DEPARTMENT OF THE AIR FORCE
AIR FORCE OFFICE OF SPECIAL INVESTIGATIONS

HQ AFOSI/XILI
Attn: FOIA Section
27130 Telegraph Rd
Quantico VA 22134

JAN 06 2015

Karl Grindal
4601 N Fairfax Drive, Suite 1200
Arlington, VA 22203

Dear Mr. Grindal

This is in response to your Freedom of Information Act (FOIA) request, dated 11 January 2012, that was originally submitted to the Federal Bureau of Investigation (FBI), reference 1181137-000. During the processing of your request, AFOSI documents were identified and forwarded to our office for processing and direct response to you. We received your request on 26 August 2013 and assigned tracking number 2014-02850-F.

Information from AFOSI criminal investigative records are exempt from release under the Privacy Act, Title 5 United States Code (USC) Section 552(a)(J)(2). In order to provide you the maximum amount of releasable information, we are processing your request under the FOIA. Since portions of the information requested are also exempt from disclosure under the FOIA, we have inserted the exemptions below in the attached document(*s*).

a. Exemption b6 permits the withholding of all information about individuals in "personnel and medical files and similar files" when the disclosure of such information "would constitute a clearly unwarranted invasion of personal privacy."

b. Exemption b7c provides protection for personal information in law enforcement records the disclosure of which "could reasonably be expected to constitute an unwarranted invasion of personal privacy."

c. Exemption b7e provides protection to all law enforcement information which "would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law."

The authority for the exemptions used can be found in 5 USC § 552 and in Air Force Manual 33-302, which can be accessed via the Air Force FOIA page at http://www.foia.af.mil/.

If you interpret my response as not fully complying with your request, you may appeal this decision with the Secretary of the Air Force by email to afosi_hq_foia_request@us.af.mil, by mail to AFOSI/XILI, ATTN: FOIA Office, 27130 Telegraph Rd, Quantico, VA 22134, or by fax to (571) 305-8229 no later than 60 calendar days from the date of this letter. Include your reason(s) for reconsideration and attach a copy of this letter.

If you decide to appeal the FBI's redactions, you must write to them at the following address: Director, Office of Information Policy (OIP), U.S. Department of Justice, 1425 New York Ave., NW Suite 11050, Washington, D.C. 20530-0001, or you may submit an appeal through OIP's eFOIA portal http://www.justice.gov/oip/efoia-portal.html. The letter and the envelope should be clearly marked "Freedom of Information Appeal" and the Freedom of Information Privacy Acts' request number should be cited in the letter. Please be advised that your envelope must be postmarked within 60 days of the date of our letter. Please cite the FOIPA Request Number in any correspondence to them for proper identification of the request.

Sincerely

STEPHANIE J. COURTNEY
Chief, Information Release Branch

Attachment:
Cy of Pages from Section 5 Serial 238 of FBI file 288-HQ-1242560

139

Statement of (b) (6), (b) (7)(C)
Social Security Number: (b) (6), (b) (7)(C)
Father's Name: (b) (6), (b) (7)(C)
Date of Birth: (b) (6), (b) (7)(C)
Place of Birth: (b) (6), (b) (7)(C)
Marital Status: (b) (6), (b) (7)(C)
Address: (b) (6), (b) (7)(C)
Work Address: (b) (6), (b) (7)(C)
Home Phone Number: (b) (6), (b) (7)(C)
Work Phone Number:

Date/Time: 29 March 1998, XXXX

I am a Special Agent with the United States Air Force Office of Special Investigations (AFOSI). I work at our Headquarters in Washington DC in the Computer Crime Investigations Division. My duties include investigation of intrusions into US Air Force (USAF) computer systems. During the course of my regular duties I became involved in the investigation of (b) (6), (b) (7)(C) aka (b) (6), (b) (7)(C) aka (b) (6), (b) (7)(C) an Israeli citizen living in Hod Hasharon, Israel. The investigation involved AFOSI, the Federal Bureau of Investigation (FBI), the National Aeronautic and Space Administration Office of the Inspector General (NASA/OIG), and the US Navy Criminal Investigative Service (NCIS). I was selected to be part of an investigative team to travel to Israel to verify the true identity of (b) (6), (b) (7)(C) and collect evidence concerning intrusions into USAF, NASA, and other US Government, educational, and commercial computer systems. I traveled with Special Agent (b) (6), (b) (7)(C) (NASA/OIG), Special Agent (b) (6), (b) (7)(C) (FBI), and Special Agent (b) (6), (b) (7)(C) (FBI). We met with investigators from the Israel Police National Unit for Fraud Investigations in Bat-yam, Israel. Investigator (b) (6), (b) (7)(C) was assigned this investigation, and has worked with us to gather facts and evidence concerning the allegations against (b) (6), (b) (7)(C) During the course of our cooperative effort with the Israel Police, we produced a package of information concerning our case against (b) (6), (b) (7)(C) and the evidence that US Government agencies have collected to date. Special Agent (b) (6), (b) (7)(C) Special Agent (b) (6), (b) (7)(C) and I gave statements explaining the details of this package to the National Unit for Fraud Investigations on 17 March 1998. In addition to these statements and initial package of case information, AFOSI and NASA/OIG are providing Investigator (b) (6), (b) (7)(C) with data obtained from various evidentiary sources. Investigator (b) (6), (b) (7)(C) requested I prepare this statement to elaborate on various case details and provide an explanation of the investigative data being provided by AFOSI and NASA/OIG.

Case Information

Background concerning the initial break-ins into USAF computer systems was provided in the initial package of information produced by myself and the other US investigators, and was explained to Investigator (b) (6), (b) (7)(C) in detail on 26 March 1998. To summarize, six different computer systems were broken in to on 3 and 4 February 1998, which we believe are tied to (b) (6), (b) (7)(C) The table below details what system was broken into, its Internet Protocol (IP) address, where it was located, where the attack came from, and the date and time of the attack, in **Eastern Standard Time.**

Victim System	IP Address	Location	Attacking Site	Attacking IP	Date/Time
(b) (6), (b) (7)(C)		Andrews AFB MD	(b) (6), (b) (7)(C)		
		Channel Island CA			
		Lackland AFB TX			
		Kirtland AFB NM			
		Columbus AFB MS			
		Gunter Annex AL			

The definitions for abbreviations used in the table are listed below:

AFB - Air Force Base
MD - Maryland, USA
CA - California, USA
TX - Texas, USA
NM - New Mexico, USA
MS - Mississippi, USA
AL - Alabama, USA

The entry in the table for (b) (6), (b) (7)(C) lists the date/time of the intrusion as UNKNOWN. This information is available, and will be provided to Investigator (b) (6), (b) (7)(C) I do not have a detailed copy of information from that site with me, and it must be retrieved and sent after my return to the US. The table also lists the initial attacking site against (b) (6), (b) (7)(C) (the system at Andrews AFB) as (b) (6), (b) (7)(C) a computer system at Utah State University in the US. Further review of security logs showed (b) (6), (b) (7)(C) was accessed from (b) (6), (b) (7)(C) on 5 February 1998, indicating the break in of that system is related to the break ins of the other USAF systems. Attachment 1 to this statement is a diagram prepared by me detailing some of this activity. This diagram is only a working copy, and may contain errors. It should be used only as an investigative aid, NOT AS EVIDENCE.

In response to these intrusions, AFOSI, FBI and NCIS began investigating the incidents. As part of that investigation, AFOSI installed network monitoring devices at various locations to obtain further information and evidence, and attempt to identify a suspect. A network monitor is very similar to a phone tap - it is a device that allows you to "listen" on a network to computer transmissions and record them without interrupting them. The following list shows locations where AFOSI installed network monitors, the computer systems that were being monitored, and the dates the monitors were activated:

1. Andrews AFB MD, (b) (6), (b) (7)(C) 6 February 1998
2. Maroon.com, College Station TX, (b) (6), (b) (7)(C) 11 February 1998
3. Channel Island CA, (b) (6), (b) (7)(C) 12 February 1998
4. Netdex Incorporated, (b) (6), (b) (7)(C) 20 February 1998

An analysis of the network monitor data was accomplished by AFOSI, which I assisted in. I am providing this data to Investigator (b) (6), (b) (7)(C) The formats are explained in the **Data Formats and Examples** section of this statement. In addition, two examples of intrusions from Netvision into computers in the United States through (b) (6), (b) (7)(C) are provided.

Investigator (b) (6), (b) (7)(C) inquired as to the involvement of Netvision in the investigation, and how they played a role during the events of our case. The following information was provided to me by Special Agent (b) (6), (b) (7)(C) Department of Defense computer security personnel reviewed log information which showed that the intruder to USAF computer systems had downloaded patch files to those systems from sunsite.unc.edu, an Internet site containing extensive software archives. A patch file is a usually a file that fixes some "bug" or problem with a computer. Sunsite.unc.edu is a site on the Internet that contains a large software archive. In this archive are numerous patches to various operating systems. The intruder was regularly accessing this site to download a specific patch file named (b) (6), (b) (7)(C) Computer security personnel thought that if Sunsite had records of where this file was downloaded to, it would help identify what other computers the intruder may have broken in to. After obtaining records from Sunsite, computer security personnel discovered two Netvision computer systems had downloaded the patch file on 3 February 1998: (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) The security personnel contacted Netvision system administration personnel to notify them that the patch file had been downloaded to their computers. (b) (6), (b) (7)(C) a system administrator for Netvision, said an unknown intruder had compromised the two Netvision systems. (b) (6), (b) (7)(C) looked into the incident, and related he felt the attacks may have originated from a local school in Israel. Israeli media sources identify the school as the School for Environmental Education at Sdeh Boker (Israel News Today, 10 March 1998). According to (b) (6), (b) (7)(C) the Sdeh Boker system administrator related his systems had been compromised from another Israeli ISP called (b) (6), (b) (7)(C) The Sdeh Boker system administrator identified the user account utilized for the attacks against Netvision, and interviewed the student who owned it. The student related he gave his account to someone with the nickname (b) (6), (b) (7)(C) on an Internet Relay Chat (IRC) channel on the Undernet IRC network. (b) (6), (b) (7)(C) said the principal at Sdeh Boker spoke with the student, who gave him (b) (6), (b) (7)(C) cell phone number.

Investigator (b) (6), (b) (7)(C) wanted further details about how we identified two suspects in the US, and an explanation of information we obtained from them on (b) (6), (b) (7)(C) AFOSI reviewed security logs and discovered that during a connection to the Andrews AFB system (b) (6), (b) (7)(C) at 1930 EST on 4 February 1998, the intruder copied a sniffer log file from (b) (6), (b) (7)(C) to sonic.net, an Internet Service Provider (ISP) in California. A sniffer is a program often used by hackers to illegally capture network data from systems they have broken in to. This data usually contains usernames and passwords to other computer systems, allowing the hacker to then break in to more computers. The log file was transferred via file transfer protocol (FTP) to IP address (b) (6), (b) (7)(C) AFOSI agents contacted sonic.net and spoke with the owner of the company. He stated that the IP address was dynamic - an address assigned to users as they dial into sonic.net via modems. He also stated that only one dial-up was active at the time of the

sniffer log file transfer, and he knew who was logged on at that time. We felt this would help us identify who might be responsible for some of the attacks.

The following information was provided to me by Special Agent (b) (6), (b) (7)(C) The FBI obtained records from sonic.net that identified two individuals that might be responsible for some of the hacking activity that the USAF detected. The two suspects were known as (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) on IRC. Sonic.net monitored their network and recorded conversations via IRC between (b) (6), (b) (7)(C) and another individual using a computer named (b) (6), (b) (7)(C) on 19 February 1998 from approximately 1644 PST to 2243 PST. Attachment 2 is a print out of this conversation. This conversation was later compared to logs found on (b) (6), (b) (7)(C) computer system. This particular conversation was found in a file called (b) (6), (b) (7)(C) LOG, and is reviewed in detail later in this statement.

The FBI and AFOSI searched (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) houses on 25 February 1998 and interviewed both of them. The information provided by (b) (6), (b) (7)(C) did not pertain to (b) (6), (b) (7)(C) Information from (b) (6), (b) (7)(C) however, indicated (b) (6), (b) (7)(C) was involved in hacking activity. Special Agent (b) (6), (b) (7)(C) interviewed (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) told him (b) (6), (b) (7)(C) had been teaching him how to break in to computer systems. He also said he and were members of a hacking group known as the "Enforcers", who often used the #enforcers channel on the Undernet IRC network. (b) (6), (b) (7)(C) told (b) (6), (b) (7)(C) he was (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) said (b) (6), (b) (7)(C) had broken into college, military, and government systems, as well as the Knesset World Wide Web (WWW) page. (b) (6), (b) (7)(C) stated (b) (6), (b) (7)(C) claimed to possess 600 megabytes (MB) of compressed sniffer output files, has access to over 1000 different computer systems, and allegedly has installed sniffer programs on US military systems. (b) (6), (b) (7)(C) also stated 500 MB of the sniffer output files were maintained by a friend of (b) (6), (b) (7)(C) According to (b) (6), (b) (7)(C) used to work at (b) (6), (b) (7) but was fired for hacking.

I reviewed information from (b) (6), (b) (7)(C) computer system, and discovered IRC logs produced by the program "mIRC". The logs showed numerous conversations between (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) (another name often used by (b) (6), (b) (7)(C) Review of the logs disclosed (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) trading user names and passwords to US Government systems, and (b) (6), (b) (7)(C) instructing (b) (6), (b) (7)(C) on how to compromise Domain Name Service (DNS) sites. (b) (6), (b) (7)(C) also stated that he commonly used the login name (b) (6), (b) (7)(C) and the password (b) (6), (b) (7)(C) to access systems he's compromised. During one of the conversations, (b) (6), (b) (7)(C) indicated his close associate and "hacking partner" was an individual identified as (b) (6), (b) (7)(C) Special Agent (b) (6), (b) (7)(C) told me that the clock on (b) (6), (b) (7)(C) computer system was set wrong. By reviewing our case information, we discovered that (b) (6), (b) (7)(C) computer was set to PST, and was 2 years, 10 days, 22 minutes slow. Investigator (b) (6), (b) (7)(C) requested I print out and review two IRC log files on (b) (6), (b) (7)(C) system which showed (b) (6), (b) (7)(C) admitting to various illegal activities. These files were named (b) (6), (b) (7)(C) LOG and (b) (6), (b) (7)(C) LOG, and are Direct Client Connection logs They are attached to this statement at Attachment 3 (b) (6), (b) (7)(C) LOG) and Attachment 4 (b) (6), (b) (7)(C) LOG).

(b) (6), (b) (7)(C) **LOG:** On pages 6 and 7 of Attachment 3, (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) are discussing hacking. The date and time of this conversation (corrected for the error in the clock of (b) (6), (b) (7)(C) computer) is 12 February 1998, at approximately 2151 PST. The log also shows (b) (6), (b) (7)(C) is using IP address (b) (6), (b) (7)(C) states "i am over (b) (6), (b) house". Review of the WWW page for the Enforcers hacking group showed an Enforcer member named (b) (6), (b) (7)(C) Review of (b) (6), (b) (7)(C) web page showed he was (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) 3 also shows (b) (6), (b) (7)(C) talking about user names and passwords at Lawrence Livermore National Laboratory (LLNL) systems. On Page 7 of Attachment 3, he states (b) (6), (b) (7)(C) in conjunction with a listing of computer systems at LLNL. The systems he lists are (b) (6), (b) (7)(C) On page 8 of Attachment 3, (b) (6), (b) (7)(C) tells (b) (6), (b) (7)(C) that he has seen a message displayed on a computer system he broke in to. He displays the message in the conversation. The message displayed is a message installed by AFOSI at (b) (6), (b) (7)(C) Note, the message shows a line that states (b) (6), (b) (7)(C) is another name for (b) (6), (b) (7)(C) - both names refer to the same computer system. The message was installed at (b) (6), (b) (7)(C) to satisfy United States legal requirements so AFOSI could monitor the network at (b) (6), (b) (7)(C)

(b) (6), (b) (7)(C) **LOG:** On page 1 of Attachment 4, (b) (6), (b) (7)(C) tells (b) (6), (b) (7)(C) where the command is that will give him root access on (b) (6), (b) (7)(C) This conversation takes place (corrected for (b) (6), (b) (7)(C) system clock error) on 1 February 1998, at approximately 1319 PST, and (b) (6), (b) (7)(C) is using IP (b) (6), (b) (7)(C) On page 2, (b) (6), (b) (7)(C) tells (b) (6), (b) (7)(C) that "I HACKED THE ISRAELI PENTAGON...like u guys have whitehouse.gov right? our whitehouse.gov

= knesset.gov.il". This conversation takes place on 2 February 1998 at approximately 1724 PST, but the IP used by (b) (6), (b) (7)(C) for this session is not recorded in the log file. On page 7 of Attachment 4, (b) (6), (b) (7)(C) tells (b) (6), (b) (7)(C) a user name and password to (b) (6), (b) (7)(C) According to Special Agent (b) (6), (b) (7)(C) this computer system belongs to a book publishing company in Maryland, USA, and has files stored on it containing numerous credit card numbers. (b) (6), (b) (7)(C) then proceeds to teach (b) (6), (b) (7)(C) about modifying Domain Name Servers. This conversation takes place on 19 February 1998, at approximately 1901 PST. (b) (6), (b) (7)(C) is using IP address (b) (6), (b) (7)(C) during this session.

On 3 March 1998, the monitor installed by AFOSI at (b) (6), (b) (7)(C) detected a connection from Netvision. The intruder then connected to (b) (6), (b) (7)(C) and modified their web page. This activity is covered in more detail in the **Data Formats and Examples** section of this statement. The web page states (b) (6), (b) (7)(C) is responsible for hacking into Department of Defense computer systems, and (b) (6), (b) (7)(C) is innocent. The page also displays (b) (6), (b) (7)(C) as an e-mail address to reach (b) (6), (b) (7)(C) Special Agent (b) (6), (b) (7)(C) contacted Hotmail and obtained logs from their computer systems. These logs are at Attachment 5, and show numerous connections from Netvision to hotmail.com to access the "hsecurity" account. The times listed on Attachment 5 are PST.

On 9 March 1998, a review of media sources disclosed (b) (6), (b) (7)(C) an Israeli reporter with Walla! News interviewed (b) (6), (b) (7)(C) During the course of the interview, the interviewee confessed to hacking US Government computer systems, as well as systems belonging to the Israeli government. The Israeli reporter obtained account names, passwords, and system addresses from (b) (6), (b) (7)(C) to verify his identity. The reporter passed this information to Antionline, who notified the FBI. I reviewed the information provided to my supervisor by the FBI, and the account names and passwords for USAF systems proved to be authentic.

Special Agent (b) (6), (b) (7)(C) provided the following information to me concerning intrusions into NASA computer systems: On 4 June 1997, NASA system administrators reported (b) (6), (b) (7)(C) a computer system at Goddard Space Flight Center (GSFC), Maryland, had been compromised and was being illegally utilized for IRC communications. On 6 June 97, system administrators reported (b) (6), (b) (7)(C) (GSFC) and (b) (6), (b) (7)(C) (located at the Jet Propulsion Laboratory, California) had also been compromised. Review of system logs and network security systems disclosed the attacks against (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) were initiated from a system in the (b) (6), (b) (7)(C) domain (b) (6), (b) (7)(C) The intruder replaced the WWW page on (b) (6), (b) (7)(C) with a new page that stated (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) had attacked the (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) computer systems. Initial access was gained to these systems via the PHF exploit - an attack that utilizes vulnerability in a computer's WWW service. On 9 June 97, review of network security logs disclosed a connection attempt to (b) (6), (b) (7)(C) from (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) On or about 9 October 1997, a well known hacker had conducted a denial of service attack against IRC operators on the Undernet IRC network. Undernet security personnel reported the attack was initiated from (b) (6), (b) (7)(C) by user name (b) (6), (b) (7)(C) They also stated the attack originated from a hacking group known as "VirII", and identified the IRC nicknames of the group members as (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) Undernet security also provided a reference to a WWW site containing information about (b) (6), (b) (7)(C) true identity. Review of that site disclosed (b) (6), (b) (7)(C) was (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) and he was responsible for extensive computer hacking activity. The site also contained a photograph of (b) (6), (b) (7)(C)

Special Agent (b) (6), (b) (7)(C) also told me the following: In November 1997, an Undernet IRC operator confronted an individual online using the nickname (b) (6), (b) (7)(C) The Undernet operator told (b) (6), (b) (7)(C) he knew his name was (b) (6), (b) (7)(C) acknowledged that was correct. Special Agent (b) (6), (b) (7)(C) told me the following: On 23 February 98, Undernet operators reported an individual using the nickname (b) (6), (b) (7)(C) had accessed the Undernet IRC network from (b) (6), (b) (7)(C) indicating that system had been compromised. Further review disclosed the system, a Cray super computer, had been compromised. NCIS was monitoring a computer system named (b) (6), (b) (7)(C) (IP (b) (6), (b) (7)(C), and detected a connection going to (b) (6), (b) (7)(C) (IP (b) (6), (b) (7)(C) on 23 February 1998, at approximately 2048 EST. Transcripts from this connection were provided to Investigator (b) (6), (b) (7)(C) by Special Agent (b) (6), (b) (7)(C) The **Data Formats and Examples** section of this statement explains the format of this transcript.

Special Agent (b) (6), (b) (7)(C) provided me with the following information concerning (b) (6), (b) (7)(C) Additional investigative activity identified (b) (6), (b) (7)(C) as (b) (6), (b) (7)(C) On 10 March 98, (b) (6), (b) (7)(C) was arrested and interviewed. He disclosed (b) (6), (b) (7)(C) trained him on hacking techniques, and assisted him with numerous computer intrusions, including US Government and military sites. (b) (6), (b) (7)(C) admitted to knowing (b) (6), (b) (7)(C) for 1.5 - 2 years, and stated (b) (6), (b) (7)(C) first name was (b) (6), (b) (7)(C) stated he was (b) (6), (b) (7)(C) "number one" friend, and he

"didn't want to give him up." He stated (b) (6), (b) (7)(C) provided him access to hundreds of computer systems, including US Government and military sites. He said he thought (b) (6), (b) (7)(C) lived in a town near (b) (6), (b) (7)(C) also stated (b) (6), (b) (7)(C) was the primary person responsible for hacking NASA networks, and he also liked to break into military sites hoping to gain notoriety. He also stated there were two people that used the nickname (b) (6), (b) (7)(C) on IRC - one was the person responsible for a large number of hacking attacks (b) (6), (b) (7)(C) the other individual, who used the nickname for approximately five minutes a month, was the person providing (b) (6), (b) (7)(C) with hacking tools and other program code. (b) (6), (b) (7)(C) stated (b) (6), (b) (7)(C) associated with other individuals known as (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) whom also are believed to reside in (b) (6), (b) (7)(C) He also stated either (b) (6), (b) (7)(C) or (b) (6), (b) (7)(C) may be (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) stated he had pictures of (b) (6), (b) (7)(C) and his house on the hard drive of his computer system.

Review of a computer system owned by (b) (6), (b) (7)(C) by NASA/OIG disclosed an IRC log from 21 November 1997 where he had accessed "iarel-info.gov.il" (most likely a misspelling for "israel-info.gov.il") and been discovered during the process. The log file didn't record what IP address (b) (6), (b) (7)(C) was using during that conversation. The log is at Attachment 6 of this statement. The clock for the computer was found to be approximately 20 minutes slow, and set for PST.

Special Agent (b) (6), (b) (7)(C) has provided a set of CD-ROMs that contain data seized from computer systems belong to (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) These have been provided to Investigator (b) (6), (b) (7)(C) and their general layout is described in the **Data Formats and Examples** section of this statement.

Data Formats and Examples

Time Zones: At the request of Investigator (b) (6), (b) (7)(C) I am providing the following definitions concerning different time zones in relation to Israel time:

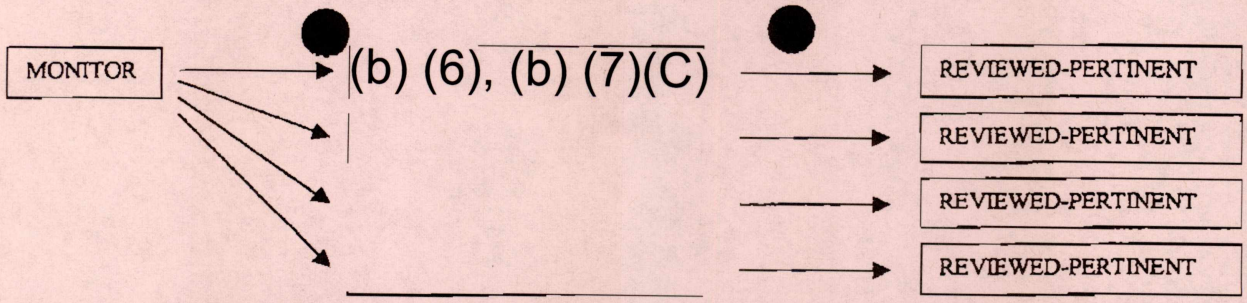
Eastern Standard Time (EST) + 7 hours = Israel Time
Central Standard Time (CST) + 1 hour = EST; CST + 8 hours = Israel Time
Mountain Standard Time (MST) + 2 hours = EST; MST + 9 hours = Israel Time
Pacific Standard Time (PST) + 3 hours = EST; PST + 10 hours = Israel Time

Greenwich Mean Time (GMT) + 2 hours = Israel Time
EST + 5 hours = GMT
CST + 6 hours = GMT
MST + 7 hours = GMT
PST + 8 hours = GMT

Note that these time conversions work prior to Israel clocks being set forward one hour to the summer time standard on 20 March 1998. Currently, information provided by the US investigating team is not set to a standard time zone. At the request of Investigator (b) (6), (b) (7)(C) I will attempt to provide another set of data with all dates and times set to EST at a future date.

AFOSI Network Monitor Data: The data from network monitor devices that AFOSI installed (see **Case Details** section) is stored in two basic formats: a series of text files containing the actual transcripts from the network monitors and a Microsoft Access 97 database. Details about these formats are explained below:

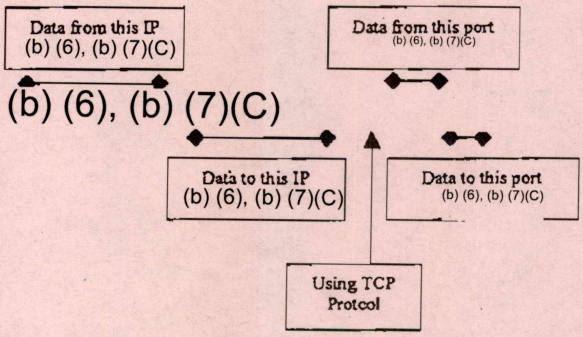
Text Transcripts: A directory of files is provided containing the transcripts from all of the network monitors listed above. They are organized in a directory structure that explains where each text file came from. The diagram below details this directory structure:



A directory called "MONITOR" contains multiple directories, each containing the relevant transcripts from one monitor site, for one day. For example, the diagram above shows four of these directories. The directory named (b) (6), (b) (7)(C) contains the relevant monitor transcripts from the Andrews monitor site at (b) (6), (b) (7)(C) for 3 March 1998. Inside of that directory is another directory called "REVIEWED_PERTINENT". Inside of this directory are the actual transcripts. Below is a sample directory listing of transcript files:

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

The transcript files come in pairs, and they are named according to the IP addresses of computers involved in the connection, the protocol they are using, and the ports they are using. One file contains the data from the initiating computer being sent to the destination computer, and the other contains the data from the destination computer being sent back to the initiating computer. For example, the file (b) (6), (b) (7)(C) contains data from IP address (b) (6), (b) (7)(C) being sent to (b) (6), (b) (7)(C) The communication is using Transmission Control Protocol (TCP), and is going from port (b) (6), (b) (7) on (b) (6), (b) (7)(C) to port (b) (6), on (b) (6), (b) (7)(C) The companion file to this file is (b) (6), (b) (7)(C) This file name shows us data going from (b) (6), (b) (7)(C) on TCP port (b) (6), (t to (b) (6), (b) (7)(C) on TCP port (b) (6), (b) (7)(The diagram below details this information:



The actual transcript files are simple text files containing data intercepted by the network monitor. The example below shows a header from one of these files:

```
Connection File: (b) (6), (b) (7)(C)
Src IP: (b) (6), (b) (7)(C)                    Src Port: (b) (6), (b) (7)(C)
Dst IP:                                        Dst Port:
Start time: Tue Mar  3 17:25:22 1998
```

This header shows the name of the file, a Source IP address, Destination IP address, Source Port, Destination Port, and the Start Time for the session. The Source IP listed here simply means that the data is travelling from the IP listed as the Source to the IP listed as the Destination. It DOES NOT mean that the Source IP is the initiator of the connection. To obtain this information we must look at the end of the transcript file. Below is a sample end of file marking:

```
End time: Tue Mar  3 17:27:39 1998

SYN/no-ACK received: Src IP is initiator
FIN received: Src IP closed this connection half
```

This example shows the end time for the session, and then some information about how the connection ended. The most important piece of data is the part that says "Src IP is initiator". This tells us the that IP address listed as Source IP was in fact the initiator of the connection (meaning that the Source "called" the Destination). Below is the starting and ending of the companion file for this example:

```
Connection File: (b) (6), (b) (7)(C)
Src IP:    (b) (6), (b) (7)(C)                    Src Port:  (b) (6), (b) (7)(C)
Dst IP:  (b) (6), (b) (7)(C)                      Dst Port:
Start time: Tue Mar  3 17:25:22 1998
-------------

End time: Tue Mar  3 17:27:39 1998

SYN/ACK received: Src IP is receiver
FIN received: Src IP closed this connection half
```

This end of file marking shows us that the listed Source IP is the receiver, meaning that the Destination listed in this file "called" the Source. Compare the Source IP and Destination IP from this example to the previous example. They are swapped. Remember that Source IP and Destination IP in these monitor log files simply tell you what direction the data in the transcript file is travelling. The end of the file (the portion that says "Source IP is receiver" or "Source IP is initiator") tell you which machine "called" the other.

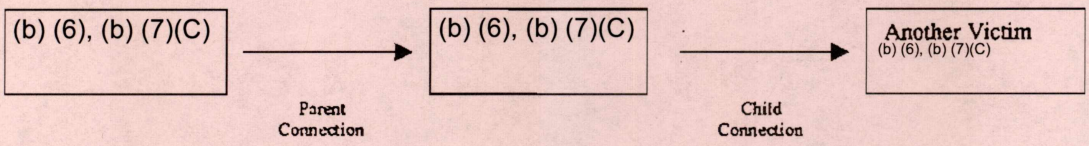
Dates and times are not standardized. The log files from (b) (6), (b) (7)(C) (those directories whose names start with (b) (6), (b) (7)(C) are set to CST. The log files from (b) (6), (b) (7)(C) (directories starting with (b) (6), (b) (7)(C) and the log files from (b) (6), (b) (7)(C) (directories starting with (b) (6), (b) (7)(C) are set to PST. The log files from Andrews AFB (directories starting with ANDREWS) are set to EST.

Access 97 Database: This database was created by AFOSI to summarize all of the information from the network monitor transcripts (described above) and USAF security logs. Each record contains a review of the two transcript files pertaining to a connection (the section above describes in detail the transcript file format). It contains several fields which summarize the data and make it easier to review. The fields used in the database are described below:

Init IP	Initiating IP for the connection	**Init URL**	Domain name assigned to Init IP, if known
Dest IP	Destination IP for the connection	**Dest URL**	Domain name assigned to the Dest IP, if known
Start Date	Starting date and time of the connection	**End Date**	Ending date and time for the connection
Access	Unused field	**OSV**	Operating system version for the victim computer system (typically the Dest IP)
Init Port	Protocol and port for the Init IP (for example, (b) (6), (b) (7)(C)	**Dest Port**	Protocol and port for the Dest IP (for example. (b) (6), (b) (7)(C)
Login	Login name used by person entering the Dest IP system	**File**	Name of the transcript file containing details about the connection, preceded by the date of the connection.
Activity	Summary produced by an analyst of what occurred during the connection	**Tools**	Summary produced by an analyst of what software tools the intruder used during the connection

NOTE - If the "File" field contains an entry that looks something like "Feb-04-98.connections.log.9554" (the date and ending number may not be the same) the information from USAF network security personnel. These transcripts are not included in data given to Investigator (b) (6), (b) (7)(C)

The database is organized by "parent" and "child" connections. A parent connection is the connection between an intruder and a computer system being monitored (b) (6), (b) (7)(C) or (b) (6), (b) (7)(C) A child connection is a connection an intruder makes from the victim system (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) or www.(b) (6), (b) (7)(C) to some other computer system on the Internet. The diagram below gives an example of parent and child connections:



This example shows a connection from (b) (6), (b) (7)(C) to (b) (6), (b) (7)(C) Because the AFOSI monitor is installed at (b) (6), (b) (7)(C) this is called the parent connection. If the intruder then used (b) (6), (b) (7)(C) to connect to another victim system, that connection would be called a child connection.

The original database contains forms for viewing the above data in an organized fashion and easily determining which child connections belong to which parent connections, and producing an official report. Unfortunately, during the process of producing a CD-ROM with the above data, these forms were not copied. I will produce a new CD-ROM containing a revised database and send it directly to Investigator (b) (6), (b) (7)(C) by the fastest means upon my return to the US.

The database datasheets can be viewed, and used to print summary information about connections that were intercepted by AFOSI. Two datasheets, RawData and RawData2, exist in the database. RawData contains information about the parent connections. RawData2 contains information about the child connections. Attachment 7 contains a printout of connection data contained in the database. It displays the Init IP, Init URL, Dest IP, Dest URL, Start Date, and Dest Port fields from the database. Note that the Start Date field is according to the clock of the network monitor that intercepted the data. A future version of the database will standardize all times to EST.

Examples of Monitor Data: Investigator (b) (6), (b) (7)(C) requested I review two connection sessions and provide examples of network monitor data to demonstrate how it can be used during the investigation. For these examples, we selected two connections to (b) (6), (b) (7)(C) that have subsequent connections to other computer systems. One connection is to (b) (6), (b) (7)(C) a US Government Cray computer system, and the other is to (b) (6), (b) (7)(C) when (b) (6), (b) (7)(C) is suspected of changing the Netdex web page to take credit for intrusions into Department of Defense computer systems.

(b) (6), (b) (7)(C) Attachments 8 and 9 contain the transcript files of a connection from IP (b) (6), (b) (7)(C) to (b) (6), (b) (7)(C) , IP (b) (6), (b) (7)(C) The connection started on 15 February 1998 at 1729 CST, and ended on 16 February 1998 at 0057 CST. Attachment 8 contains the data sent from (b) (6), (b) (7)(C) to (b) (6), (b) (7)(C) (filename (b) (6), (b) (7)(C) , which represents the keystrokes pressed by the intruder, and Attachment 9 contains the data sent from (b) (6), (b) (7)(C) to (b) (6), (b) (7)(C) (filename (b) (6), (b) (7)(C) which represents data displayed on the terminal of the intruder. The attachments contain the entire transcript. In order to make explanation easy, I have handwritten comments on the attachments explaining what the intruder is doing at various points in the transcript file. I have only annotated Attachment 9, which shows the data that was displayed on the intruders terminal, for simplicity. Attachment 7, a summary of connection information, contains entries that detail these log files. I have marked the entries on the Attachment with a * symbol that pertain to this session.

(b) (6), (b) (7)(C) Attachments 10 and 11 contain the transcript files of a connection from (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) IP (b) (6), (b) (7)(C) to (b) (6), (b) (7)(C) IP (b) (6), (b) (7)(C) The connection started on 3 March 1998 at 1728 CST, and ended on 3 March 1998 at 2149 CST. Attachment 10 contains the data sent from from (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) to (b) (6), (b) (7)(C) (filename (b) (6), (b) (7)(C) which represents the keystrokes pressed by the intruder, and Attachment 11 contains the data sent from (b) (6), (b) (7)(C) to from (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) (filename (b) (6), (b) (7)(C) , which represents data displayed on the terminal of the intruder. The attachments contain the entire transcript. In order to make explanation easy, I have handwritten comments on the attachments explaining what the intruder is doing at various points in the transcript file, and verified my handwriting by my initials. I have only annotated Attachment 11, which shows the data that was displayed on

the intruders terminal, for simplicity. Attachment 7, a summary of connection information, contains entries that detail these log files. I have marked the entries on the Attachment with a '-' symbol that pertain to this session.

(b) (6), (b) (7)(C) **IRC Transcripts:** During the AFOSI review of (b) (6), (b) (7)(C) computer system, I separated the IRC data and produced a Microsoft Excel 97 spreadsheet of automated search results called IRC_REVIEW.XLS. The spreadsheet contains four different worksheets. Examples from each are listed below:

1. hotlist - a listing of keywords that were discovered in the IRC log files. The worksheet contains the keyword, nickname of the person that "said" it, the line of text where the word was discovered, the session date (according to (b) (6), (b) (7)(C) system clock, 2 years, 10 days, 22 minutes slow), and a URL to the IRC log file containing the data.

Keyword	Nickname (b) (6), (b) (7)(C)	Channel	Text	Session Date	File
.GOV		UNKNOWN	(b) (6), (b) (7)(C)	Feb 11 11:19:01 1996	(b) (6), (b) (7)(C)
.GOV		UNKNOWN		Feb 11 11:19:01 1996	
.GOV		UNKNOWN		Jan 11 12:35:34 1996	
.GOV		#the_company		Feb 02 17:18:29 1996	
.GOV		#the_company		Feb 02 17:18:29 1996	

2. alias - shows where IRC users change their nickname. The worksheet contains the original nickname used, the new nickname, the channel where the user was talking, the session date (according to (b) (6), (b) (7)(C) system clock), and a URL to the IRC log file containing the data.

Original Nickname	New Nickname	Channel	Session Date	File
(b) (6), (b) (7)(C)			Dec 23 23:05:52 1995	(b) (6), (b) (7)(C)
			Dec 26 19:25:12 1995	
			Jan 14 23:42:09 1996	
			Dec 24 15:24:31 1995	
			Dec 31 18:18:11 1995	

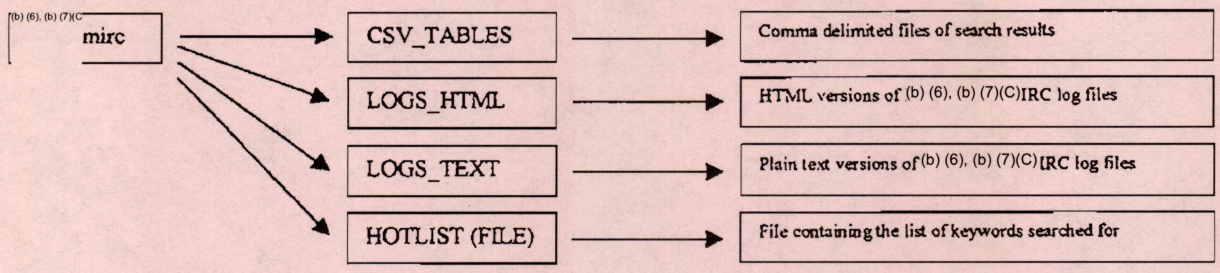
3. nick_id - shows where IRC messages are displayed that identify usernames and system addresses being used by other IRC users. The worksheet contains the nickname of the person identified, the channel they were talking in, the username they were using, the system address, the session date (according to (b) (6), (b) (7)(C) system clock), and a URL to the IRC log file containing the data.

Nickname	Channel	Username	System Address	Session Date	File
(b) (6), (b) (7)(C)				Feb 15 17:42:23 1996	(b) (6), (b) (7)(C)
				Feb 14 17:20:49 1996	
				Feb 05 15:44:02 1996	
				Dec 26 19:25:12 1995	
				Dec 26 19:25:12 1995	

4. system - shows where IRC users discuss other computer systems. The worksheet contains the nickname of the person discussing the system, the channel where it was discussed, the identity of the system, the session date (according to (b) (6), (b) (7)(C) system clock), and a URL to the IRC log file containing the data.

Nickname	Channel	System Discussed	Session Date	File
(b) (6), (b) (7)(C)			Dec 24 15:24:31 1995	(b) (6), (b) (7)(C)
			Dec 18 20:08:20 1995	
			Jan 20 11:[illegible] 1996	
			Jan 25 17:36:29 1996	
			Jan 27 21:28:02 1996	

IRC Log Directory Structure: The diagram below explains how the IRC logs from (b) (6), (b) (7)(C) computer system are stored on the set of data provided to Investigator (b) (6), (b) (7)(C)



CD-ROMs of Computer Systems Involving (b) (6), (b) (7)(C) NASA/OIG prepared CD-ROMs containing copies of the logical file structure from computer systems involved in their investigation of (b) (6), (b) (7)(C) I have labeled the CD-ROMs and provided a brief description of their contents below:

Disk 1: Composite CD containing relevant files from (b) (6), (b) (7)(C)
(b) (6), (b) (7)(C) computer, and (b) (6), (b) (7)(C)

Disk 2: Logical file structure from (b) (6), (b) (7)(C) computer system.

Disk 3: Logical file structure from (b) (6), (b) (7)(C) computer system, 1st partition.

Disk 4: Logical file structure from computer system, 2nd partition.

Disk 5: Logical file structure from (b) (6), (b) (7)(C) computer system.

Monitor Transcript from NCIS: NCIS conducted monitoring operations at (b) (6), (b) (7)(C) Their monitor detected a connection from (b) (6), (b) (7)(C) to (b) (6), (b) (7)(C) on 23 February 1998 at approximately 1803 EST. The transcript is at Attachment 12. As I do not have sufficient personal knowledge of the transcript, I cannot provide an explanation of the transcript materials. Further information on this topic will be available at a later date.

Attachment Listing

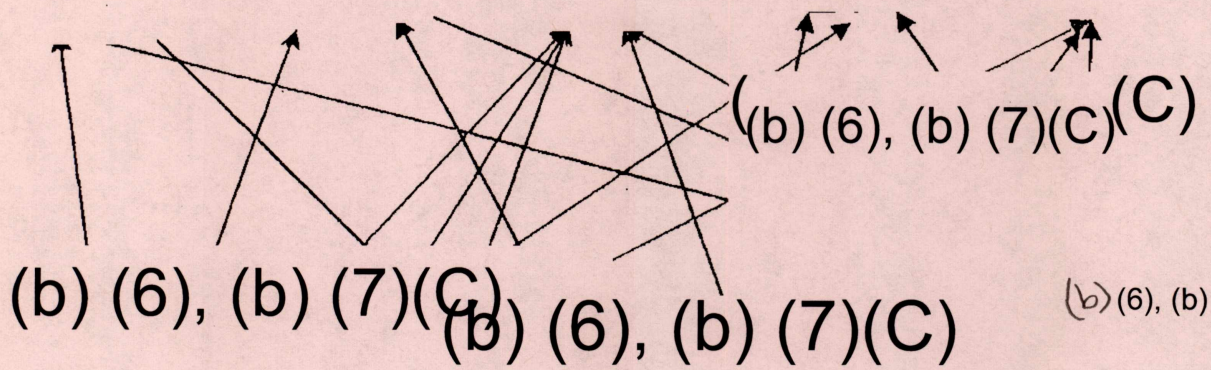
The following list of Attachments has been prepared by me and is part of my official statement:

1. Diagram of initial attack activity against USAF systems (3 pages)
2. IRC conversation intercepted by sonic.net (14 pages)
3. (b) (6), (b) (7)(C) LOG (12 pages)
4. Excerpt from (b) (6), (b) (7)(C) LOG (10 pages)
5. Hotmail logs for (b) (6), (b) (7)(C) account (3 pages)
6. Excerpt from (b) (6), (b) (7)(C) LOG on (b) (6), (b) (7)(C) computer (1 page)
7. Connection data from Access 97 database of monitor logs (7 pages)
8. Monitor transcript for (b) (6), (b) (7)(C) (7 pages)
9. Monitor transcript for (34 pages)
10. Monitor transcript for 3 pages)
11. Monitor transcript for 28 pages)
12. Monitor transcript from (b) (6), (b) (7)(C) (10 pages)

(b) (6), (b) (7)(C) SA, USAF
AFOSI Computer Crime Investigations Division

Attachment 1

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

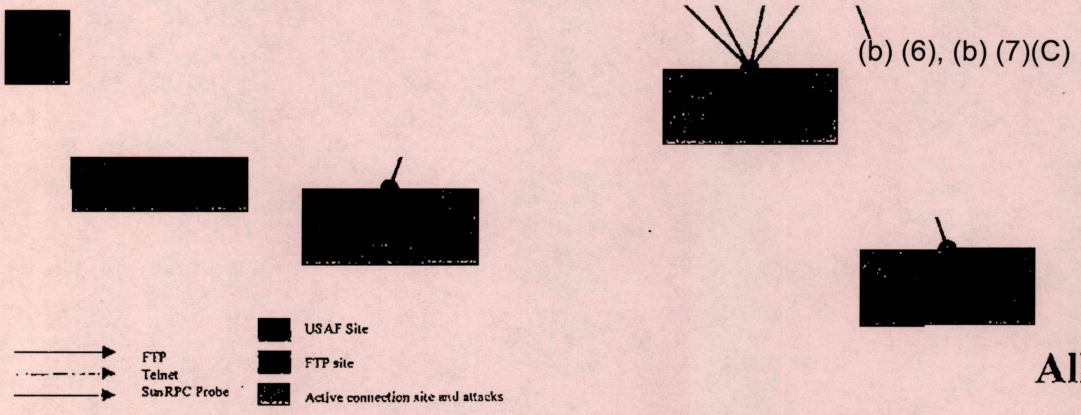


(b) (6), (b) (7)(C)

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

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

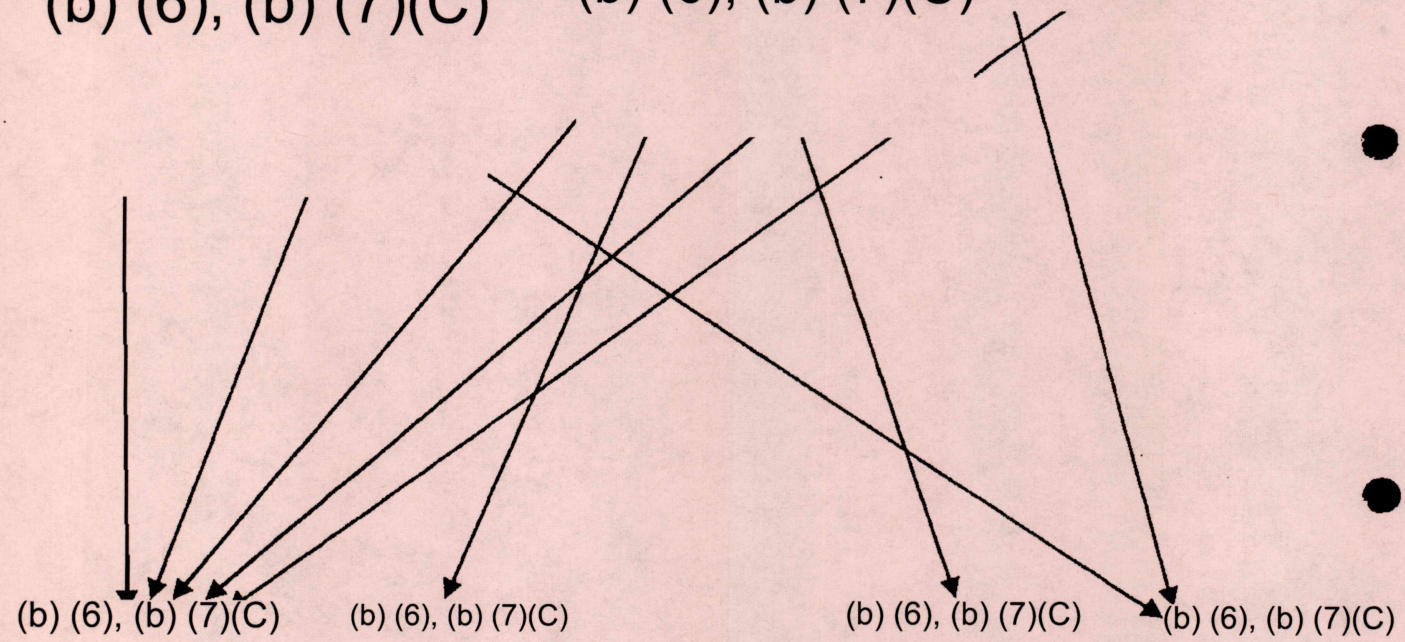
(b) (6), (b) (7)(C)



All times EST

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

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

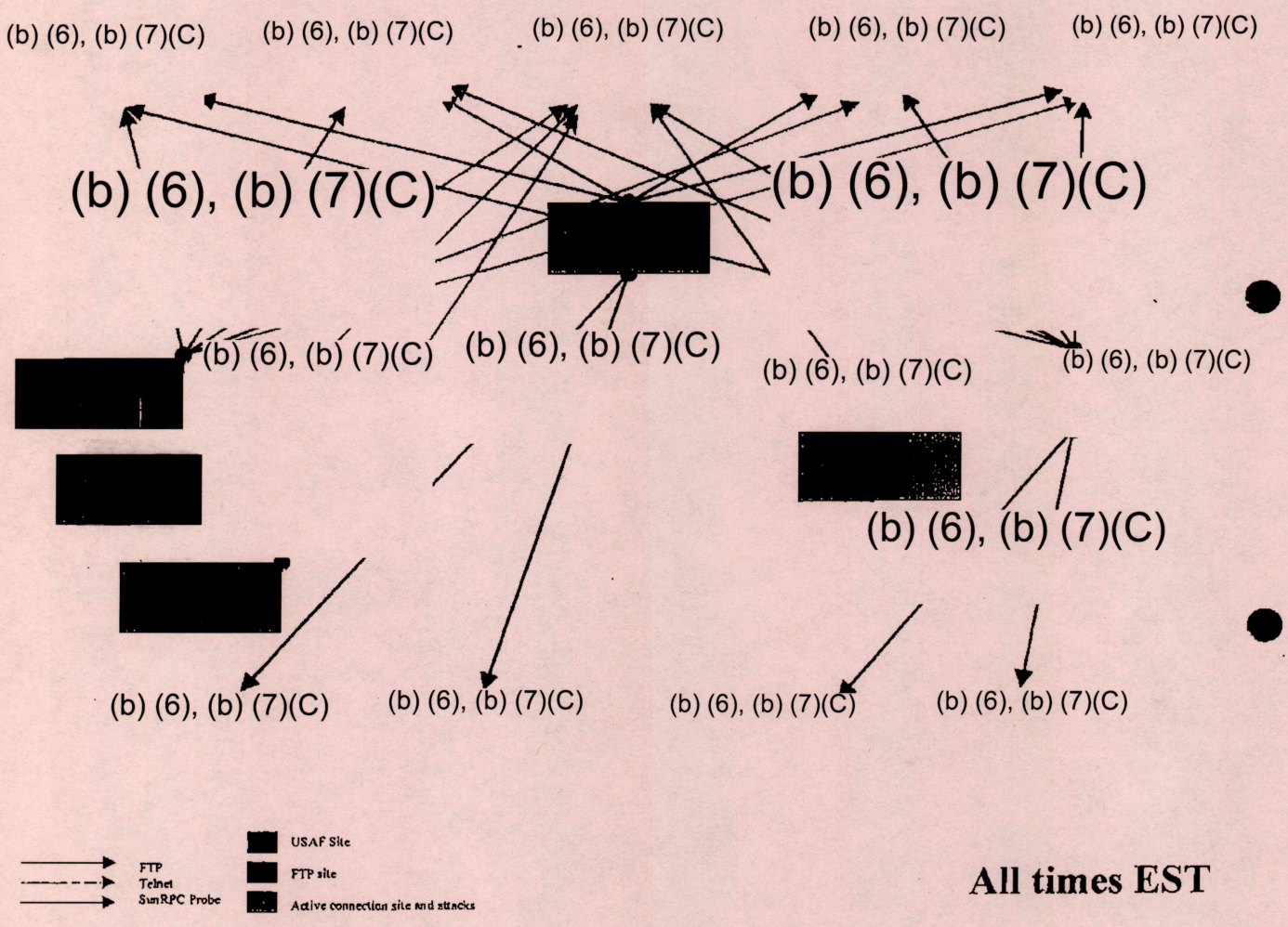


(b) (6), (b) (7)(C) (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) (b) (6), (b) (7)(C)

FTP
Telnet
SunRPC Probe

USAF Site
FTP site
Active connection site and attacks

All times EST



All times EST

Attachment 2

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Attachment 3

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

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

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

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

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

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

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

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

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

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

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

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

Attachment 4

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

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

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

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

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

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