dock to the laptop via a USB cable. SA (b)(6)(b)(7)(C) connected a 400 GB Seagate Barracuda, SATA hard drive (Serial Number: 3NFODYJ1) to the laptop using the drive dock and assigned that drive the letter "X". Using Microsoft's Internet Explorer, SA (b)(6)(b)(7)(C) navigated to the page www.nonrel.cie.centcom.smil.mil. From this screen, SA (b)(6)(b)(7)(C) clicked on "Organization" link. SA (b)(6)(b)(7)(C) created a screen capture of this page and saved it in a folder in the Desktop Directory called "screen shots". From this screen, SA (b)(6)(b)(7)(C) clicked on "Special Staff" link. SA (b)(6)(b)(7)(C) created a screen capture of this page and saved it in the "screen shots" folder. From this screen, SA (b)(6)(b)(7)(C) clicked on "Judge Advocate" link. SA (b)(6)(b)(7)(C) created a screen capture of this page and saved it in the "screen shots" folder. From this screen, SA (b)(6)(b)(7)(C) clicked on "JA Document Page" link. SA (b)(6)(b)(7)(C) created a screen capture of this page and saved it in the "screen shots" folder. From this screen, SA (b)(6)(b)(7)(C) clicked on the folder icon "Investigations". SA (b)(6)(b)(7)(C) created a screen capture of this page and saved it in the "Investigations" folder. From this screen, SA (b)(6)(b)(7)(C) clicked on the folder icon "FARAH". SA (b)(6)(b)(7)(C) created a screen capture of this page and saved it in the "screen shots" folder. The folder "FARAH" contained the following sub-folders, "Admin Material", "Briefs", "Email", Investigations Tabs", "Reports and Exsums", "Timelines", and "Videos". SA (b)(6)(b)(7)(C) navigated to each of the sub-folders and created a screen capture for each page then saved it in the "screen shots" folder. The screen shots showed how the SharePoint portal was arraigned and the path to the "FARAH" folder.

About 1232, 20 Aug 10, SA (b)(6)(b)(7)(C) recreated the folder "FARAH" on the Desktop Directory of the laptop and included all of the subfolders that resided in the "FARAH" folder. SA (b)(6)(b)(7)(C) then downloaded each individual file contained in the folder "FARAH" into the same location inside the recreated "FARAH" folder on the Desktop Directory of the laptop computer. After verifying that all of the files downloaded correctly, SA (b)(6)(b)(7)(C) installed EnCase version 6.14.3 on the laptop computer. Using EnCase, SA (b)(6)(b)(7)(C) created logical evidence file of the folder "FARAH" and all of its sub-folders. The logical evidence file was named JA-Investigations-Farah Folder.LO1. An MD5 hash of 46e11229a5d678cabf9c3fa6839f662c was obtained and recorded. The logical evidence file of the folder "FARAH" was placed in a folder named "EnCase" on the root of the "X" drive connected to the laptop. SA (b)(6)(b)(7)(C) also copied the recreated "FARAH" folder and all of the sub-folders and placed them onto the root of the "X" drive. Subsequently the folder "Screen Shots" was then copied by SA (b)(6)(b)(7)(C) and placed on the root of the "X" drive as well.

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION Washington Metro Resident Agency Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SA (b)(6)(b)(7)(C), (b) (7)(E)		
SIGNATURE SA (b)(6)(b)(7)(C)	DATE 23 Aug 10	EXHIBIT 164

DETAILS

About 1308, 20 Aug 10, SA (b)(6)(b)(7)(C) connected a second 400 GB Seagate Barracuda, SATA hard drive (Serial Number: 3NFOHTG4) to the laptop using the drive dock and assigned that drive the letter "Y". SA (b)(6)(b)(7)(C) then recreated the process a second time placing the folder EnCase, containing the EnCase logical evidence file for the folder "FARAH", the recreated folder "FARAH", and the folder "Screen Shots" onto the root of the "Y" drive. The second evidence drive was created as a backup in case the first evidence drive suffered a failure.

Between 1307 and 1501 SA (b)(6)(b)(7)(C) collected as evidence two SATA hard drives, containing images of three folders (EnCase, FARAH and Screen Shots), copied from the CENTCOM Sharepoint server IP address 131.240.47.33, which was documented on Evidence/Property Custody Document (EPCD), Document Number (DN) 123-10

About 1613 SA (b)(6)(b)(7)(C) collected as evidence one DVD containing the SharePoint usage data logs, from Mr. (b)(6)(b)(7)(C) which was documented on EPCD, DN 122-10.

AGENT'S COMMENTS: It should be noted that when SA (b)(6)(b)(7)(C) accessed the URL: www.nonrel.cie.centcom.smil.mil, there was no login or password window on the main page. SA (b)(6)(b)(7)(C) was able to navigate to any page and access all folders and documents in the document library, including the SJA Investigations folder and the FARAH folder without ever entering any authentication or credential information. ////LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION Washington Metro Resident Agency Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SA (b)(6)(b)(7)(C), (b) (7)(E)		
SIGNATURE SA (b)(6)(b)(7)(C)	DATE 23 Aug 10	EXHIBIT 164

AGENT'S INVESTIGATION REPORT CID Regulation 195-1	ROI NUMBER 0028-10-CID221-10117 0388-10-CID014- PAGE 1 OF 1 PAGES

DETAILS

About 1455, 24 Aug 10, this office received a Request For Assistance (RFA) (0028-10-CID221-10117), from the Arizona Branch Office (ABO), Computer Crime Investigative Unit (CCIU), Fort Huachuca, AZ, which requested the interview of SFC (b)(6)(b)(7)(C) Headquarters and Headquarters Troop (HHT), 6th Squadron, 1st Cavalry Regiment, 1st Armored Division (AD), Fort Bliss, TX, 79916; pertaining to any knowledge he may have regarding the unauthorized disclosure of information by PFC Bradley E. MANNING, Headquarters and Headquarters Company (HHC), 2nd Brigade Combat Team (BCT), 10th Mountain Division (MTN DIV), Forward Operating Base (FOB) Hammer, Iraq.

About 1550, 24 Aug 10, SFC (b)(6)(b)(7)(C) was interviewed and stated he had no recollection of any Soldier by the name of PFC MANNING. SFC (b)(6)(b)(7)(C) further stated he had no knowledge of a Soldier receiving corrective action/training for violating OPSEC. SFC (b)(6)(b)(7)(C) did verify he was formerly assigned to Fort Huachuca, AZ, as a Drill Sergeant.

About 1630, 24 Aug 10, SA (b)(6)(b)(7)(C) briefed SA (b)(6)(b)(7)(C) Special Agent in Charge, ABO, CCIU, concerning the interview of SFC (b)(6)(b)(7)(C) SA (b)(6)(b)(7)(C) stated no further investigative assistance was required. ///LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Fort Bliss CID Office Fort Bliss, TX 79916	
SIGNATURE (b)(6)(b)(7)(C)	DATE 24 Aug 10	EXHIBIT 165

CID FORM 94
1 FEB 77

FOR OFFICIAL USE ONLY
Law Enforcement Sensitive

End 1

Exhibit(s) 166 thru 168

Page(s) 001030 thru 001039 referred to:

Federal Bureau of Investigation
Record Information/Dissemination Section
170 Marcel Drive
Winchester, Virginia 22602-4843

AGENT'S INVESTIGATION REPORT *CID Regulation 195-1*	ROI NUMBER 0028-10-CID221-10117 0056-10-CID838
	Page 1 of 1

DETAILS

BASIS FOR INVESTIGATION: This office received a Request for Assistance from the Computer Crime Investigative Unit, Arizona Branch Office, RFA 0028-10-CID221-10117, to conduct a witness interview of 1SG (b)(6)(b)(7)(C) A Company, 1st Brigade Special Troops Battalion, United States Army Garrison-Casey, Korea, pertaining to his interactions with PFC Bradley E. MANNING, (b)(6)(b)(7)(C) Headquarters and Headquarters Company, 2d Brigade Combat Team, 10th Mountain Division, Forward Operating Base Hammer, Iraq.

About 1230, 25 Aug 10, SA (b)(6)(b)(7)(C) interviewed 1SG (b)(6)(b)(7)(C) who provided a statement wherein he detailed he was the 1SG of D company, 305th Military Intelligence Battalion, Ft. Huachuca, AZ, of which PFC MANNING was a trainee. 1SG (b)(6)(b)(7)(C) could not recall any specific details of his interactions with PFC MANNING.///LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	USAG-Casey CID Office USAG-Casey, APO AP 96224	
SIGNATURE (b)(6)(b)(7)(C)	DATE 25 Aug 2010	EXHIBIT 169

0028-10-CID221-10117
0056-10-CID838

SWORN STATEMENT

CASE NUMBER: 0056-10-CID838
LOCATION: United States Army Garrison-Casey, Korea TIME: 1315 (b)(6)(b)(7)(C)
NAME: (b)(6)(b)(7)(C)
SSN: (b)(6)(b)(7)(C)
GRADE/STATUS: E-8/AD
DATE: 25 August 201(b)(6)(b)(7)(C)
ORG/ADDRESS: A Company, 1st Brigade Special Troops Battalion, USAG-Casey, Korea

(b)(6)(b)(7)(C)
I, (b)(6)(b)(7)(C) WANT TO MAKE THE FOLLOWING STATEMENT UNDER OATH:

Q: Do you know PFC Bradley MANNING?
A: I recognize the name.
Q: How do you recognize the name?
A: As being the 1SG for D company, 305th Military Intelligence (MI) Battalion. He was one of the Soldiers that went through the 35F Advanced Individual Training (AIT).
Q: When was the last time you had contact with PFC MANNING?
A: It would have to be upon his graduation from AIT.
Q: When did he graduate AIT?
A: I would have no clue when any individual Soldier graduated.
Q: How many Soldiers went through AIT while you were there?
A: Approximately 3,200 Soldiers per year.
Q: When were you the 1SG there?
A: July 07 to August 09.
Q: Are you aware of any security incidents involving PFC MANNING?
A: No. I'm not tracking any security incidents while he was at the school house or otherwise.
Q: Are you aware of any disciplinary incidents involving PFC MANNING?
A: Not at this time.
Q: What do you know about an OPSEC incident in which PFC MANNING posted YouTube videos pertaining to a SCIF?
A: I vaguely remember things being posted on YouTube or Facebook, but I don't remember any OPSEC incidents involving PFC MANNING.
Q: What did the things you remember involve?
A: Just young Soldiers doing stupid stuff and posting it to the internet like wrestling in the barracks and some of the trips they were going on around Ft. Huachuca.
Q: What do you know about an incident in which PFC MANNING stabbed or attempted to stab another Soldier with a pencil?
A: I have no recollection of any physical altercation with that Soldier.
Q: Did PFC MANNING ever discuss the unauthorized release of classified information with you?

EXHIBIT 170
Encl 001041

0028-10-CID221-10117
0056-10-CID838

(b)(6)(b)(7)(C) "Statement of (b)(6)(b)(7)(C) taken on **25 August 2010**, at **USAG-Casey, Korea**, continued:"

A: No.
Q: Did PFC MANNING ever mention WikiLeaks?
A: No.
Q: Did PFC MANNING ever say why he joined the Army?
A: If he did I have no recollection of why he joined the Army.
Q: Did PFC MANNING ever mention any of his friends?
A: No.
Q: Do you know who PFC MANNING was friends with?
A: No.
Q: Was any documentation prepared as a result of conduct, performance or disciplinary issues pertaining to PFC MANNING?
A: I'm sure there was and it would have been kept in his student record at Ft. Huachuca.
Q: Is there a specific incident you have in mind?
A: No. Just whenever a Soldier is counseled it gets put in their student evaluation folder and they get counseled for everything.
Q: Is there anything you would like to add to your statement at this time?
A: No.///END OF STATEMENT///(b)(6)(b)(7)(C)

AFFIDAVIT

I, (b)(6)(b)(7)(C) have read or have had read to me this statement which begins on page 1 and ends on page 2. I fully understand the contents of the entire statement made by me. The statement is true. I have initialed all corrections and have initialed the bottom of each page containing the statement. I have made this statement freely without hope of benefit or reward, without threat of punishment, without coercion, unlawful influence, or unlawful inducement.

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

WITNESSES:

_____

_____

_____

Subscribed and sworn to before me, a person authorized by law to administer oaths, 25 August 2010, at United States Army Garrison – Casey, Korea APO AP 96224

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

(Signature of Person Administering Oath)

ORGANIZATION AND ADDRESS

_____

_____

_____

SA (b)(6)(b)(7)(C), (b) (7)(E)
(Typed Name of Person Administering Oath)

10 USC 936
(Authority to Administer Oath)

INITIALS OF PERSON MAKING STATEMENT: (b)(6)(b)(7)(C)

EXHIBIT 170
001042

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

About 1107, 25 Aug 10, SA (b)(6)(b)(7)(C) SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) both assigned to the National Security Agency (NSA), 9800 Savage Road, Fort Meade, MD 20755, interviewed U.S. Air Force Staff Sergeant (SSgt) (b)(6)(b)(7)(C) 22nd Intelligence Squadron, 9804 Love Road, Fort Meade, MD 20755, as he was identified as having been assigned with PFC MANNING in Iraq. SSgt (b)(6)(b)(7)(C) statemed he was deployed to Iraq from 1 Jan 10 through 1 Jul 10, as part of NSA Cryptological Support Team 5 (CST5). SSgt (b)(6)(b)(7)(C) related he was the replacement for U.S. Marine Corporal (b)(6)(b)(7)(C) and was a Digital Network Intelligence (DNI) Analyst at Forward Operating Base (FOB) Hammer, Iraq. SSg (b)(6)(b)(7)(C) explained he only spent about a month to six weeks at FOB Hammer (January to mid-February 2010) as there had been a decision made to have all DNI personnel moved to a central location within Iraq. SSgt (b)(6)(b)(7)(C) said consequently he spent about four to six weeks at FOB Hammer to learn what his supported Army Brigade Combat Team (BCT) was doing, but was then reassigned to a location on Camp Slayer and/or the Victory Base Complex, for the remainder of his tour in Iraq. SSg (b)(6)(b)(7)(C) stated due to his work at FOB Hammer as a DNI Analyst, he really didn't have any working contact with the 'Organic' soldiers assigned to 2nd BCT, 10th Mountain Division. SSgt (b)(6)(b)(7)(C) said this was largely in part due to the nature of his duties and/or databases which only he was cleared to have access to. SSgt (b)(6)(b)(7)(C) escribed his Iraq tour and time at FOB Hammer as "pretty mundane" and further related he would not have recognized PFC MANNING if shown a picture of him. SSgt (b)(6)(b)(7)(C) further explained he did not remember having any interaction with PFC MANNING during his brief assignment at FOB Hammer. SSgt (b)(6)(b)(7)(C) related he did not remember anyone on his team being overly outgoing or talkative, and that he remembered the shift hand-off briefings between the Sensitive Compartmented Information Facility (SCIF) personnel of 10th Mountain Division running fairly smoothly. SSgt (b)(6)(b)(7)(C) explained, when asked about PFC MANNING's mention of the '9/11 Pager Messages' (which PFC MANNING had mentioned during Internet chat conversations found on his personal computer), that PFC MANNING would have no way of knowing this information and that he was probably making this information up. SSgt (b)(6)(b)(7)(C) said in regard to other topics mentioned by PFC MANNING during PFC MANNING's chat conversations, he had never heard of the chat encryption application 'OTR' nor had he heard of the website WikiLeaks.org until just a couple of weeks ago. SSgt (b)(6)(b)(7)(C) related he was told by CW2 (b)(6)(b)(7)(C) that PFC MANNING had gotten in trouble for disclosing classified information, but SSg (b)(6)(b)(7)(C) said he didn't have any details or the specifics of any incidents. SSgt (b)(6)(b)(7)(C) related he had not spoken with anyone in PFC MANNING's unit about the subject of the Foreign Intelligence Surveillance Act (FISA), and would have told anyone that asked he cannot talk about this subject. SSgt (b)(6)(b)(7)(C) mentioned he had written a report and provided a briefing for other NSA personnel regarding the iPhone, but PFC MANNING should have never have seen that report or received this briefing. SSgt (b)(6)(b)(7)(C) stated the term "reflection" is sometimes used to describe an intelligence indication. SSgt (b)(6)(b)(7)(C) detailed the other NSA personnel he was assigned with at FOB Hammer during his assignment in Iraq as: CW2 (b)(6)(b)(7)(C) SPC (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) who was an National Geospatial Agency (NGA) employee and dealt with imagery; a Navy E-6 who SSgt (b)(6)(b)(7)(C) believed was named (b)(6)(b)(7)(C) and Senior Airman (SrA) (b)(6)(b)(7)(C) who SSgt (b)(6)(b)(7)(C) said was sent home from Iraq early due to some type of issue. SSgt (b)(6)(b)(7)(C) said he believes that SrA (b)(6)(b)(7)(C) was currently assigned to NSA, as SSgt (b)(6)(b)(7)(C) said he saw SrA

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060
SIGNATU (b)(6)(b)(7)(C)	DATE: 25 Aug 10 / EXHIBIT: 171

FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

(b)(6)(b)(7)(C) recently on Fort Meade, MD. SSgt (b)(6)(b)(7)(C) could not immediately provide any additional information related to this investigation or PFC MANNING.

AGENTS COMMENT: The U.S. Navy personnel SSgt (b)(6)(b)(7)(C) initially identified as having been assigned with him on FOB Hammer, was later identified as Petty Officer First Class (PO1) (b)(6)(b)(7)(C) Additionally, the circumstances of SSgt (b)(6)(b)(7)(C) having been reassigned after a short period of time at FOB Hammer were also corroborated by other interviews of personnel serving as part of CST5.

// **LAST ENTRY** //

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE (b)(6)(b)(7)(C)	DATE 25 Aug 10	EXHIBIT 171

FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE

001044
Approved_____

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER 0110-10-CID112 (RFA)
0028-10-CID221-10117

PAGE 1 OF 1 PAGE

DETAILS

BASIS FOR INVESTIGATION: About 0900, 25 Aug 10, this office received a Category One (CAT 1) Request For Assistance (RFA) from the Arizona Branch Office, Computer Crime Investigative Unit (CCIU), Washington Metro Resident Agency, 9805 Lowen Road, Building 193, Fort Belvoir, VA 22060, requesting this office interview CPT (b)(6)(b)(7)(C) Headquarters and Headquarters Company (HHC), 22nd Chemical Battalion (BN), Aberdeen Proving Ground-South, MD 21010 (APG-S), in regards to the "Wikileaks" investigation.

About 1144, 25 Aug 10, SA (b)(6)(b)(7)(C) interviewed CPT (b)(6)(b)(7)(C), who provided a Sworn Statement regarding her assignment as the Commander of the Advanced Individual Training (AIT) unit PFC MANNING was assigned to. (See Sworn Statement for details)

STATUS: This investigation is terminated in the files of this office. No further investigative activity is anticipated or requested.///LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Aberdeen Proving Ground CID Office Aberdeen Proving Ground, MD 21005	
SIGNATURE (b)(6)(b)(7)(C)	DATE 25 Aug 10	EXHIBIT 172

CID FORM
1 FEB 77

SWORN STATEMENT

For use of this form, see AR 190-45; the proponent agency is PMG.

PRIVACY ACT STATEMENT

AUTHORITY:	Title 10 USC Section 301; Title 5 USC Section 2951; E.O. 9397 dated November 22, 1943 (SSN).
PRINCIPAL PURPOSE:	To provide commanders and law enforcement officials with means by which information may be accurately identified.
ROUTINE USES:	Your social security number is used as an additional/alternate means of identification to facilitate filing and retrieval.
DISCLOSURE:	Disclosure of your social security number is voluntary.

1. LOCATION	2. DATE (YYYYMMD)	3. TIME	4. FILE NUMBER
Building 1942E Aberdeen Proving Gound-South	2010/08/25	1144	0028-10-CID221-10117

5. LAST NAME, FIRST NAME, MIDDLE NAME	6. SSN	7. GRADE/STATUS
(b)(6)(b)(7)(C)	(b)(6)(b)(7)(C)	O-3/CPT

8. ORGANIZATION OR ADDRESS

HHC, 22nd Chemical Battalion, Aberdeen Proving Gound-South, MD 21010

9.

I, CPT (b)(6)(b)(7)(C), WANT TO MAKE THE FOLLOWING STATEMENT UNDER OATH:

Q: SA (b)(6)(b)(7)(C)
A: CPT (b)(6)(b)(7)(C)
Q: How do you know PFC MANNING?
A: I was his AIT company commander in Delta Company, 305th MI BN.
Q: When was the last time you had any contact with PFC MANNING?
A: When he graduated from AIT, do not know the approximate date.
Q: Are you aware of any security incidents involving PFC MANNING?
A: After reading about him in the news, my old platoon sergeant contacted me via email to remind me that he was the Soldier that received UCMJ while he was at AIT. I previously administered UCMJ (can't remember if I admistered a summarized article 15 or company grade) for him posting a video on YouTube on the topic of his training while at Fort Huachuca. The video was not specific to operational security but talked about how he missed his family, barracks life, marching to class, how hard PT was, and the different names of the buildings where he was attending class.
Q: Are you aware of disciplinary incidents involving PFC MANNING?
A: See above, I can't remember his punishment but it went through JAG at Huachuca for approval.
Q: What do you know about an OPSEC incident in which PFC MANNING posted YouTube videos pertaining to a SCIF?
A: He received UCMJ, his video was removed the day after it was posted so I only heard about it from the platoon sergeant and never actually viewed it for myself. I was only tracking that the video contained the names of the buildings and how much he missed his family, that he was homessick etc.
Q: What do you know about an incident in which PFC MANNING stabbed/attempted to stab/assaulted another Soldier with a pencil?
A: Nothing, never heard of it.
Q: Did PFC MANNING ever discuss the unauthorized release of classified information with you? If so explain.
A: No
Q: Did PFC MANNING ever mention WikiLeaks? If so, in what context?
A: No
Q: Did PFC MANNING ever say why he joined the Army? If so, why?
A: No
Q: Did PFC MANNING ever mention any of his friends? If so, why?
A: No
Q: Was any documentation prepared as a result of conduct/perforce/disciplinary issues? If so, by who, and where is that documentation located?
A: His platoon sergeant was SFC (b)(6)(b)(7)(C) who was the same NCO that contacted me via email to remind me of the Soldier when he hit the news. I did not keep a copy of his UCMJ but the company records maintains three years worth of records in the back of the orderly room (under the Soldier's name), across from the supply office. To my knowledge SFC (b)(6)(b)(7)(C) is still at Fort Huachuca. He moved to Charlie Company right before I changed out of command but when he emailed me a few months ago he was still at Huachuca.
Q: Do you have anything you wish to add to this statement?
A: No///End of Statement// (b)(6)(b)(7)(C)

10. EXHIBIT	11. INITIALS OF PERSON MAKING STATEMENT (b)(6)(b)(7)(C)	PAGE 1 OF 3 PAGES

ADDITIONAL PAGES MUST CONTAIN THE HEADING "STATEMENT OF _____ TAKEN AT ____ DATED ____

THE BOTTOM OF EACH ADDITIONAL PAGE MUST BEAR THE INITIALS OF THE PERSON MAKING THE STATEMENT, AND PAGE NUMBER MUST BE BE INDICATED.

USE THIS PAGE IF NI . IF THIS PAGE IS NOT NEEDED, PLEASE PROCEED TO FINAL PAGE OF THIS FORM.

0028-10-CID221-10117

STATEMENT OF CPT (b)(6)(b)(7)(C) TAKEN AT Building 1942E, APG DATED 2010/08/25

9. STATEMENT *(Continued)*

Not used (b)(6)(b)(7)(C)

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

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

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

INITIALS OF PERSON MAKING STATEMENT (b)(6)(b)(7)(C)

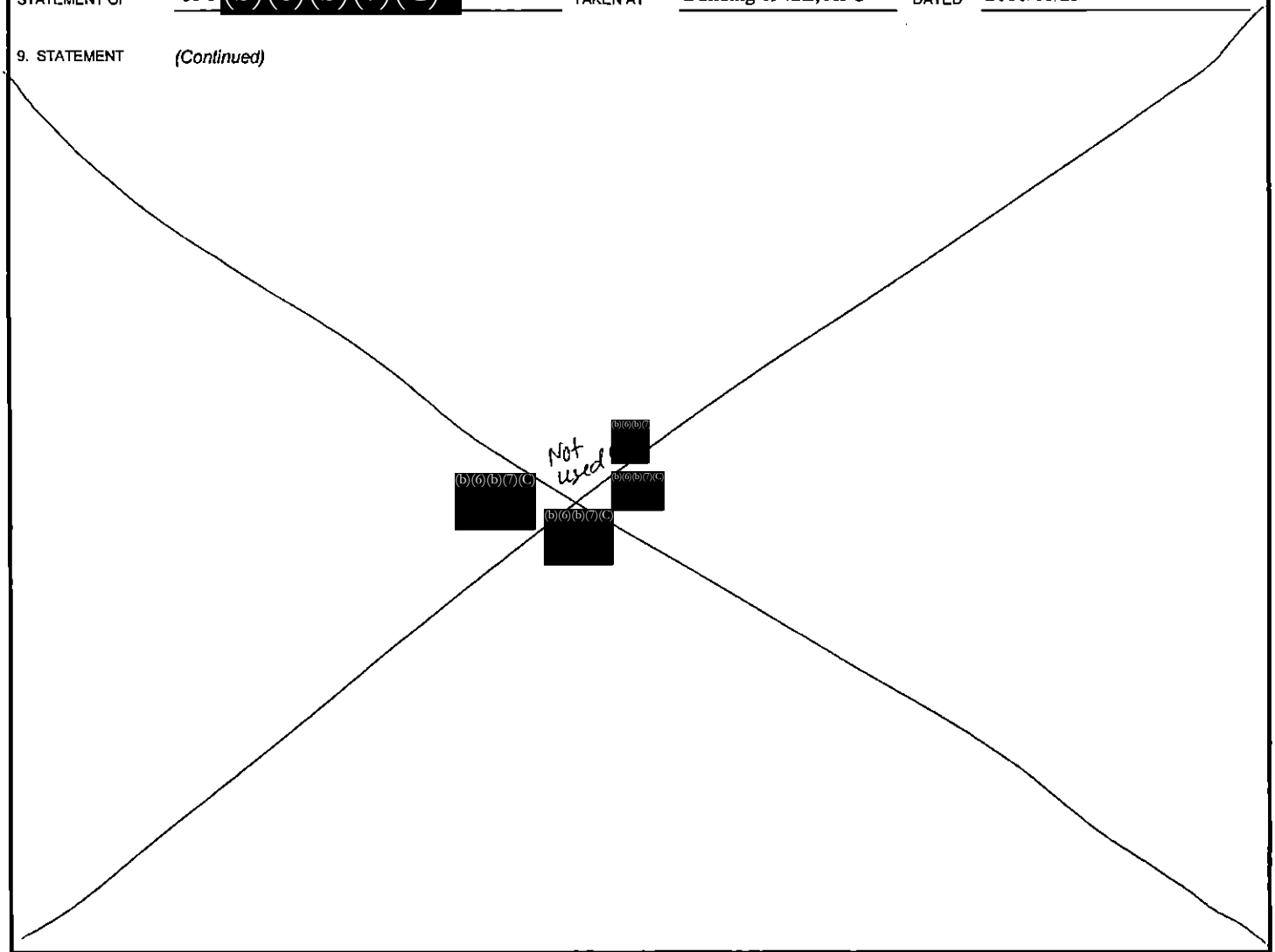
PAGE 2 OF 3 PAGES

EXHIBIT 173

0010471

STATEMENT OF CPT (b)(6)(b)(7)(C) TAKEN AT Building 1942E, APG DATED 2010/08/25

9. STATEMENT *(Continued)*



AFFIDAVIT

I, CPT (b)(6)(b)(7)(C), HAVE READ OR HAVE HAD READ TO ME THIS STATEMENT WHICH BEGINS ON PAGE 1, AND ENDS ON PAGE 3. I FULLY UNDERSTAND THE CONTENTS OF THE ENTIRE STATEMENT MADE BY ME. THE STATEMENT IS TRUE. I HAVE INITIALED ALL CORRECTIONS AND HAVE INITIALED THE BOTTOM OF EACH PAGE CONTAINING THE STATEMENT. I HAVE MADE THIS STATEMENT FREELY WITHOUT HOPE OF BENEFIT OR REWARD, WITHOUT THREAT OF PUNISHMENT, AND WITHOUT COERCION, UNLAWFUL INFLUENCE, OR UNLAWFUL INDUCEMENT.

(b)(6)(b)(7)(C)
(Signature of Person Making Statement)

WITNESSES:

ORGANIZATION OR ADDRESS

ORGANIZATION OR ADDRESS

Subscribed and sworn to before me, a person authorized by law to administer oaths, this 25 day of August, 2010 at Building 1942E, APG-S, MD 21010

(b)(6)(b)(7)(C)
(Signature of Person Administering Oath)

SA (b)(6)(b)(7)(C)
(Typed Name of Person Administering Oath)

10 USC 936
(Authority To Administer Oaths)

INITIALS OF PERSON MAKING STATEMENT (b)(6)(b)(7)(C)

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER: 0603-10-CID034

PAGE 1 OF 1 PAGE(S)

DETAILS

BASIS FOR INVESTIGATION: This office received a Request for Assistance (RFA) from the United States Army Criminal Investigation Command, Computer Crime Investigative Unit, Washington Metro Resident Agency, 9805 Lowen Road, Building 193, Fort Belvoir, VA 22060, to locate, fully identify and interview SFC (b)(6)(b)(7)(C) 66th Military Intelligence (MI) Company, SSG (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) TF ODIN and 1LT (b)(6)(b)(7)(C) G Company, 15th Combat Support Battalion, Fort Hood, TX 76544 (FHTX).

About 1025, 25 Aug 10, SA (b)(6)(b)(7)(C) interviewed 1LT (b)(6)(b)(7)(C) who provided a statement wherein he stated who were the Drill Sergeants of PFC MANNING at the time.

About 1045, 25 Aug 10, SA (b)(6)(b)(7)(C) coordinated with CSM (b)(6)(b)(7)(C) 21st CAV BDE (Air Combat), FHTX, who stated SFC (b)(6)(b)(7)(C) was currently deployed to Camp Spiecher, Tikrit, Iraq.

About 1200, 25 Aug 10, SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) coordinated with SFC (b)(6)(b)(7)(C) (Rear Detachment 1SG), 66TH MI Company, FHTX, who stated SFC (b)(6)(b)(7)(C) is currently deployed to Kuwait, Main Body 2-A team, departed from FHTX on 23 Aug 10.

About 1244, 25 Aug 10, SA (b)(6)(b)(7)(C) coordinated with SA (b)(6)(b)(7)(C) Computer Crime Investigative Unit, who stated there is no further investigation needed.

STATUS: Further activity by this office is not anticipated at this time. This matter is closed within the files of this office. Additional activity, if deemed necessary, will be conducted under a separate sequence number.
///LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Fort Hood CID Office Fort Hood, TX 76544	
SIGNATURE (b)(6)(b)(7)(C)	DATE 25 Aug 10	EXHIBIT 174

CID FORM 94 FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
1 FEB 77

8883-10-CID034-

SWORN STATEMENT

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

LOCATION: Fort Hood CID Office, Fort Hood, TX 76544 **DATE:** 2010-08-25 **TIME:** 1025
NAME: (b)(6)(b)(7)(C)
SSN: (b)(6)(b)(7)(C)
STATUS: 2LT/AD
ORGANIZATION/ADDRESS: G Company, 3-82nd FA, 15th Combat Support Battalion, FHTX

I, (b)(6)(b)(7)(C) **want to make the following statement under oath:**
I would like to complete my statement in a question and answer format as explained by SA (b)(6)(b)(7)(C)
Q: SA (b)(6)(b)(7)(C)
A (b)(6)(b)(7)(C)
Q: How do you know PFC MANNING?
A: I was a Drill Sergeant, of D. Company, 305th Military Intelligence (MI), Battalion. (b)(6)(b)(7)(C)
Q: What year were you the Drill Sergeant?
A: 2007 through 2008. (b)(6)(b)(7)(C)
Q: When was the last time you had contact with PFC MANNING?
A: It would have been during the time frame October and December 2007. (b)(6)(b)(7)(C)
Q: Are you aware of any security incidents involving PFC MANNING?
A: No. (b)(6)(b)(7)(C)
Q: Are you aware of any disciplinary incidents involving PFC MANNING?
A: I remember hearing about he attempted to stab another soldier with a pencil, in the dining facility. (b)(6)(b)(7)(C) Wouldn't know personally, because he wasn't my soldier.
Q: What do you know about an OPSEC incident in which PFC MANNING posted You Tube videos pertaining to a SCIF?
A: I don't know anything about that. But the SCIF is a high security area located at the school house. (b)(6)(b)(7)(C)
Q: Did PFC MANNING ever discuss the unauthorized release of classified information with you? If so, please explain.
A: No. (b)(6)(b)(7)(C)
Q: Did PFC MANNING ever mention WikiLeaks? If so, in what context?
A: No. (b)(6)(b)(7)(C)
Q: Did PFC MANNING ever say why he joined the Army? If so, why?
A: No, not to me. (b)(6)(b)(7)(C)
Q: Did PFC MANNING ever mention any of his friends? If so, who?
A: No. (b)(6)(b)(7)(C)
Q: Were you part of PFC MANNING's chain of command?
A: No. (b)(6)(b)(7)(C)
Q: Do you know who was PFC MANNING's, Drill Sergeant at the time?
A: It might have been SSG (b)(6)(b)(7)(C) nd SSG (b)(6)(b)(7)(C) not sure. I was basically just assisting these guys, because I had already done my two years. So I really didn't deal with the soldiers too much, I was preparing for OCS. I just did physical training with them and marched them to class. (b)(6)(b)(7)(C)
Q: Are there any details you think might help this investigation? (b)(6)(b)(7)(C)

INITIALS OF PERSON MAKING STATEMENT: (b)(6)(b)(7)(C)

EXHIBIT

EXHIBIT 175
001050

"Statement of 1LT (b)(6)(b)(7)(C) TAKEN AT Fort Hood CID Office, DATED: **2010-08-25**
Continued:"

A: No.

Q: Is there anything else you would like to add to this statement?

A: No._____///End of Statement///

"Statement of 2LT (b)(6)(b)(7)(C) TAKEN AT Fort Hood CID Office, DATED: **2010-08-25**
Continued:"

AFFIDAVIT

I, 2LT (b)(6)(b)(7)(C) HAVE READ OR HAVE HAD READ TO ME THIS STATEMENT WHICH BEGINS ON PAGE 1 AND ENDS ON PAGE 3 . I FULLY UNDERSTOOD THE CONTENTS OF THE ENTIRE STATEMENT MADE BY ME. THE STATEMENT IS TRUE. I HAVE INITIALED ALL CORRECTIONS AND HAVE INITIALED THE BOTTOM OF EACH PAGE CONTAINING THE STATEMENT. I HAVE MADE THIS STATEMENT FREELY WITHOUT HOPE OF BENEFIT OR REWARD, WITHOUT THREAT OF PUNISHMENT, AND WITHOUT COERCION, UNLAWFUL INFLUENCE, OR UNLAWFUL INDUCEMENT.

(b)(6)(b)(7)(C)
(Signature of Person Making Statement)

WITNESSES:

Subscribed and sworn to before me, a person authorized by law to administer oaths, this day 25th of August, 2010 at Fort Ho[illegible] CID Off[illegible]

(b)(6)(b)(7)(C)
(Signature of Person Administering Oath)

ORGANIZATION AND ADDRESS

Special Agent (b)(6)(b)(7)(C), (b) (7)(E)
(Typed Name of Person Administering Oath)

Title 10 USC, Section 936
(Authority to Administer Oath)

INITIALS OF PERSON MAKING STATEMENT: (b)(6)(b)(7)(C)

EXHIBIT 175

AGENT'S INVESTIGATION REPORT

ROI NUMBER **0028-10-CID221-10117**
0327-10-CID056-

CID Regulation 195-I

PAGE 1 OF 1 PAGES

DETAILS

Basis for Investigation: This office received a Category I Request for Assistance from the Computer Crime Investigative Unit (CCIU), Washington Metro Resident Agency, 9805 Lowen Road, Building 193, Fort Belvoir VA 22060, to interview SFC (b)(6)(b)(7)(C) A Company (Co), 2nd Special Troops Battalion, 2nd Brigade Combat Team, 4th Infantry Division, Fort Carson, CO 80913 (FCCO), and SFC (b)(6)(b)(7)(C) B Co, Division Special Troops Battalion, 4th Infantry Division, FCCO, pertaining to their knowledge of PFC MANNING.

About 1417, 25 Aug 10, SA (b)(6)(b)(7)(C) interviewed SFC (b)(6)(b)(7)(C) who provided a Sworn Statement wherein he stated he was assigned to Fort Huachuca from Jun 05 until May 08; however he did not remember PFC MANNING. (See Sworn Statement for details)

About 1424, 25 Aug 10, SA (b)(6)(b)(7)(C) this office, interviewed SFC (b)(6)(b)(7)(C) who provided a Sworn Statement wherein she stated she did not know PFC MANNING personally while assigned to Fort Huachuca. (See Sworn Statement for details)

About 1435, 25 Aug 10, SA (b)(6)(b)(7)(C) coordinated with SA (b)(6)(b)(7)(C) Special Agent in Charge, Arizona Branch Office, CCIU, who stated no further assistance was needed from this office.

All requested leads have been completed; this investigation was closed in the files of this office.///LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	48th Military Police Detachment (CID) Fort Carson, CO 80913	
SIGNATURE (b)(6)(b)(7)(C)	DATE 25 Aug 10	EXHIBIT 176

CID Form 94
1 FEB 77