

03/12/99  
10:03:41

FD-192

ICMIPR01  
Page 1

Title and Character of Case:

AIR FORCE INSTITUTE OF TECHNOLOGY  
MOONLIGHT MAZE

Date Property Acquired: Source from which Property Acquired:

02/08/1999

[Redacted box]

b3  
OTHER

Anticipated Disposition: Acquired By: Case Agent:

[Redacted box]

b6  
b7C

Description of Property:

Date Entered

1B 9

[Redacted box]

b3  
OTHER

Barcode: E1394242

Location: ~~ECRAU1~~

~~BIN1~~

~~S4~~

02/08/1999

ECR/L/4

**FILE COPY**

Case Number: 288-CI-68562 - 1B(9)  
Owning Office: SAN ANTONIO

RDW/BB

288-CI-68562-109

10/11/98  
10:10:34

~~SECRET~~  
FD-192

ICMIPR01  
Page 1

Title and Character of Case:

AIR FORCE INSTITUTE OF TECHNOLOGY

Date Property Acquired: Source from which Property Acquired:

09/25/1998

[Redacted] EIU

CHARLESTON IL

b6  
b7C

Anticipated Disposition: Acquired By: Case Agent:

[Redacted]

Description of Property:

Date Entered

1D 1

TAPE #14058  
1 8MM SONY DATA CARTRIDGE  
VOLUNTEERED

Barcode: E1474422 Location: ELSUR1 CAB4 S3 10/11/1998

*288-CI-68562-131*

SEARCHED INDEXED  
SERIALIZED FILED  
*[Signature]*

Case Number: <sup>(U)</sup> 288-CI-68562 ~~(S)~~ - 1D 1  
Owning Office: SPRINGFIELD

~~SECRET~~

*Tape 14058*

SEARCHED INDEXED  
SERIALIZED FILED  
OCT 11 1998  
FBI - SPRINGFIELD  
*[Signature]*

03/22/99  
21:03:07

Title and Character of Case:

AIR FORCE INSTITUTE OF TECHNOLOGY  
MOONLIGHT MAZE

Date Property Acquired: Source from which Property Acquired:

03/15/1999

[REDACTED] AUBURN UNIVERSITY

b6  
b7c

Anticipated Disposition: Acquired By: Case Agent:

[REDACTED]

Description of Property:

Date Entered

1B 15

ONE(1) SONY 8MM DATA CARTRIDGE

Barcode: E1182456

Location: ECR

CAB8

S2

03/18/1999

Case Number: 288-CI-68562  
Owning Office: MOBILE

1B15

FILE COPY

SEARCHED	INDEXED
SERIALIZED	FILED
MAR 22 1999	
FBI-MOBILE	

03/17/99  
12:03:13

FD-192

Title and Character of Case:

AIR FORCE INSTITUTE OF TECHNOLOGY  
MOONLIGHT MAZE

Date Property Acquired: 03/12/1999  
Source from which Property Acquired: [redacted] PEN REGISTER [redacted] b3

Anticipated Disposition: Acquired By: [redacted] Case Agent: [redacted] b6 b7C

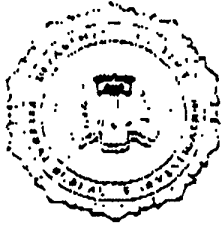
Description of Property: 1B 14 Date Entered

[redacted] PEN REGISTER [redacted] b3

Barcode: E1663896 Location: [redacted] Date Entered: 03/17/1999

Case Number: 288-CI-68562-1B14  
Owning Office: PHILADELPHIA

[redacted] b6 b7C



~~Secret~~

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 07-03-2012 BY 60324/UC/baw/sab/aio

FBI FACSIMILE

COVERSHEET

PRECEDENCE

Immediate  
Priority  
Routine

CLASSIFICATION

Top Secret  
Secret  
Confidential  
Sensitive  
Unclassified

Time Transmitted \_\_\_\_\_  
Sender's Initials \_\_\_\_\_  
Number of Pages 2  
(including coversheet)

To Cincinnati

Name of Office

Date: 7-14-98

Facsimile Number 513 562 548 5838

Via SSA

Name

Room

Telephone

From: NIP & CIU

Name of Office

Subject: Unsub;  
University of Cin - Victim  
Wright - Patterson Air Force Base - Victim  
June 1, 1998 to July 9, 1998  
CETA - Intrusion  
Special Handling Instructions: FYI

b6  
b7c

Originator's Name

Telephone:

Originator's Facsimile Number: 202 324 0311

Approved: [Signature]

Referral/Consult

Brief Description of Communication Faxed:

[Redacted area]

~~Secret~~

JUL 21 1998

CINNATI

[Signature]

b6  
b7c



# FBI FACSIMILE COVER SHEET

### PRECEDENCE

- Immediate
- Priority
- Routine

### CLASSIFICATION

- Top Secret
- Secret
- Confidential
- Sensitive
- Unclassified

Time Transmitted: 3:30  
 Sender's Initials: bee  
 Number of Pages: 26  
 (including cover sheet)

To: FBIHQ NIPC  
 Name of Office

Date: 7/14/98

Facsimile Number: 202 324 - 0311

Attn: UC   
 Name Room Telephone

*288/RW/SPK*  
*w/n: NATL SEC PROBLEM*  
*OF ASSISTANCE*  
*BY UE STUDENT*  
  
*: COORD OSI - WILL NEED*  
*INTERVIEW OF*  
*ATEIA ACCOUNT*  
*ROMANIAN STUDENT.*  
  
*: EC TO OPEN 288*  
  
*COMPUTER CONTACTS.*  
  
*: FORM 801-*  
  
*ONE 288-0*  
*OF 88*

From: CINCINNATI  
 Name of Office

Subject: OSI COMPUTER CASE  
AT WPAFB

Special Handling Instructions: \_\_\_\_\_

Originator's Name: SSA  Telephone:

Originator's Facsimile Number: 513 562 - 5650

Approved: RW

Brief Description of Communication Faxed: \_\_\_\_\_

### WARNING

Information attached to the cover sheet is U.S. Government Property. If you are not the intended recipient of this information, disclosure, reproduction, distribution, or use of this information is prohibited (18.U.S.C., § 641). Please notify the originator or local FBI Office immediately to arrange for proper disposition.

# FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 06/15/1998

To: Director, FBI

Attn: Computer Investigations  
Unit, CIOS, NIPC,  
Rm. 11887

From: SAC, Cincinnati

Approved By:

[Redacted Signature Box]

Drafted By:

*[Handwritten initials/signature]*

b6  
b7C

Case ID #: 288-CI-0

Title: Subject: UNSUB;  
Victim: USAF-Cataloging and Standardization  
Type: Intrusion  
Date: 6/2/98

SUBMISSION:  Initial  Supplemental  Closed

CASE OPENED: \_\_\_/\_\_\_/\_\_\_

CASE CLOSED: \_\_\_/\_\_\_/\_\_\_

- No action due to state/local prosecution  
(Name/Number \_\_\_\_\_)
- USA declination
- Referred to Another Federal Agency  
(Name/Number: \_\_\_\_\_)
- Placed in unaddressed work
- Closed administratively
- Conviction

*[Large handwritten circle containing signature and date 8/12/98]*  
*[Redacted box]*  
*[Handwritten date 8/17/98]*

b6  
b7C

COORDINATION: FBI Field Office IP SA [Redacted] (LRA)  
Government Agency AFOSI Detachment 101 WPAFB, Dayton, OH  
Private Corporation \_\_\_\_\_

Company name/Government agency: USAF  
Address/location: Federal Center, Battle Creek, MI

Purpose of System: 1) Dracula; e-mail; back up DNS 2) Hyde; Data base server  
Highest classification of information stored in system: Unclassified *288-CI-68562-3*

SEARCHED	INDEXED
SERIALIZED	FILED
JUN 17 1998	
FBI - CINCINNATI	

*[Handwritten notes: Transfer to 288-CI-68562-3, 68562]*

167CLW03.0TH

To: Director, FBI From: SAC,  
Re: 288- , Date

**System Data:**

Hardware/configuration (CPU):\_1) SunSpare 20 2) SunSpare 1000\_\_\_\_\_  
Operating System: \_\_Solaris 2.4\_\_\_\_\_  
Software: \_\_E-mail exchanger; Unify\_\_\_\_\_

**Security Features:**

Security Software Installed:  yes (identify \_\_\_\_\_)  no  
Logon Warning Banner:  yes  no

**INTRUSION INFORMATION**

**Access for intrusion:**  Internet connection  dial-up number  LAN (insider)

If Internet: Internet address:

Network name:

b7E

**Method:**

Technique(s) used in intrusion: \_\_\_\_\_ (list provided)

**Path of intrusion:**

addresses: 1. \_\_\_\_\_ 2. \_\_\_\_\_ 3. \_\_\_\_\_ 4. \_\_\_\_\_ 5. \_\_\_\_\_

country: 1. \_\_\_\_\_ 2. \_\_\_\_\_ 3. \_\_\_\_\_ 4. \_\_\_\_\_ 5. \_\_\_\_\_

facility: 1. \_\_\_\_\_ 2. \_\_\_\_\_ 3. \_\_\_\_\_ 4. \_\_\_\_\_ 5. \_\_\_\_\_

**Subject:**

Age: \_\_\_\_\_ Race: \_\_\_\_\_

Sex: \_\_\_\_\_ Education: \_\_\_\_\_

Alias(s): \_\_\_\_\_ Motive: \_\_\_\_\_

Group Affiliation: \_\_\_\_\_

Employer: \_\_\_\_\_

Known Accomplices: \_\_\_\_\_

Equipment used:

Hardware/configuration (CPU): \_\_\_\_\_

Operating System: \_\_\_\_\_

Software: \_\_\_\_\_

**Impact:**

Compromise of classified information:  yes  no

Estimated number of computers affected: \_\_2\_\_\_\_\_

Estimated dollar loss to date: \_\_Unknown\_\_\_\_\_



To: Director, FBI From: SAC,  
Re: 288- , Date

**Category of Crime:**

**Impairment:**

- Malicious code inserted
- Denial of service
- Destruction of information/software
- Modification of information/software

**Theft of Information:**

- Classified information compromised
- Unclassified information compromised
- Passwords obtained
- Computer processing time obtained
- Telephone services obtained
- Application software obtained
- Operating software obtained

**Intrusion:**

- Unauthorized access Stat D
- Exceeding authorized access

---

**REMARKS**

◆◆

(01/26/1998)

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 07-03-2012 BY 60324/UC/baw/sab/aio

~~SECRET~~

**FEDERAL BUREAU OF INVESTIGATION**

Precedence: ROUTINE

Date: 08/10/1998

To: National Security

Attn: NIPC-CIU, Room 11887;  
SSA [redacted]

From: Cincinnati  
Squad 4

Contact: SA [redacted]

b6  
b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: ~~(U)~~ ~~(S)~~ ✓ 288-CI-68562 - (Pending) 4

Title: ~~(U)~~ ~~(S)~~ UNSUB(S);  
UNITED STATES AIR FORCE  
INSTITUTE OF TECHNOLOGY,  
HACKING ATTACK ON:  
[redacted]

b7E

Synopsis: ~~(U)~~ ~~(S)~~ Preliminary information and case summary  
concerning captioned matter.

~~(U)~~ ~~(S)~~ Derived From: G-3  
Declassify On: X1

[redacted]

(U) Administrative: Referenced enclosures serve as a means to  
furnish NSD, NIPC-CIU, a more detailed synopsis of captioned  
matter.

[redacted]

Referral/Consult

~~SECRET~~

288-CI-68562-4

Searched \_\_\_\_\_  
Serialized \_\_\_\_\_  
Indexed \_\_\_\_\_  
Filed \_\_\_\_\_

TJW/BB

2223B01.EC



[Redacted]

[Redacted]

[Redacted] shows [Redacted]  
DOB [Redacted] arrived on [Redacted] on a F-1 (student) visa.

LEXIS/NEXIS shows current address [Redacted]  
[Redacted] Previous addresses [Redacted]  
[Redacted]

b6  
b7C  
b7E

LEADS shows [Redacted]  
[Redacted] with a current [Redacted] driver's license [Redacted] issued  
[Redacted] expiring [Redacted] is described as [Redacted]  
[Redacted]

That's all I found.

[Redacted]

288-17-68562-5  
SEARCHED INDEXED  
SERIALIZED FILED  
AUG 12 1998  
NATI  
[Redacted] [Signature]

b6  
b7C

7/31/98

FD-759 (Rev 5-25-95)

To: Director, FBI ( )  
Attn: CID, DIPC-CTD Section

From: SAC, CINCINNATI ( 288-CI-68562 ) ( 2 )

For FBI Field Office use only

Title: UNSUB(S);  
UCAP  
LIBRARY OF TECHNOLOGY,  
HACKING ATTACK ON  
[Redacted]

Notification of SAC Authority Granted for Use of  
CONSENSUAL Monitoring Equipment  
(Check only ONE)  
 Routine Use  
 Emergency Use-Sensitive Circumstances (cannot exceed  
30 days & may be extended only by FBIHQ).

b7E

This form must be typewritten & submitted within 10 working days  
of the date authority is granted as shown in Item 5 below.

1. Reason for Proposed Use: (Check) <input type="checkbox"/> Corroborate Testimony <input type="checkbox"/> Protect Consenting Party <input type="checkbox"/> Protect Government Property <input checked="" type="checkbox"/> Collect Evidence <input type="checkbox"/> Other (Specify) _____		2. Type of Equipment: (Check) <input type="checkbox"/> Transmitter/Receiver <input type="checkbox"/> Concealed Recorder <input type="checkbox"/> CCTV/Audio & Video <input type="checkbox"/> CCTV Video only <input type="checkbox"/> Microphone <input type="checkbox"/> Telephone <input checked="" type="checkbox"/> Other (Specify) <u>Network Monitor</u>	
3. Consenting Party (Identify ONLY on Field Office Copy) <input checked="" type="checkbox"/> Nonconfidential Party <input type="checkbox"/> Confidential Source <input type="checkbox"/> Cooperative Witness		4. Interceptee(s): (Include Title if Public Official) <u>University of Cincinnati, College of Engineering &amp; Computer Science</u> & others as yet unknown.	
5. Duration of proposed use: Authorized On: _____ <input checked="" type="checkbox"/> For the duration of investigation <input type="checkbox"/> For 30 days (Emergency NTCM usage) Expiring On: _____	6. Equipment Concealed: <input type="checkbox"/> In a Motel Rm. <input type="checkbox"/> In a Residence <input type="checkbox"/> In a Vehicle <input checked="" type="checkbox"/> Other (Specify) <u>Secured Network Room</u>	7. City & State where Equipment will be used: <u>Cincinnati, Ohio</u>	
8. The following mandatory requirements have been met: <input checked="" type="checkbox"/> Consenting party has agreed to testify; <input checked="" type="checkbox"/> Consenting party has executed a consent form; & <input checked="" type="checkbox"/> Recording/transmitting device will be activated only when consenting party is present.		9. Government Attorney in judicial district where monitoring and/or recording will take place has been contacted; foresees no entrapment; & concurs in the use of the technique. <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Date of Contact: <u>4/17/14</u> Identity of Gov't Atty: <u>AUSA [Redacted]</u> Judicial District: <u>Southern District of Ohio</u>	
10. Violation(s): Title(s) <u>18</u> Sec(s) <u>1030</u> USC			
11. DOJ notification required <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No. If "Yes" check reason below: NOTE: Requests for Routine NTCM usage involving any of the 7 sensitive circumstances requires a teletype to HQ prepared in the format described in the MIOG, Part II, Section 10-10.3 (8). Request for Emergency NTCM usage involving Item 6 below requires immediate contact with the FBIHQ substantive desk for DOJ approval. The 7 sensitive circumstances do not apply to the use of CCTV video only.			
1. <input type="checkbox"/> Interception relates to an investigation of a member of Congress; a Federal Judge; a member of the Executive Branch at Executive Level IV or above; or a person who has served in such capacity within the previous 2 years.			
2. <input type="checkbox"/> Interception relates to an investigation of any public official and the offense investigated is one involving bribery; conflict of interest; or extortion relating to the performance of his/her official duties.			
3. <input type="checkbox"/> Interception relates to an investigation of a Federal law enforcement official.			
4. <input type="checkbox"/> Consenting/nonconsenting party is a member of the diplomatic corps of a foreign country.			
5. <input type="checkbox"/> Consenting/nonconsenting party is or has been a member of the Witness Security Program and that fact is known to the agency involved or its officers.			
6. <input type="checkbox"/> Consenting/nonconsenting party is in the custody of the Bureau of Prisons or the U.S. Marshals Service.			
7. <input type="checkbox"/> Attorney General; Deputy Attorney General; Associate Attorney General; Assistant Attorney General for the Criminal Division; or the U.S. Attorney in the district where an investigation is being conducted has requested the investigating agency to obtain prior written consent for making a consensual interception in a specific investigation.			

b6 |  
b7C

12. Synopsis of Case: (Attach additional page if necessary)  
Please see attached.

13. Justification statement necessitating emergency authorization:  
 Emergency 30 day authorization granted due to imminent need (within 48 hours) for use of consensual monitoring device(s), which precluded the handling of this request in the usual manner.  
 Other (Attach Additional Page to Specify)

<b>Field Approval</b>	
14. CDC (If Sensitive Circumstances Exist) Signature _____ Date: _____	
15. SAC Signature <u>[Signature]</u> Date: <u>7/31/98</u>	
<b>FBIHQ Approval</b>	
16. Unit Chief (If Sensitive Circumstances Exist) Signature _____ Date: _____	

1-Government Attorney's Office

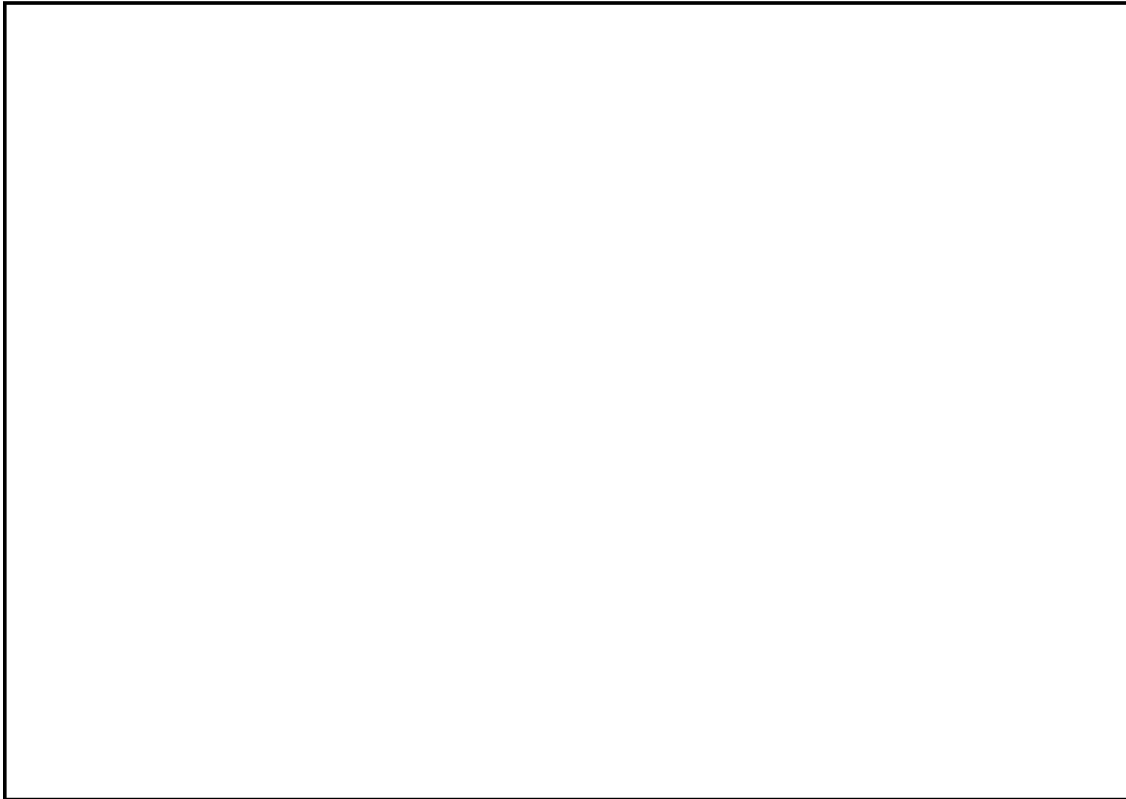
Attn: \_\_\_\_\_

~~SECRET~~

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 07-05-2012 BY 60324/UC/baw/sab/aio

**Background:**

Referral/Consult



**b. Governing Statutes:**

(U) Title 18, United States Code (USC), Section 1030, Fraud and Related Activity in Connection with Computers

**MISSION:**

(U) ~~(S)~~ The primary mission of this operation will be to identify modus operandi, tradecraft and tools being utilized by this hacker. If possible, determine if the hacker is associated with a Foreign Intelligence Service and the extent of the FIS involvement and direction in his/her activity. If this is a FIS operation it would also provide extensive insight in to the conduct of FIS and their capabilities in attacking our information systems. Through these efforts we will identify the vulnerabilities which allowed this individual to gain access to the computer systems, thereby being able to anticipate and develop countermeasures to prevent this from taking place in the future. This would not only apply to the AFIT/WPAFB systems but to computer systems throughout the Department of Defense.

(U) A secondary objective of this investigation is to reduce, through prosecution, the hacking activities against military, commercial and private computer and network systems.

~~SECRET~~

7/31/98

FD-759 (Rev. 5-25-95)

To: Director, FBI ( )  
Attn: CID, NIPC-CID Section

From: SAC, CINCINNATI ( 208-CI-60562 )

For FBI Field Office use only  
CM#:

Title: UNSUB(S);  
UCAP  
INSTITUTE OF TECHNOLOGY  
HACKING ATTACK ON  
[REDACTED]

Notification of SAC Authority Granted for Use of  
CONSENSUAL Monitoring Equipment  
(Check only ONE) AUG 01 11 09 20

- Routine Use
- Emergency Use Sensitive Circumstances (cannot exceed 30 days & may be extended only by FBIHQ).

b7E

This form must be typewritten & submitted within 10 working days of the date authority is granted as shown in Item 5 below.

<p>1. Reason for Proposed Use: (Check)</p> <p><input type="checkbox"/> Corroborate Testimony    <input type="checkbox"/> Protect Consenting Party    <input type="checkbox"/> Protect Government Property    <input checked="" type="checkbox"/> Collect Evidence</p> <p><input type="checkbox"/> Other (Specify) _____</p>	<p>2. Type of Equipment: (Check)</p> <p><input type="checkbox"/> Transmitter/Receiver    <input type="checkbox"/> Concealed Recorder  <input type="checkbox"/> CCTV/Audio &amp; Video    <input type="checkbox"/> CCTV Video only  <input type="checkbox"/> Microphone    <input type="checkbox"/> Telephone  <input checked="" type="checkbox"/> Other (Specify) <u>Network Monitor</u></p>
<p>3. Consenting Party (Identify ONLY on Field Office Copy)</p> <p><input checked="" type="checkbox"/> Nonconfidential Party  <input type="checkbox"/> Confidential Source  <input type="checkbox"/> Cooperative Witness</p>	<p>4. Interceptee(s): (Include Title if Public Official)</p> <p><u>Wright State University, College of Engineering &amp; Computer Science</u>        &amp; others as yet unknown.</p>
<p>5. Duration of proposed use:</p> <p>Authorized On: _____  <input checked="" type="checkbox"/> For the duration of investigation  <input type="checkbox"/> For 30 days (Emergency NTCM usage)        Expiring On: _____</p>	<p>6. Equipment Concealed:</p> <p><input type="checkbox"/> In a Motel Rm.    <input type="checkbox"/> In a Telephone  <input type="checkbox"/> In a Residence    <input type="checkbox"/> On a Person  <input type="checkbox"/> In a Vehicle  <input checked="" type="checkbox"/> Other (Specify) <u>Secured Network Room</u></p>
<p>8. The following mandatory requirements have been met:</p> <p><input checked="" type="checkbox"/> Consenting party has agreed to testify;  <input checked="" type="checkbox"/> Consenting party has executed a consent form; &amp;  <input checked="" type="checkbox"/> Recording/transmitting device will be activated only when consenting party is present.</p>	<p>9. Government Attorney in judicial district where monitoring and/or recording will take place has been contacted; foresees no entrapment; &amp; concurs in the use of the technique.</p> <p><input checked="" type="checkbox"/> Yes    <input type="checkbox"/> No    Date of Contact: <u>8/17/98</u></p> <p>Identity of Gov't Atty: <u>RUSA</u> [REDACTED]        Judicial District: <u>Southern District of Ohio</u></p>
<p>10. Violation(s): Title(s) <u>18</u> Sec(s) <u>1030</u> USC</p>	
<p>11. DOJ notification required <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No. If "Yes" check reason below:        NOTE: Requests for Routine NTCM usage involving any of the 7 sensitive circumstances requires a teletype to HQ prepared in the format described in the MIOG, Part II, Section 10-10.3 (8). Request for Emergency NTCM usage involving Item 6 below requires immediate contact with the FBIHQ substantive desk for DOJ approval. The 7 sensitive circumstances do not apply to the use of CCTV video only.</p> <ul style="list-style-type: none"> <li>1. <input type="checkbox"/> Interception relates to an investigation of a member of Congress; a Federal Judge; a member of the Executive Branch at Executive Level IV or above; or a person who has served in such capacity within the previous 2 years.</li> <li>2. <input type="checkbox"/> Interception relates to an investigation of any public official and the offense investigated is one involving bribery; conflict of interest; or extortion relating to the performance of his/her official duties.</li> <li>3. <input type="checkbox"/> Interception relates to an investigation of a Federal law enforcement official.</li> <li>4. <input type="checkbox"/> Consenting/nonconsenting party is a member of the diplomatic corps of a foreign country.</li> <li>5. <input type="checkbox"/> Consenting/nonconsenting party is or has been a member of the Witness Security Program and that fact is known to the agency involved or its officers.</li> <li>6. <input type="checkbox"/> Consenting/nonconsenting party is in the custody of the Bureau of Prisons or the U.S. Marshals Service.</li> <li>7. <input type="checkbox"/> Attorney General; Deputy Attorney General; Associate Attorney General; Assistant Attorney General for the Criminal Division; or the U.S. Attorney in the district where an investigation is being conducted has requested the investigating agency to obtain prior written consent for making a consensual interception in a specific investigation.</li> </ul>	
<p>12. Synopsis of Case: (Attach additional page if necessary)</p> <p style="text-align: center;"><b>Please see attached.</b></p>	

b6  
b7C

13. Justification statement necessitating emergency authorization:  
 Emergency 30 day authorization granted due to imminent need (within 48 hours) for use of consensual monitoring device(s), which precluded the handling of this request in the usual manner.  
 Other (Attach Additional Page to Specify)

1-Government Attorney's Office

Attn: \_\_\_\_\_

COPY 4

<b>Field Approval</b>	
14. CDC (If Sensitive Circumstances Exist) Signature _____	Date: _____
15. SAC Signature _____	Date: _____
<b>FBIHQ Approval</b>	
16. Unit Chief (If Sensitive Circumstances Exist) Signature _____	Date: _____

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/12/98

[redacted]  
employed at [redacted] provided witness  
accounts of hacking related activity at his business location.  
[redacted] can be contacted at his work, [redacted] Also  
present during this interview/meeting were [redacted]

b6  
b7C

[redacted] At the outset  
of the interview [redacted] was provided with a certified copy of  
United States District Court Order, For the Southern District of  
Ohio, Western Division, Number 98-235 E, filed 08/07/1998, signed  
by United States Magistrate Judge, Timothy S. Hogan, Cincinnati,  
Ohio.

[redacted] advised, that on [redacted] he was contacted by  
[redacted] in reference to a possible intruder (hacker) who  
appeared to have broken into one of [redacted] computer systems.

[redacted]

b6  
b7C  
b7E

[redacted] are located in the same building. The IP of the computer  
system in question is [redacted] and this IP address resolves to  
cartman.atcorp.org.

[redacted] advised [redacted] that while doing routine network  
duties he utilized [redacted]

[redacted]

Due to this unknown connection to their system, [redacted]  
started [redacted]

[redacted]

b6  
b7C  
b7E

[redacted] then attempted to contact AFCERT, CERT, WPAFB,  
and the FBI. [redacted] was only able to reach WPAFB and made  
contact with a [redacted] and a [redacted] at  
AFCERT.

*no hard copy  
see id list*

Investigation on 08/07/98 at North Charleston, SC

File # 288-CI-68562-6 Date dictated 08/12/98

b6  
b7C

by SA [redacted]



288-CI-68562

Continuation of FD-302 of [redacted], On 08/07/98, Page 2

[Large redacted area containing several smaller redacted boxes]

b6  
b7C  
b7E

[redacted] is assigned to [redacted]  
[redacted] AFRL/IFTA, Building 620, Room N3F22, 2241 Avionics  
Circle, Wright-Patterson AFB, OH 45433-7334, Phone: [redacted]  
[redacted] E-mail: [redacted]  
[redacted] explained [redacted] They share a working

b6  
b7C

288-CI-68562

Continuation of FD-302 of [redacted], On 08/07/98, Page 3

[redacted] relation in their professional dealings. [redacted] did not provide a broad background on what a [redacted] is or does.

b6  
b7C

[redacted] is assigned to [redacted]  
[redacted] ATI Corp., 7611 Barclay Ave., North Charleston, SC  
29418, Phone: [redacted] E-mail: [redacted]

[Large redacted area containing several small rectangular boxes]

b6  
b7C  
b7E

288-CI-68562

Continuation of FD-302 of , On 08/07/98, Page 4

b6  
b7C  
b7E

b3  
b6  
b7C

OTHER Sealed Court Documents

(01/26/1998)

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 07-05-2012 BY 60324/UC/baw/sab/aio

# FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 08/13/1998

To: Cincinnati

Attn: SA [redacted]

From: Columbia

Charleston Resident Agency

Contact: SA [redacted]

b6  
b7c

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: 288-CI-68562 (Pending)

Title: Unknown Subject;  
Wright-Patterson Air Force Base - Victim;  
CITA - THEFT

Synopsis: Lead to interview officials at South Carolina Research Authority (SCRA) [redacted]

Administrative: [redacted]

[redacted]

[redacted] The results of the interview of [redacted] are set forth in the enclosed FD-302. The items provided by [redacted] during the interview were furnished in duplicate. The originals of the items were received by the FBI and a receipt was provided to [redacted] for the items. The original items received and the receipt are also enclosed to this EC. The copy of the [redacted] OTHER Sealed Court Documents by [redacted] was made available to AFOSI.

b3  
b6  
b7c

Enclosures: Enclosed for CI is the original and two copies of an FD-302 [redacted]

[redacted] interview which was jointly conducted by the FBI and AFOSI.

Also enclosed for CI are the following:

1. A 1-A containing the original receipt provided to SCRA.

[redacted]

*no hard copy rec'd yet*

288-CI-68562-7

To: Cincinnati From: Columbia  
Re: 288-CI-68562, 08/13/1998

b3  
OTHER Seal Court Documents

[Redacted]

Details:

[Redacted]

b7E

. Columbia Division, Charleston RA, is taking no further action regarding this investigation, unless requested to do so by OO.

◆◆

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/05/1998

[redacted] white male, [redacted] College of Engineering, 628 Engineering Research Center, University of Cincinnati, Cincinnati, Ohio 45221, telephone number [redacted] [redacted] was advised of the identity of the interviewing Agent and the purpose of the interview.

[redacted] advised that he had the authority to monitor the activities of the computers located in the Engineering Research Center. [redacted] signed an FD-472, authorizing the Federal Bureau of Investigation to initiate the monitoring of these computers.

b6  
b7C

[redacted] provided a list of the Transmission Control Protocol/Internet Protocol (TCP/IP) addresses and fully qualified domain names for the computers in the Engineering Research Center. [redacted] also advised that all of these computers contained the appropriate banners.

Investigation on 07/31/1998 at Cincinnati, Ohio

File # 288-CI-68562 - R Date dictated 08/05/1998

by SA [redacted] mwd *[signature]*

b6  
b7C

*RDW/BB*

July 31, 1998  
(Date)

University of Cincinnati, Ohio  
(Location)

I,  of

University of Cincinnati, Cincinnati, Ohio, hereby  
(Address)

b6  
b7C

authorize Special Agents  and

, of the Federal Bureau of  
Investigation, United States Department of Justice, to:

install a recording device on any telephone utilized by me for the  
purpose of recording any telephone conversation(s) I may have with  
\_\_\_\_\_ and others as yet unknown  
(Name of Subject(s))  
on or about \_\_\_\_\_ and continuing thereafter.  
(Date)

I understand that I must be a party to any conversation in order to  
record that conversation. I therefore agree not to leave the recording  
equipment unattended or take any action which is likely to result in the  
recording of conversations to which I am not a party.

and/or to:

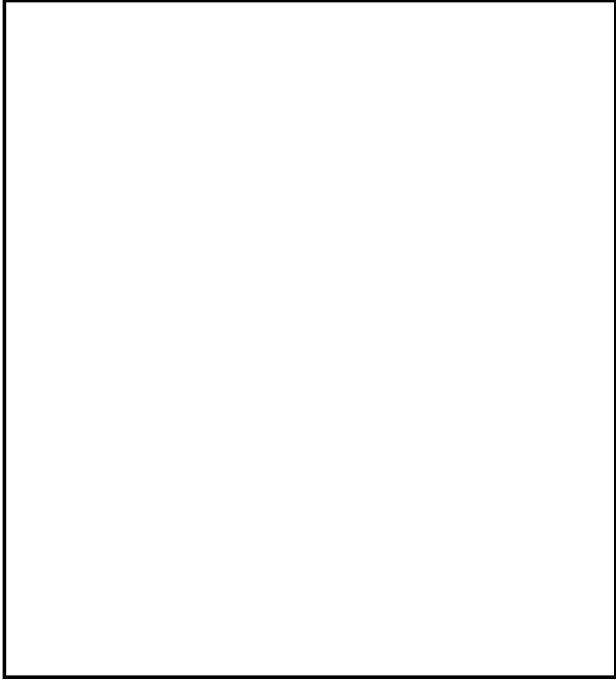
install a Trap and Trace device in conjunction with the  
appropriate provider(s) of electronic or wire communications  
service and/or long distance carrier for the purpose of  
identifying telephone numbers from which incoming calls are  
placed to telephone number \_\_\_\_\_  
located at \_\_\_\_\_  
which is used by me.

*Initiate the monitoring of the computers in the University of Cincinnati Engineering Department  
computer lab. I have the authority to monitor these computers.*  
I have given this written permission to the above-named Special Agents  
voluntarily, and without threats or promises of any kind.

(Signature)

b6  
b7C

Witness:



b6  
b7c

FAX TO (202) 324-0311  
FROM SA [redacted]  
Cincinnati, OH



(01/26/1998)

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 07-05-2012 BY 60324/UC/baw/sab/aio

~~SECRET~~

# FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY

Date: 08/23/1998

To: National Security

Attn: NIPC-CIIL Room 11887;  
SSA [redacted]

From: Cincinnati  
Squad 4

Contact: SA [redacted]

b6  
b7c

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: (U) ~~(S)~~ 288-CI-68562 (Pending)

Title: (U) ~~(S)~~ UNSUB(S);  
UNITED STATES AIR FORCE  
INSTITUTE OF TECHNOLOGY,  
HACKING ATTACK ON:  
[redacted]

b7E

Synopsis (U) ~~(S)~~ Summary update of captioned matter.

(U) ~~(S)~~ ~~Derived From: G-3~~  
~~Declassify On: X1~~

(U) ~~(S)~~ Details: What follows is a brief synopsis of actions  
accomplished as of 08/21/1998:

[redacted]

Referral/Consult

(U) ~~(S)~~ FBI Cincinnati obtains consent to monitor UC's  
College of Engineering and Computer Science subnet 129.137.41.x  
utilizing FBI Form FD-472 on July 31, 1998.

[redacted]

~~SECRET~~

288-CI-68562-9

Searched  
Serialized  
Indexed  
Filed

235 BBD1.EC

~~SECRET~~

To: National Security From: Cincinnati  
Re: ~~(U)~~~~(S)~~ 288-CI-68562, 08/23/1998

~~(U)~~

Referral/Consult

~~(U)~~~~(S)~~ On August 21, 1998, [redacted]  
[redacted] Engineering Research Facility (ERF), Quantico,  
Virginia, and [redacted] ERF,  
visited Cincinnati, Ohio, for the purpose of determining how to  
expand the network monitoring system at UC.

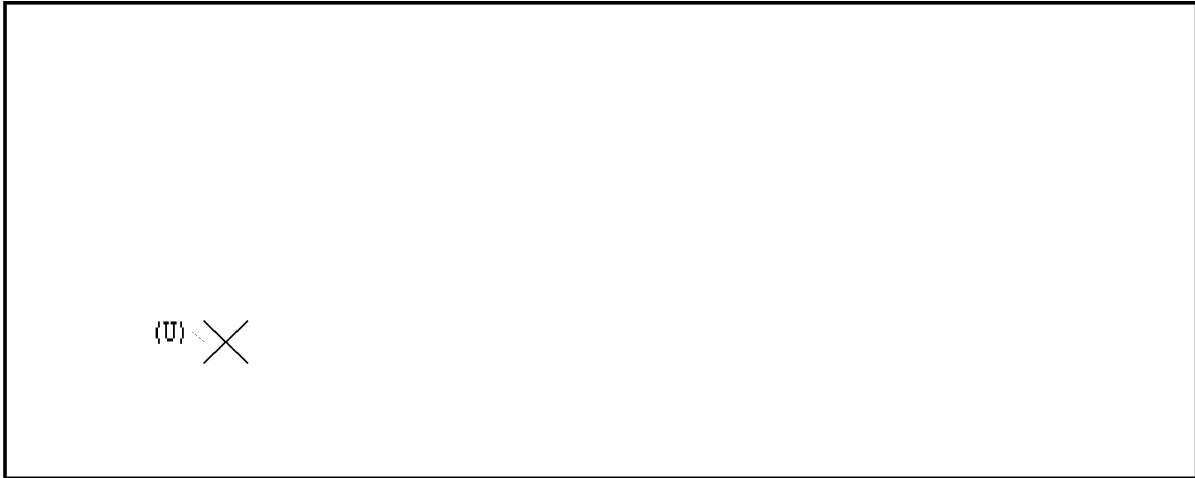
~~(U)~~~~(S)~~ Subsequent a meeting with UC staff to include  
systems engineers and administrators, the following issues were  
discussed:

~~(U)~~~~(S)~~ There are various end user systems identified as  
their own system administrators linked to the UC systems. If and

~~SECRET~~

~~SECRET~~

To: National Security From: Cincinnati  
Re: ~~(U)~~ ~~(S)~~ 288-CI-68562, 08/23/1998



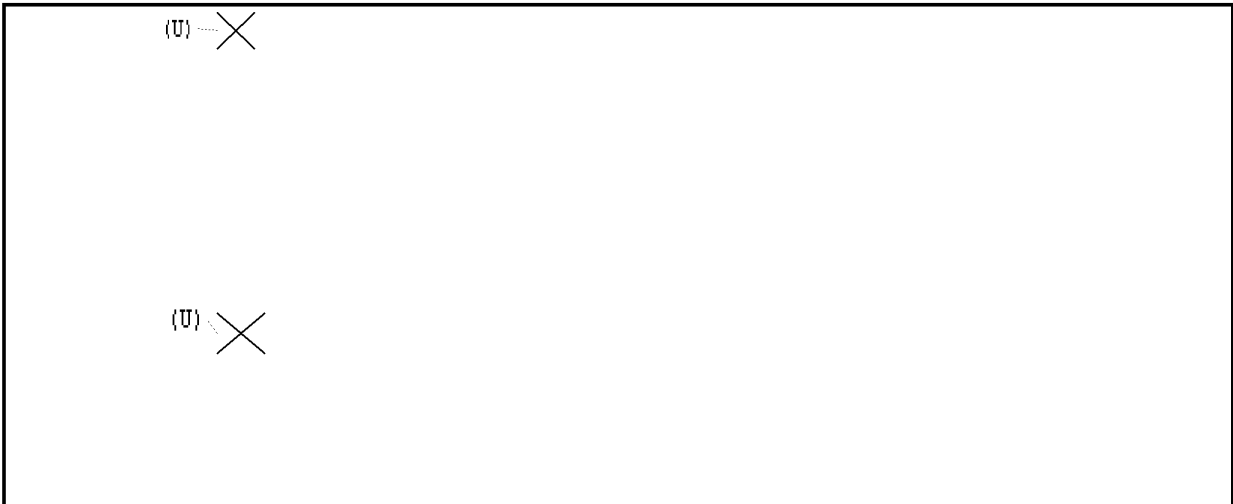
~~(U)~~

b7E

~~(U)~~ ~~(S)~~ [redacted] learned the following, UC's system network interface utilizes a 10 megabit Ethernet pipe out to the Internet.

b6  
b7C

~~(U)~~ ~~(S)~~ In order to monitor UC's College of Engineering and Computer Science subnet, two options exist:



~~(U)~~

~~(U)~~

b7E

~~(U)~~ ~~(S)~~ A mutual suggestion was discussed. Inasmuch that SCRA's network has been blocked from all possible angles from UC, WSU, Infinet and WPAFB, the consensus was that SCRA be dropped from further scrutiny due to limited resources and time constraints.

~~SECRET~~

~~SECRET~~

To: National Security From: Cincinnati  
Re: ~~(U)~~ ~~(S)~~ 288-CI-68562, 08/23/1998

~~(U)~~ ~~(S)~~ Cincinnati respectfully requests that FBIHQ coordinate with AFOSI HQ (DOD) to ameliorate legality issues presented on page three of this communication.

~~(U)~~ ~~(S)~~ Cincinnati Division expects to conduct witness/suspect/victim interviews during the latter part of August, 1998, and the first week of September, 1998.

~~(U)~~ ~~(S)~~ Investigation continuing at Cincinnati.

♦♦

~~SECRET~~

(01/26/1998)

DATE: 07-06-2012  
CLASSIFIED BY 60324/UC/baw/sab/aio  
REASON: 1.4 (c)  
DECLASSIFY ON: 07-06-2037

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED EXCEPT  
WHERE SHOWN OTHERWISE

~~SECRET~~

# FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 08/13/1998

To: Cincinnati

Attn: SA [redacted]

From: Cincinnati

Squad 4

Contact: SA [redacted]

b6  
b7C

Approved By: [redacted]

*DK* Drafted By: [redacted]

Case ID #: ~~(S)~~ [redacted] (Pending)

(U) ~~(S)~~ 288-CI-68567 (Pending)

b1  
b3

Title: (U) ~~(S)~~

UNSUB(S);  
United States Air Force  
Institute of Technology,  
Hacking Attack On:  
[redacted]

*1+2*  
*[handwritten mark]*

b7E

(S)

Synopsis: ~~(S)~~ [redacted]

(U) ~~(S)~~

~~Derived From: G-3~~  
~~Declassify On: X1~~

b1  
b3  
b7E

(U) [redacted]

Details: [redacted]

(S)

(S)

~~SECRET~~

*288-68567-10*

*288-CI-68562-10*  
*288-CI-68567*

SEARCHED <i>mm</i>	INDEXED <i>mm</i>
SERIALIZED <i>mm</i>	FILED <i>mm</i>
AUG 17 1998	
FBI - CINCINNATI	

*[Signature]*

~~SECRET~~

To: Cincinnati From: Cincinnati  
Re: ~~(S)~~ [redacted] 08/13/1998

b1  
b3

[Large redacted area]

~~(S)~~

[Redacted area]

~~(S)~~

(U) ~~(S)~~ [redacted] Lexis/Nexis, and LEADS confirmed portions of the above information and by separate insert added certain details.

b7E

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/31/98

[redacted]  
 [redacted]  
 [redacted] was furnished a copy of an Order (Case No. 98 244  
 E), signed by the Honorable [redacted] U.S. Magistrate  
 Judge Cincinnati, Ohio. [redacted]  
 [redacted]

b3  
b6  
b7C

During the late evening of 08/26/1998 and early morning hours of 08/27/1998, [redacted]

[redacted] a pen register and  
 trap and trace device [redacted]

[redacted]

b3  
b6  
b7C

Investigation on 08/26/1998 at Cincinnati, Ohio

File # 288-CI-68562 -13 Date dictated 08/31/1998

by SA [redacted]  
 SA [redacted]

b6  
b7C

(01/26/1998)

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 07-05-2012 BY 60324/UC/baw/sab/aio

~~SECRET~~

# FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY

Date: 09/04/1998

To: National Security  
Springfield

Attn: NIPC-CIU, Room 11887;  
SSA [redacted]  
Attn: Champaign RA

From: Cincinnati  
Squad 4

Contact: SA [redacted]

b6  
b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID # (U) ~~(S)~~ ✓ 288-CI-68562 - (Pending) 15

Title (U) ~~(S)~~ UNSUB(S);  
UNITED STATES AIR FORCE  
INSTITUTE OF TECHNOLOGY,  
HACKING ATTACK ON:  
[redacted]

b7E

Synopsis: (U) ~~(S)~~ Lead set for Springfield Division, Champaign RA,  
[redacted]

(U) ~~(S)~~ ~~Derived From: G-3~~  
~~Declassify On: X1~~

b3  
OTHER Sealed Court Document

Enclosures: (U) ~~(S)~~ Enclosed for Springfield Division, Champaign  
RA [redacted]

b6  
b7C

Details: (S) For information of Springfield Division, Champaign  
RA, Cincinnati Division, along with United States Air Force  
Office of Special Investigations (AFOSI), are jointly  
investigating intrusions into computers located at Wright-  
Patterson Air Force Base (WPAFB), Dayton, Ohio. The intrusions  
appear to be originating in Russia, hopping through University of  
Cincinnati, then terminating at WPAFB. The intruder has  
transferred several sensitive, though not classified files, to

~~SECRET~~

288-CI-68562-15

Searched \_\_\_\_\_  
Serialized \_\_\_\_\_  
Indexed \_\_\_\_\_  
Filed \_\_\_\_\_

24773301, EC



~~SECRET~~

To: National Security From: Cincinnati  
Re: (U) ~~(S)~~ 288-CI-68562, 09/04/1998

Referral/Consult

(U) ~~(S)~~ On 08/26/1998, the intruder was observed making connections to various other sites not previously seen, to include Eastern Illinois University (EIU). At approximately 0403 CDT, August 31, 1998, the intruder connected to ux1.cts.eiu.edu (139.67.8.3) via telnet, and subsequently via File Transfer Protocol (FTP). Cincinnati Division is desirous of obtaining the username which the intruder accessed into EIU's system.

(U) ~~(S)~~ Cincinnati Division appreciates assistance from the Springfield Division, Champaign RA.

~~SECRET~~

~~SECRET~~

To: National Security From: Cincinnati  
Re: (U) ~~(S)~~ 288-CI-68562, 09/04/1998

LEAD (s):

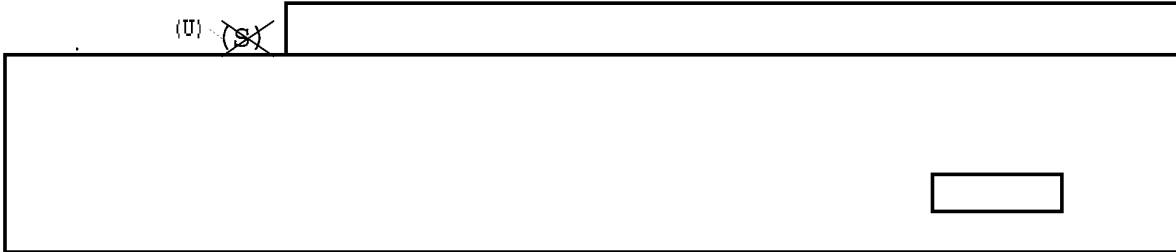
Set Lead 1:

SPRINGFIELD

AT CHARLESTON, IL

b3  
b6  
b7C  
OTHER Sealed Court Document

(U) ~~(S)~~



♦♦

~~SECRET~~

~~SECRET~~

09/08/98  
15:15:18

Lead Upload Report

ICMLPE11  
Page 1

Case ID: 288-CI-68562  
Serial: 15

---

Lead 1          Set to: SPRINGFIELD

---

Total leads set:            1  
Total leads not set:        0

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 09/19/98

[redacted] white Female DOB [redacted] SSAN [redacted]  
[redacted] POB [redacted] Visa# [redacted]  
[redacted] Telephone: [redacted]

was advised of the identity of the interviewing Agents and the purpose of the interview. [redacted] voluntarily furnished the following information:

[redacted] advised she came to Cincinnati under an F-1 visa from [redacted]. She chose to attend [redacted] because it was one of the few universities that accepted her. She obtained limited funds from [redacted] an entity from [redacted] that funds [redacted] students to study abroad. She is currently a Ph.D. candidate in [redacted].

b6  
b7C

Prior to arriving in the U.S., [redacted] was employed as a [redacted]. Her duties involved [redacted].

b6  
b7C

From [redacted] worked as [redacted] at the [redacted]. Her job entailed [redacted].

[redacted] attended and studied [redacted] at [redacted]. She obtained an M.S. degree in [redacted].

[redacted] advised she has no family and/or relatives residing with her [redacted]. She maintains telephonic and e-mail contact with family and friends [redacted].

b6  
b7C

[redacted] revealed she gave her computer password out to her boyfriend [redacted] so that he could e-mail messages to her. Her password at that time was [redacted]. She claims she changed her password after only two days because she knew it was wrong to give out her password. Her boyfriend is a [redacted]. She claims not to [redacted].

Investigation on 09/18/98 at Cincinnati, Ohio

File # 288-CI-68562-16 Date dictated 09/19/98

by SA [redacted]  
SA [redacted]

b6  
b7C

26165 01.302/

288-CI-68562

Continuation of FD-302 of [redacted], On 09/18/98, Page 2

know whether her boyfriend ever served with [redacted] and/or ever held a clearance.

[redacted] affirmed she visited her parents and friends in [redacted]. With respect to her long term goals, [redacted] expects to remain at [redacted] for another four to five years to pursue her Ph.D. [redacted] Upon graduation, she would like to work in the U.S. for about one year, provided she can find a host and obtain employment, before returning to [redacted] or some other European country.

b6  
b7C

[redacted] stated she has never maintained contact with any government officials either in the U.S. or overseas. She has never been tasked by a Foreign Intelligence Officer to operate either covertly or overtly in the U.S. [redacted] advised she would contact the writer if any unusual activity would ever take place concerning her studies [redacted] and her travels abroad [redacted]

b6  
b7C

[redacted] is currently a [redacted] wherein she receives a stipend to cover tuition and modest living expenses. Her research, though unclassified, involves [redacted]

[redacted]

[redacted] recalled that in [redacted] or so, she was informed by the systems administrator to change her password. She learned that someone unknown had used her password to hack into [redacted] network using her account. She changed her password and never heard back from the systems administrator.

b6  
b7C

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 09/14/98

[redacted] DOB [redacted] SSAN [redacted]  
[redacted] telephone:  
[redacted] was advised of the identity of the interviewing  
Agents and the purpose of the interview. [redacted] voluntarily  
furnished the following information:

b6  
b7C

[redacted] recollected that on or about May 15, 1998,  
he returned from a business trip to Japan. Upon returning to  
work, he was informed by two co-workers that his Picard account  
had been hacked into. He learned that the intrusion came from  
the University of Cincinnati (UC).

b6  
b7C

[redacted] revealed that his computer usage is minimal.  
He uses the computer for word processing and e-mail. He has two  
e-mail accounts; Picard for long distance e-mail and Teamlinks  
for e-mail within Wright Patterson Air Force Base (WPAFB).

[redacted] advised that as a result of the hacking  
incident, the computer network systems administrator issued  
everyone with a new password, based on name and telephone number.  
Despite this precaution, the account was again hacked. As  
recently as July, 1998, the systems administrator instructed  
every user to alter their passwords to make them more difficult  
to penetrate.

[redacted] relayed that his Picard e-mail contacts are  
extensive. He stated that in the last year he has received many  
messages from the U.S. and from numerous countries abroad to  
include: England, France, Germany, Finland, Russia, Chile,  
Japan, New Zealand and Australia. The e-mail message from Russia  
came from [redacted] a reputed well known scientist from

[redacted] He believes [redacted] is from  
[redacted] recalled that [redacted] has traveled to  
Dayton and/or Columbus, Ohio and San Francisco, California  
sometime in 1996. [redacted] annually makes numerous requests  
seeking joint venture projects with WPAFB researchers. WPAFB is  
precluded from accepting any joint venture projects with  
[redacted] according to [redacted] added that  
[redacted] has published numerous articles on titanium aluminite.

b6  
b7C

[redacted] recollected that he received one e-mail

Investigation on 09/11/98 at Dayton, Ohio

File # 288-CI-68562 -17 Date dictated 09/14/98

by SA [redacted] SA [redacted] (AFOSI)

b6  
b7C

254 66 01. 302

288-CI-68562

Continuation of FD-302 of [redacted], On 09/11/98, Page 2

message from a [redacted] who inquired about scientific research.

According to [redacted] his e-mail contacts with U.S. persons and individuals overseas are all researchers and scientists from sundry educational institutes. The e-mail messages concern scientific discussions relating to metallurgy. [redacted] asserted that none of his e-mail contacts appear to be out of the scope of his purview. [redacted] added that none of the e-mail messages requested secret or proprietary information.

b6  
b7c

[redacted] revealed he obtained his U.S. citizenship on [redacted]. He has a sister and cousins residing in England. He has worked in [redacted] in the past. As a physicist working in the aforementioned countries, he has never held a security clearance. He maintains no foreign government contacts.

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 09/14/98

[redacted] DOB [redacted] SSAN [redacted] telephone: [redacted] was advised of the identity of the interviewing Agents and the purpose of the interview. [redacted] voluntarily furnished the following information:

[redacted] recalled that approximately a few months ago she received a telephone call on a Monday from [redacted] (ATI-CORP), inquiring whether or not she was logged on to their system at 3:00 A.M. in the morning. [redacted] responded negatively and from that moment forward they realized that an unknown individual utilized her username and password to break into the SCRA/ATI-CORP computers and then into Wright Patterson Air Force Base (WPAFB), Dayton, Ohio.

b6  
b7C

[redacted] had an account at SCRA/ATI-Corp for about three years to transfer files and slides relating to the Rapid Prototyping of Application Specific Signal Processing (RASSP) program. She stated that she no longer holds this account since this incident occurred. The account was shut down. She claims that none of this information was classified or sensitive. Her job requires that she review material to ensure that it is cleared for public domain. The information was publicly released/releasable.

[redacted] advised she maintains accounts on elhp and Fleetwood at her office. She also has root password with her system administrator, [redacted] maintains a flyer net account and a sabre account at the University of Dayton (UD). She had an account at the Air Force Institute of Technology (AFIT) but believes it is no longer valid. [redacted] had a temporary account at the University of Cincinnati (UC) for a three day course she attended at UC [redacted] She held one other account at a company called RTI but believes it is no longer open.

b6  
b7C

[redacted] asserted that her ATI-Corp account was mainly used for education modules and to transfer files through FTP. She occasionally remote shelled to that account. [redacted] recalled that a week prior to this incident, she logged onto the ATI-Corp machine to FTP some files. She believes she logged on from elhp.

Investigation on 09/11/98 at Dayton, Ohio

File # 288-CI-68562-18 Date dictated 09/14/98

by SA [redacted] SA [redacted] (AFOSI)

b6  
b7C

25466 62.3021



288-CI-68562

Continuation of FD-302 of [REDACTED], On 09/11/98, Page 2

She FTP'd information from her PC on other occasions.

[REDACTED] affirmed that she has never given out any of her passwords with the exception of her root password on elhp which [REDACTED] has access to.

[REDACTED] revealed that her password [REDACTED] at ATI-Corp was a combination of upper and lower case letters and symbols which would have been difficult to decipher. [REDACTED] changed her password to [REDACTED] per the request of [REDACTED]

[REDACTED] added that "the subject probably could have gotten away with it if they wouldn't have logged in at 3:00 A.M. on a Sunday morning."

[REDACTED] was born in [REDACTED] the daughter of a [REDACTED]. She has one brother who resides in [REDACTED] with their mother. Her father is deceased. [REDACTED] arrived in the U.S. in [REDACTED] to finish high school in [REDACTED] where her brother previously resided. She returned to [REDACTED] to visit her parents and taught English grammar at [REDACTED] for three months during the summer.

[REDACTED] was previously married to an active duty U.S. military serviceman. She has been divorced for [REDACTED] years. She is a U.S. citizen through her previous marriage to a U.S. citizen. [REDACTED] occasionally travels overseas to visit her family [REDACTED]. Her last trip [REDACTED] was approximately [REDACTED] years ago. [REDACTED] affirmed she has never held a security clearance either in the U.S. or overseas. [REDACTED] maintains limited contact with friends and family overseas via e-mail.

b6  
b7Cb6  
b7C

(01/26/1998)

~~SECRET~~

# FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY

Date: 09/19/1998

To: National Security

Attn: NIPC-CIU, Room 11887;  
SSA [redacted]

From: Cincinnati  
Squad 4  
Contact: SA [redacted]

b6  
b7C

Approved By: [redacted]  
Drafted By: [redacted]

Case ID #: (U) ~~(S)~~ 288-CI-68562 (Pending)

Title: CHANGED  
(U) ~~(S)~~ MOONLIGHT MAZE

Synopsis (U) ~~(S)~~ Interviews conducted at Cincinnati Division.

(U) ~~(S)~~ ~~Derived From : G-3~~  
~~Declassify On: X1~~

Previous Title (U) ~~(S)~~ Title marked "Changed" to reflect new title as, "MOONLIGHT MAZE." Title previously carried as, "UNSUBS; UNITED STATES AIR FORCE INSTITUTE OF TECHNOLOGY, HACKING ATTACK ON: [redacted]

(A)  
b7E

Enclosures: (U) ~~(S)~~ Enclosed for FBIHQ are three separate copies of FD-302s of interviews conducted by the writer of [redacted] and one Air Force Form 1168 with attached statement of [redacted]

b6  
b7C

Details: (U) ~~(S)~~ For information of FBIHQ, FBI Cincinnati and United States Air Force, Office of Special Investigations (AFOSI), Wright-Patterson AFB, Dayton, Ohio, conducted four victim/witness interviews. The results of those interviews are enclosed as enclosures for NIPC-CIU, FBIHQ.

(U) ~~(S)~~ Cincinnati Division plans to re-interview [redacted] based on her nervous demeanor and her apparent, less than candid responses concerning her boyfriend who resides in [redacted] computer password at [redacted] will be closely monitored to [redacted]

b6  
b7C

~~SECRET~~

288-CI-68562-19

SEARCHED  
SERIALIZED  
INDEXED  
FILED

262BBO1.1C

for

~~SECRET~~

To: National Security From: Cincinnati  
Re: (U) ~~(S)~~ 288-CI-68562, 09/19/1998

determine whether a change in the subject(s) modus operandi (hacking tools and signature) is detected. A change in the subject(s) hacking activity could explain a nexus between the subject(s) and [redacted] considering her telephonic and e-mail contacts with her boyfriend [redacted] and her recent travels [redacted]

(U) ~~(S)~~ Based on the aforementioned, Cincinnati Division will re-interview the subject with additional probing questions concerning her contacts [redacted] and if deemed appropriate, will consider the use of a polygraph [redacted]

b6  
b7c

♦♦

~~SECRET~~

(01/26/1998)

~~SECRET~~

# FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY

Date: 09/28/1998

To: Cincinnati

Attn: SA [redacted]  
Squad 4

From: Springfield

Squad 3/Champaign RA

Contact: SA [redacted]

b6  
b7C

Approved By: [redacted]  
Drafted By: [redacted]

Case ID #: (U) ~~(S)~~ 288-CI-68562 (Pending) -20

Title: (U) ~~(S)~~ UNSUBS;  
UNITED STATES AIR FORCE  
INSTITUTE OF TECHNOLOGY;  
HACKING ATTACK ON: [redacted]

b7E

Synopsis: (U) ~~(S)~~ Lead set for Springfield at Charleston, Illinois has been covered.

~~(U) ~~(S)~~ Derived From: G-3  
Declassify On: X1~~

Reference: (U) ~~(S)~~ 288-CI-68562 Serial 15

Administrative: (U) ~~(S)~~ Re telcall between SA [redacted] and SSA [redacted] on 09/28/1998.

b6  
b7C

Enclosures: (U) ~~(S)~~ Enclosed for Cincinnati are two copies of computer activity logs.

Package copy: (U) ~~(S)~~ Being forwarded under a separate cover is one 8 mm Data cartridge.

Details: (U) ~~(S)~~ [redacted]

b3  
b6  
b7C

OTHER Sealed Court Documents [redacted]

~~SECRET~~

Lead covered 9/28/98.

288-CI-68562-20

SEARCHED	INDEXED
SERIALIZED	FILED
OCT 6 1998	
FBI - CINCINNATI	

*[Signature]*

b6  
b7C

SEP 27 1998

~~SECRET~~

To: Cincinnati From: Springfield \*  
Re: (U) ~~(S)~~ 288-CI-68562, 09/28/1998

directly. Per telcall between SA [redacted] and SSA [redacted]  
nothing will be sent directly to the National Security Division  
for evaluation. Springfield considers this lead covered.

◆◆

b6  
b7c

~~SECRET~~

(12/31/1995)

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 07-06-2012 BY 60324/UC/baw/sab/aio

# FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 08/24/1998

To: Cincinnati

Attn:

From: NSD

NIPC/CIOS/CIU/11719

Contact: SSA

b6  
b7C

Approved By:

Drafted By:

Case ID #: 288-CI-68562 (Pending)

Title: UNSUB(S);  
UNITED STATES AIR FORCE  
INSTITUTE OF TECHNOLOGY - VICTIM;  
CITA - COMPUTER INTRUSION;  
OO: CINCINNATI

Synopsis: This communication is to forward documents to the original case file.

Referral/Consult

Enclosure(s): Two copies of Request For Information letters sent to  One copy of response from NAVCIRT regarding possible material related to captioned matter.

Details: Enclosed for Cincinnati are copies of documents generated by or directed to the National Infrastructure Protection Center (NIPC) regarding captioned matter. These documents are being forwarded to Cincinnati for inclusion in the original case file.

◆◆

*288-CI-68562-21*

SEARCHED	INDEXED
SERIALIZED	FILED
AUG 25 1998	
FBI - CINCINNATI	

*[Signature]*

b6  
b7C



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

August 4, 1998

[Redacted]

Dear [Redacted]

Referral/Consult

This letter is to request information from [Redacted] databases and published reports that may be relevant to an ongoing FBI criminal investigation. The investigation centers on a series of intrusions into computer systems located at Wright Patterson Air Force Base. The intrusions appear to originate from a series of Internet service providers located in the Russian Federation. It also appears that the intruder is connecting to the ISPs through a "dial-up" connection, which suggests a local (i.e. Russian) point of origin. The FBI currently possesses no information indicating that the attacker is a U.S. person.

Technical information relevant to this request is provided in the enclosure, which also specifies an operational point of contact in the FBI. As additional technical information becomes available, it will be forwarded to the operational point of contact at [Redacted]

The FBI legal contact point for this matter is Assistant General Counsel [Redacted]  
[Redacted] Please do not hesitate to call him if you require additional information.  
Thank you for your assistance in this matter.

Sincerely,

[Redacted Signature]

Associate General Counsel for National  
Security Affairs

b6  
b7c

cc:

[Redacted]  
[Redacted] OGC/NIPC

The Wright Patterson Air Force Base (WPAFB), a key educational and research and development base, has documented numerous intrusions into approximately eight of their systems. The attacks primarily come through computers located in the computer lab at the University of Cincinnati. However, attacks have been seen from Wright University, located in Dayton, OH and Aticorp.net located in Charleston, SC. The intrusions into these U.S. systems appears to be originating from a dialup connection to four Internet Service Providers (ISPs) located in Russia. The hacking occurs Monday through Friday, midnight and approximately 9:00 a.m. EDT.

The following are the [redacted] involved:

[redacted]

b7E

The following passwords or environment variables have been used during the intrusions:

[redacted]

b6  
b7C

The following are usernames, software authors or tool names:

[redacted] is the name of [redacted] student whose account is being used at [redacted] Our information indicates she is a non-U.S. person.)  
[redacted]

The following files are known to have been taken by the hacker from WPAFB:

[redacted]

b7E

NIPC Operational POC is SSA [redacted]

b6  
b7C



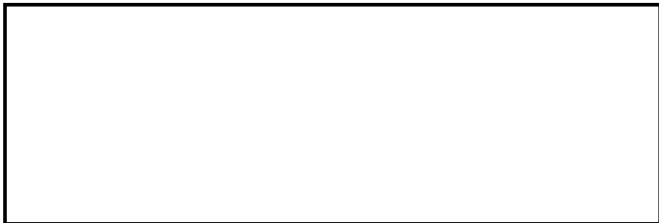


U.S. Department of Justice

Federal Bureau of Investigation


Washington, D. C. 20535-0001

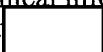
August 3, 1998

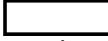



Referral/Consult

Dear 

This letter is to request information from  databases and published reports that may be relevant to an ongoing FBI criminal investigation. The investigation centers on a series of intrusions into computer systems located at Wright Patterson Air Force Base. The intrusions appear to originate from a series of Internet service providers located in the Russian Federation. It also appears that the intruder is connecting to the ISPs through a "dial-up" connection, which suggests a local (i.e. Russian) point of origin. The FBI currently possesses no information indicating that the attacker is a U.S. person.

Technical information relevant to this request is provided in the enclosure, which also specifies an operational point of contact in the FBI. As additional technical information becomes available, it will be forwarded to the operational point of contact at .

The FBI legal contact point for this matter is Assistant General Counsel   
 Please do not hesitate to call him if you require additional information.  
Thank you for your assistance in this matter.

Sincerely,



Associate General Counsel for National  
Security Affairs

b6  
b7c

cc:



OGC/NIPC  
NSA

~~SECRET~~



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

August 31, 1998



Dear [redacted]

Referral/Consult

(U) This letter is to request [redacted] technical assistance in conjunction with an ongoing FBI criminal investigation. The investigation centers on a series of intrusions into computer systems located at Wright Patterson Air Force Base. The intrusions appear to originate from a series of Internet service providers located in the Russian Federation. It also appears that the intruder is connecting to the ISPs through a "dial-up" connection, which suggests a local (i.e. Russian) point of origin. The FBI currently possesses no information indicating that the attacker is a U.S. person. (S)

(U) The FBI has already made (in an August 21, 1998, letter addressed to Acting General Counsel [redacted] a standard Request for Information in connection with this [redacted] investigation. The purpose of this letter is to add a technical assistance request so that [redacted] expert personnel can assist the FBI investigators on certain technical questions relating to computer data collected by the FBI. (S)

b6  
b7C

The FBI legal contact point for this matter is Assistant General Counsel [redacted]. Please do not hesitate to call him if you require additional information. Thank you for your assistance in this matter. (U)

Sincerely,



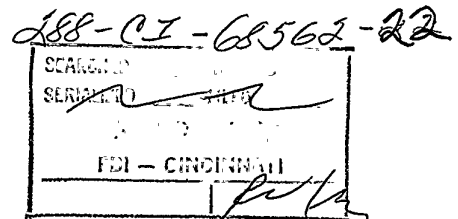
b6  
b7C

Associate General Counsel for National Security Affairs

cc: [redacted]

Referral/Consult

~~Derived From: Multiple Sources  
Declassify on: X1~~



~~SECRET~~



# FBI FACSIMILE COVER SHEET

### PRECEDENCE

- Immediate
- Priority
- Routine

### CLASSIFICATION

- Top Secret
- Secret
- Confidential
- Sensitive
- Unclassified

Time Transmitted: 3:53 p.m. MJW  
 Sender's Initials: MJW  
 Number of Pages: 2  
 (including cover sheet)

To: NSA/OGC  
 Name of Office

Date: 08/31/1998

Facsimile Number: 301-688-6017

Attn:   
 Name Room Telephone

b6  
b7c

From: NIPC  
 Name of Office

Subject: Technical Assistance Request

Special Handling Instructions: \_\_\_\_\_

Originator's Name:  Telephone:

b6  
b7c

Originator's Facsimile Number: 202-324-0311

Approved: MJW

Brief Description of Communication Faxed: See Attached

### WARNING

Information attached to the cover sheet is U.S. Government Property. If you are not the intended recipient of this information, disclosure, reproduction, distribution, or use of this information is prohibited (18.U.S.C. § 641). Please notify the originator or the local FBI Office immediately to arrange for proper disposition.



# FBI FACSIMILE COVER SHEET

### PRECEDENCE

- Immediate
- Priority
- Routine

### CLASSIFICATION

- Top Secret
- Secret
- Confidential
- Sensitive
- Unclassified

Time Transmitted: 3:58 pm.  
 Sender's Initials: MJW  
 Number of Pages: 2  
 (including cover sheet)

To: NSA/ \_\_\_\_\_  
 Name of Office

Date: 08/31/1998

Facsimile Number: 410-859-4888

Attn: 

--	--	--

  
 Name Room Telephone

b6  
b7c

From: NIPC \_\_\_\_\_  
 Name of Office

Subject: Technical Assistance Request

Special Handling Instructions: \_\_\_\_\_

Originator's Name: 



 Telephone:

b6  
b7c

Originator's Facsimile Number: 202-324-0311

Approved: MJW

Brief Description of Communication Faxed: See Attached

### WARNING

Information attached to the cover sheet is U.S. Government Property. If you are not the intended recipient of this information, disclosure, reproduction, distribution, or use of this information is prohibited (18.U.S.C. § 641). Please notify the originator or the local FBI Office immediately to arrange for proper disposition.

U.S. Department of Justice

Federal Bureau of Investigation



In Reply, Please Refer to  
File No.

550 Main Street, Room 9000  
Cincinnati, Ohio 45202  
September 21, 1998

SA [redacted]  
USAF Office of Special Investigations  
AFOSI Detachment 101  
4165 Communications Boulevard, Suite 3  
Wright-Patterson Air Force Base, Ohio 45433

b6  
b7c

To Whom It May Concern:

Upon expiration of AFOSI's Form 52 (Consensual Monitoring) at Wright State University (WSU), FBI Cincinnati will continue monitoring computers at WSU utilizing AFOSI monitoring equipment. Consensual monitoring will be in effect as of the date of this communication to the conclusion of this matter, pursuant to FBI Form FD-759, Notification of SAC authority granted for use of consensual monitoring equipment.

Sincerely yours,

Sheri A. Farrar  
Special Agent in Charge

By: [redacted]  
Supervisory Special Agent

b6  
b7c

- 1 - Addressee
- 1 - Cincinnati (288-CI-68562)

BB:jaw (2)

288-CI-68562-23

Searched \_\_\_\_\_  
Serialized \_\_\_\_\_  
Indexed \_\_\_\_\_  
Filed \_\_\_\_\_

264JAW01.OTH

U.S. Department of Justice



Federal Bureau of Investigation

In Reply, Please Refer to  
File No. 288-CI-68562

550 Main Street, Room 9000  
Cincinnati, Ohio 45202  
October 6, 1998

DCFL  
500 Duncan Avenue, Room 1009  
Bolling AFB, DC 20332-6000

SUBJECT: Request for Computer Forensic Media Analysis

1. **COMPLETE SUBJECT TITLE BLOCK INFORMATION:** Wright-Patterson AFB, Ohio, June 1, 1998, Unauthorized access of governmental and civilian computer systems. Violation of Title 18, USC, Section 1030; Fraud and Related Activity in Connection with Computers.

2. **PRIORITY:** This is a Category 1 intrusion on several military systems. This joint investigation is considered one of the highest priority cases within the FBI and AFOSI realms. The analysis of the enclosed tapes is requested immediately by the Department of Justice, Department of Defense, the Federal Bureau of Investigation and AFOSI.

3. **CLASSIFICATION:** This investigation is classified, however the evidence is not.

4. **CO-CASE AGENTS:** SA [redacted] FBI, Cincinnati, Ohio, commercial [redacted] SA [redacted] AFOSI Det 101, WPAFB, Ohio, DSN [redacted] commercial: [redacted] [redacted] AFOSI Det 101 WPAFB, Ohio, DSN [redacted] commercial: [redacted]

b6  
b7C

5. **SYNOPSIS OF THE CASE:** On or about June 1, 1998, WPAFB began detecting intrusions at several Air Force Institute of Technology and Air Force Research Laboratory machines. [redacted]

b7E

[redacted] The intrusions originally were detected coming through the University of Cincinnati; however, additional intrusions have been detected at several education sites and numerous Internet Service Providers. The unidentified intruder uses authorized accounts and valid passwords to gain access into the victim systems and then FTP's files, telnets to another system or pop roots. To date, investigative agencies have not been able to detect any sniffer, rootkit or trojanized programming.

1 - Addressee  
① - Cincinnati (288-CI-68562)  
BB:bb (2)

288-CI-68562-26  
Searched  
Serialized  
Indexed  
Filed

280BB01,OTH

**6. ITEMS TO BE ANALYZED:**

1. One 3GB Hard Drive, Western Digital Caviar 33100 (University of Wisconsin). **Remarks:** AFOSI Form 96 will be e-mailed to DCFL. The OS and other pertinent information will be on 96.

2. One 4mm Digital Data Storage cartridge, 120M, labeled NVTST/OX, (Wright State University). **Remarks:** Ditto as above.

3. Two 8mm Helical-Scan, HS-8/112 Maxell Data Cartridges [redacted]

b7E

**SUPPORT REQUESTED:**

Extract all system logs, text, document, etc.

Examine file system for modification to operating system software or configuration.

Examine file system for back doors, check for setuid and setgid files.

Examine file system for any sign of a sniffer program.

Extract data from this 4mm/8mm tape and convert to readable format - cut to CD.

Backup hard drives and place backup on a CD, tape or other format.

Analyze for deleted files and restore deleted files, cut findings to CD.

Extract all pertinent text files of a sexual nature.

Extract all trojanized programs or scripts/code programs, cut to CD.

Provide an analysis report and cut all findings to CD.

**7. PERTINENT DATA:** Coordinate with SA [redacted] and HQ AFOSI/XOII with pertinent data.

b6  
b7C

**8. AUTHORITY:** OSI Form 96 will be sent electronically.

**9. OTHER DOCUMENTS:** The ACISS report is the same as the one sent on the August 26, 1998 request.

**10. INSTRUCTIONS:** Please make five copies and send all copies of the analysis report to HQ AFOSI/XOII. HQ AFOSI/XOII will distribute the analysis accordingly. Please return all evidence to FBI Cincinnati.

11. POC: SA [redacted] AFOST Detachment 101 at DSN:  
[redacted] or commercial: [redacted]

Sincerely yours,

Sheri A. Farrar  
Special Agent in Charge

b6  
b7c

By: [redacted]  
Supervisory Special Agent



FEDERAL BUREAU OF INVESTIGATION

Date of transcription 10/26/98

[redacted] Date of Birth (DOB) [redacted] Social Security Account Number (SSAN) [redacted] was advised of the identities of the interviewing Agents and the purpose of the interview. [redacted] voluntarily furnished the following information:

[redacted] identified her boyfriend as [redacted] a white male, DOB [redacted] resides in [redacted]. He is a [redacted] who works at a factory [redacted] which utilizes a turbo prop to pump and maintain oil for commercial purposes. [redacted] was unable to identify the factory location and was unable to comment whether the factory has any ties to the [redacted]. She recalled that [redacted] has worked there since late [redacted]. [redacted] recently informed [redacted] that he is in search of a new job.

b6  
b7C

[redacted] advised her most recent contact with [redacted] was approximately [redacted] ago via e-mail. [redacted] most recently visited [redacted]. She stayed with her family for [redacted] while visiting friends and family.

Prior to enrolling at [redacted] [redacted] obtained financial assistance from [redacted] a foundation that provides funds for European students to study abroad. [redacted] logged onto [redacted] web site and learned from an advisor the type of research that is conducted at that department. [redacted] liked what [redacted] program had to offer, and as a result, she matriculated at [redacted]. [redacted] is a Ph.D. candidate matriculated in the aforementioned program [redacted].

b6  
b7C

[redacted] advised her research at [redacted] involves [redacted]. In laymen terms, [redacted] utilizes [redacted].

According to [redacted] mixed signal design can be used for any and all applications to include military application. [redacted] advised her research at [redacted] is strictly

Investigation on 10/16/98 at Cincinnati, Ohio

File # 288-CI-68562-2A Date dictated 10/29/98

by SA [redacted] [redacted]

b6  
b7C

288-CI-68562

Continuation of FD-302 of [REDACTED]

, On 10/16/98, Page 2

theoretical research. She does not know who the end user is, of the research she conducts [REDACTED] Her [REDACTED]

[REDACTED] recalled that during her visit at the U.S. Embassy [REDACTED] she was interviewed by an embassy employee concerning her request for an exit visa to study abroad. The employee spoke Romanian and English. He asked [REDACTED] the following questions:

1. Who is funding your trip?
2. How long will you be in the U.S.?
3. Why are you traveling to the U.S.?
4. When will you return?
5. Do you have any family in the U.S.?
6. Will you be working in the U.S.?

[REDACTED] asserted the interview lasted approximately fifteen minutes. The interviewer was male and was dressed in a suit and tie. The interview was conducted within the confines of the general office space where there was no expectation of privacy. [REDACTED] affirmed that at no time was she asked, promised, and/or influenced to cooperate with embassy officials and/or other government employees.

[REDACTED] stated that she maintains weekly e-mail correspondence with her boyfriend, [REDACTED] and other friends and family [REDACTED]. Her contacts at [REDACTED] are very limited. She advised that [REDACTED] has a very small [REDACTED] group that meets approximately once a month for social functions. [REDACTED] added that she would contact the FBI in the event she feels threatened and/or is confronted by any unusual person(s).

[REDACTED] advised she would not object to a polygraph if requested to do so.

b6  
b7Cb6  
b7C

U.S. Department of Justice



Federal Bureau of Investigation

In Reply, Please Refer to  
File No.

550 Main Street, Room 9000  
Cincinnati, Ohio 45202  
November 3, 1998

[Redacted]

Furman University  
3300 Poinsett Hwy.  
Greenville, SC 29613

RE: Notice to Preserve Evidence Under  
Title 18, U.S.C., 2703(f)

Dear [Redacted]

This letter is to follow up our telephone conversation on November 2, 1998. As I stated at that time, I am a Special Agent for the Federal Bureau of Investigation (FBI), a duly authorized federal law enforcement officer empowered to investigate unauthorized access into private, state, local and federal computer systems. As previously discussed, during the following dates: September 22 and 24, 1998, an unknown individual illegally entered a state owned academic institutional computer system at sumac.occ.uc.edu, [Redacted]. According to our investigation, this communication originated or passed through your system, furman.edu, [Redacted].

b6  
b7C

(X)  
L.S.H.

b7E

This letter serves to inform you that I will be pursuing the issuance of a subpoena and/or court order under Title 18, U.S.C., 2703(d), respectively, to trace the unknown individual back from your system. Inasmuch that this process can be time consuming, I have requested, pursuant to Title 18, U.S.C., 2703(f), that you take appropriate measures to preserve transactional logs, contents of any relevant communications, back-up files, and any other evidence that pertains to the aforementioned connections.

For ease of reference, Title 18, U.S.C., 2703(f), provides:

(f) Requirement to preserve evidence.

(1) In general.- A provider of a wire or electronic communication service or a remote computing service, upon the request of a government entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

- 1 - Addressee
- (1) - CI (288-68562) BB:bb (2)

307B301.0TH

288-68562-29  
Searched  
Serialized  
Indexed  
Filed

For

(2) **Period of retention.**- Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90 day period upon a renewal request by the governmental entity.

Finally, although you have been most cooperative, we have in other situations, experienced some informational leaks. While such leaks may represent misplaced good intentions, they can have serious impact upon our investigation. Accordingly, we would respectfully request that your personnel be placed on notice that they are subject to criminal liability should they disclose any privileged information. The governing statute in this regard is Title 18, U.S.C., 2232(b), which provides:

**(b) Notice of Search.**- Whoever, having knowledge that any person authorized to make searches and seizures has been authorized or is otherwise likely to make a search or seizure, in order to prevent the authorized seizing or securing of any person, goods, wares, merchandise, or other property, gives notice or attempts to give notice of the possible search and seizure to any person, shall be fined under this title or imprisoned not more than five years, or both.

Again, I greatly appreciate your cooperation in this matter with our agency. If you have any questions or comments, please feel free to call SA [redacted] at [redacted]

Sincerely yours,

Sheri A. Farrar  
Special Agent in Charge

b6  
b7c

By: [redacted]  
Supervisory Special Agent

U.S. Department of Justice



Federal Bureau of Investigation

In Reply, Please Refer to  
File No.

550 Main Street, Room 9000  
Cincinnati, Ohio 45202  
November 3, 1998

[Redacted]  
University of Pittsburgh  
600 Epsilon Drive  
Pittsburgh, PA 15238

RE: Notice to Preserve Evidence Under  
Title 18, U.S.C., 2703(f)

b6  
b7C

Dear [Redacted]

This letter is to follow up our telephone conversation on November 2, 1998. As I stated at that time, I am a Special Agent for the Federal Bureau of Investigation (FBI), a duly authorized federal law enforcement officer empowered to investigate unauthorized access into private, state, local and federal computer systems. As previously discussed, during the following date(s): September 18, 1998, an unknown individual illegally entered a state owned academic institutional computer system at sumac.occ.uc.edu, [Redacted]. According to our investigation, this communication originated or passed through your system, unixs2.cis.pitt.edu, [Redacted].

(X)  
2/1/98  
b7E

This letter serves to inform you that I will be pursuing the issuance of a subpoena and/or court order under Title 18, U.S.C., 2703(d), respectively, to trace the unknown individual back from your system. Inasmuch that this process can be time consuming, I have requested, pursuant to Title 18, U.S.C., 2703(f), that you take appropriate measures to preserve transactional logs, contents of any relevant communications, back-up files, and any other evidence that pertains to the aforementioned connections.

For ease of reference, Title 18, U.S.C., 2703(f), provides:

(f) Requirement to preserve evidence.

(1) In general.- A provider of a wire or electronic communication service or a remote computing service, upon the request of a government entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

- 1 - Addressee
- ① - CI (288-CI-68562) BB:bb (2)

3075B02.0TH/

288-CI-68562-30  
Searched \_\_\_\_\_  
Serialized \_\_\_\_\_  
Indexed \_\_\_\_\_  
Filed \_\_\_\_\_

(2) **Period of retention.**- Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90 day period upon a renewal request by the governmental entity.

Finally, although you have been most cooperative, we have in other situations, experienced some informational leaks. While such leaks may represent misplaced good intentions, they can have serious impact upon our investigation. Accordingly, we would respectfully request that your personnel be placed on notice that they are subject to criminal liability should they disclose any privileged information. The governing statute in this regard is Title 18, U.S.C., 2232(b), which provides:

(b) **Notice of Search.**- Whoever, having knowledge that any person authorized to make searches and seizures has been authorized or is otherwise likely to make a search or seizure, in order to prevent the authorized seizing or securing of any person, goods, wares, merchandise, or other property, gives notice or attempts to give notice of the possible search and seizure to any person, shall be fined under this title or imprisoned not more than five years, or both.

Again, I greatly appreciate your cooperation in this matter with our agency. If you have any questions or comments, please feel free to call SA [redacted] at [redacted]

Sincerely yours,

Sheri A. Farrar  
Special Agent in Charge

b6  
b7c

By: [redacted]

Supervisory Special Agent

U.S. Department of Justice



Federal Bureau of Investigation

In Reply, Please Refer to  
File No.

550 Main Street, Room 9000  
Cincinnati, Ohio 45202  
November 3, 1998

[Redacted]

Harvard University  
Network Services Division  
Office for Information Technology  
~~10 Ware Street~~ Oxford St.  
Cambridge, MA 02138

RE: Notice to Preserve Evidence Under  
Title 18, U.S.C., 2703(f)

Dear [Redacted]

This letter is to follow up our telephone conversation on October 30, 1998. As I stated at that time, I am a Special Agent for the Federal Bureau of Investigation (FBI), a duly authorized federal law enforcement officer empowered to investigate unauthorized access into private, state, local and federal computer systems. As previously discussed, during the following dates: September 22 and 24, 1998, an unknown individual illegally entered a state owned academic institutional computer system at sumac.occ.uc.edu, [Redacted]. According to our investigation, this communication originated or passed through your system, jsbach.harvard.edu, [Redacted].

b6  
b7C

(V)  
[Handwritten mark]

b7E

This letter serves to inform you that I will be pursuing the issuance of a subpoena and/or court order under Title 18, U.S.C., 2703(d), respectively, to trace the unknown individual back from your system. Inasmuch that this process can be time consuming, I have requested, pursuant to Title 18, U.S.C., 2703(f), that you take appropriate measures to preserve transactional logs, contents of any relevant communications, back-up files, and any other evidence that pertains to the aforementioned connections.

For ease of reference, Title 18, U.S.C., 2703(f), provides:

288-CI-68562-31

(f) Requirement to preserve evidence.

Searched \_\_\_\_\_  
Serialized \_\_\_\_\_  
Indexed \_\_\_\_\_  
Filed \_\_\_\_\_

(1) In general.- A provider of a wire or electronic communication service or a remote computing service,

- 1 - Addressee
- (1) - CI (288-CI-68562) BB:bb (2)

307 bb 03.04h

[Handwritten signature]

upon the request of a government entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

**(2) Period of retention.-** Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90 day period upon a renewal request by the governmental entity.

Finally, although you have been most cooperative, we have in other situations, experienced some informational leaks. While such leaks may represent misplaced good intentions, they can have serious impact upon our investigation. Accordingly, we would respectfully request that your personnel be placed on notice that they are subject to criminal liability should they disclose any privileged information. The governing statute in this regard is Title 18, U.S.C., 2332(b), which provides:

**(b) Notice of Search.-** Whoever, having knowledge that any person authorized to make searches and seizures has been authorized or is otherwise likely to make a search or seizure, in order to prevent the authorized seizing or securing of any person, goods, wares, merchandise, or other property, gives notice or attempts to give notice of the possible search and seizure to any person, shall be fined under this title or imprisoned not more than five years, or both.

Again, I greatly appreciate your cooperation in this matter with our agency. If you have any questions or comments, please feel free to call SA [redacted] at [redacted]

Sincerely yours,

Sheri A. Farrar  
Special Agent in Charge

b6  
b7c

By: [redacted]  
Supervisory Special Agent



U.S. Department of Justice



Federal Bureau of Investigation

In Reply, Please Refer to  
File No.

550 Main Street, Room 9000  
Cincinnati, Ohio 45202  
November 3, 1998

[Redacted]

Bryn Mawr College  
101 North Merion Ave.  
Bryn Mawr, PA 19010-2899

RE: Notice to Preserve Evidence Under  
Title 18, U.S.C., 2703(f)

Dear [Redacted]

This letter is to follow up our telephone conversation on October 30, 1998. As I stated at that time, I am a Special Agent for the Federal Bureau of Investigation (FBI), a duly authorized federal law enforcement officer empowered to investigate unauthorized access into private, state, local and federal computer systems. As previously discussed, during the following date(s): September 23, 1998, an unknown individual illegally entered a state owned academic institutional computer system at sumac.occ.uc.edu, [Redacted] According to our investigation, this communication originated or passed through your system, serendip.brynmawr.edu, [Redacted]

b6  
b7C

(K)  
12/1/98

b7E

This letter serves to inform you that I will be pursuing the issuance of a subpoena and/or court order under Title 18, U.S.C., 2703(d), respectively, to trace the unknown individual back from your system. Inasmuch that this process can be time consuming, I have requested, pursuant to Title 18, U.S.C., 2703(f), that you take appropriate measures to preserve transactional logs, contents of any relevant communications, back-up files, and any other evidence that pertains to the aforementioned connections.

For ease of reference, Title 18, U.S.C., 2703(f) provides:

CI-68562-92  
Searched \_\_\_\_\_  
Serialized \_\_\_\_\_  
Indexed \_\_\_\_\_  
Filed \_\_\_\_\_

(f) Requirement to preserve evidence.

(1) In general.- A provider of a wire or electronic communication service or a remote computing service, upon the request of a government entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

- 1 - Addressee
- ① - CI (288-CI-68562) BB:bb (2)

3075204.01h

*[Handwritten signature]*

(2) **Period of retention.**- Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90 day period upon a renewal request by the governmental entity.

Finally, although you have been most cooperative, we have in other situations, experienced some informational leaks. While such leaks may represent misplaced good intentions, they can have serious impact upon our investigation. Accordingly, we would respectfully request that your personnel be placed on notice that they are subject to criminal liability should they disclose any privileged information. The governing statute in this regard is Title 18, U.S.C., 2232(b), which provides:

**(b) Notice of Search.**- Whoever, having knowledge that any person authorized to make searches and seizures has been authorized or is otherwise likely to make a search or seizure, in order to prevent the authorized seizing or securing of any person, goods, wares, merchandise, or other property, gives notice or attempts to give notice of the possible search and seizure to any person, shall be fined under this title or imprisoned not more than five years, or both.

Again, I greatly appreciate your cooperation in this matter with our agency. If you have any questions or comments, please feel free to call SA [redacted] at [redacted]

Sincerely yours,

Sheri A. Farrar  
Special Agent in Charge

b6  
b7c

By: [redacted]

Supervisory Special Agent

U.S. Department of Justice



Federal Bureau of Investigation

In Reply, Please Refer to  
File No.

550 Main Street, Room 9000  
Cincinnati, Ohio 45202  
November 3, 1998

[Redacted]

Florida Institute of Technology (FIT-DOM)  
150 West University Blvd.  
Melbourne, FL 32901

RE: Notice to Preserve Evidence Under  
Title 18, U.S.C., 2703(f)

Dear [Redacted]

This letter is to follow up our telephone conversation on October 30, 1998. As I stated at that time, I am a Special Agent for the Federal Bureau of Investigation (FBI), a duly authorized federal law enforcement officer empowered to investigate unauthorized access into private, state, local and federal computer systems. As previously discussed, during the following date(s): September 22, 1998, an unknown individual illegally entered a state owned academic institutional computer system at sumac.occ.uc.edu, [Redacted]. According to our investigation, this communication originated or passed through your system, sunmlb.new.fit.edu, [Redacted].

b6  
b7C

(X)  
2/4

b7E

This letter serves to inform you that I will be pursuing the issuance of a subpoena and/or court order under Title 18, U.S.C., 2703(d), respectively, to trace the unknown individual back from your system. Inasmuch that this process can be time consuming, I have requested, pursuant to Title 18, U.S.C., 2703(f), that you take appropriate measures to preserve transactional logs, contents of any relevant communications, back-up files, and any other evidence that pertains to the aforementioned connections.

288-CI-68562-33

For ease of reference, Title 18, U.S.C., 2703(f), provides:

Searched \_\_\_\_\_  
Serialized \_\_\_\_\_  
Indexed \_\_\_\_\_  
Filed \_\_\_\_\_

(f) Requirement to preserve evidence.

(1) In general.- A provider of a wire or electronic communication service or a remote computing service, upon the request of a government entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

- 1 - Addressee
- 1 - CI (288-CI-68562) BB:bb (2)

30755 05.04h/

For

(2) **Period of retention.**- Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90 day period upon a renewal request by the governmental entity.

Finally, although you have been most cooperative, we have in other situations, experienced some informational leaks. While such leaks may represent misplaced good intentions, they can have serious impact upon our investigation. Accordingly, we would respectfully request that your personnel be placed on notice that they are subject to criminal liability should they disclose any privileged information. The governing statute in this regard is Title 18, U.S.C., 2232(b), which provides:

(b) **Notice of Search.**- Whoever, having knowledge that any person authorized to make searches and seizures has been authorized or is otherwise likely to make a search or seizure, in order to prevent the authorized seizing or securing of any person, goods, wares, merchandise, or other property, gives notice or attempts to give notice of the possible search and seizure to any person, shall be fined under this title or imprisoned not more than five years, or both.

Again, I greatly appreciate your cooperation in this matter with our agency. If you have any questions or comments, please feel free to call SA [redacted] at [redacted]

Sincerely yours,

Sheri A. Farrar  
Special Agent in Charge

b6  
b7c

By:

[redacted]  
Supervisory Special Agent

U.S. Department of Justice

Federal Bureau of Investigation



550 Main Street, Room 9000  
Cincinnati, Ohio 45202  
November 3, 1998

In Reply, Please Refer to  
File No.

[Redacted]  
Indiana University, South Bend Campus  
1700 Mishawaka Ave.  
South Bend, IN 46634-7111

RE: Notice to Preserve Evidence Under  
Title 18, U.S.C., 2703(f)

Dear [Redacted]

This letter is to follow up our telephone conversation on October 29, 1998. As I stated at that time, I am a Special Agent for the Federal Bureau of Investigation (FBI), a duly authorized federal law enforcement officer empowered to investigate unauthorized access into private, state, local and federal computer systems. As previously discussed, during the following date(s): August 25 and 26, 1998, an unknown individual illegally entered a state owned academic institutional computer system at sumac.occ.uc.edu, [Redacted] According to our investigation, this communication originated or passed through your system, oit1.iusb.edu, [Redacted]

b6  
b7C

(X)  
CB

b7E

This letter serves to inform you that I will be pursuing the issuance of a subpoena and/or court order under Title 18, U.S.C., 2703(d), respectively, to trace the unknown individual back from your system. Inasmuch that this process can be time consuming, I have requested, pursuant to Title 18, U.S.C., 2703(f), that you take appropriate measures to preserve transactional logs, contents of any relevant communications, back-up files, and any other evidence that pertains to the aforementioned connections.

For ease of reference, Title 18, U.S.C., 2703(f), provides:

(f) Requirement to preserve evidence.

(1) In general.- A provider of a wire or electronic communication service or a remote computing service, upon the request of a government entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

288-CI-68562-314  
Searched \_\_\_\_\_  
Serialized \_\_\_\_\_  
Indexed \_\_\_\_\_  
Filed \_\_\_\_\_

- 1 - Addressee
- (1) - CI (288-CI-68562) BB:bb (2)

3075b 06.01h

For

(2) **Period of retention.**- Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90 day period upon a renewal request by the governmental entity.

Finally, although you have been most cooperative, we have in other situations, experienced some informational leaks. While such leaks may represent misplaced good intentions, they can have serious impact upon our investigation. Accordingly, we would respectfully request that your personnel be placed on notice that they are subject to criminal liability should they disclose any privileged information. The governing statute in this regard is Title 18, U.S.C., 2232(b), which provides:

(b) **Notice of Search.**- Whoever, having knowledge that any person authorized to make searches and seizures has been authorized or is otherwise likely to make a search or seizure, in order to prevent the authorized seizing or securing of any person, goods, wares, merchandise, or other property, gives notice or attempts to give notice of the possible search and seizure to any person, shall be fined under this title or imprisoned not more than five years, or both.

Again, I greatly appreciate your cooperation in this matter with our agency. If you have any questions or comments, please feel free to call SA [redacted] at [redacted]

Sincerely yours,

Sheri A. Farrar  
Special Agent in Charge

b6  
b7c

By: [redacted]  
Supervisory Special Agent

U.S. Department of Justice



Federal Bureau of Investigation

In Reply, Please Refer to  
File No.

550 Main Street, Room 9000  
Cincinnati, Ohio 45202  
November 3, 1998

[Redacted]

California Institute of Technology  
Information Technology Services  
014-81  
Pasadena, CA 91125

RE: Notice to Preserve Evidence Under  
Title 18, U.S.C., 2703(f)

Dear [Redacted]

This letter is to follow up our telephone conversation on October 29, 1998. As I stated at that time, I am a Special Agent for the Federal Bureau of Investigation (FBI), a duly authorized federal law enforcement officer empowered to investigate unauthorized access into private, state, local and federal computer systems. As previously discussed, during the following date(s): September 22, 1998, an unknown individual illegally entered a state owned academic institutional computer system at sumac.occ.uc.edu, [Redacted] According to our investigation, this communication originated or passed through your system, newvortex.ama.caltech.edu, [Redacted]

b6  
b7C

⊗  
03/1  
b7E

This letter serves to inform you that I will be pursuing the issuance of a subpoena and/or court order under Title 18, U.S.C., 2703(d), respectively, to trace the unknown individual back from your system. Inasmuch that this process can be time consuming, I have requested, pursuant to Title 18, U.S.C., 2703(f), that you take appropriate measures to preserve transactional logs, contents of any relevant communications, back-up files, and any other evidence that pertains to the aforementioned connections.

For ease of reference, Title 18, U.S.C., 2703(f), provides:

288-CI-68562-35  
Searched \_\_\_\_\_  
Serialized \_\_\_\_\_  
Indexed \_\_\_\_\_  
Filed \_\_\_\_\_

(f) Requirement to preserve evidence.

(1) In general.- A provider of a wire or electronic communication service or a remote computing service, upon the request of a government entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

- ① - Addressee
- ① - CI (288-CI-68562) / BB:bb (2)

307 66 07.0+h

*[Handwritten signature]*

(2) **Period of retention.**- Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90 day period upon a renewal request by the governmental entity.

Finally, although you have been most cooperative, we have in other situations, experienced some informational leaks. While such leaks may represent misplaced good intentions, they can have serious impact upon our investigation. Accordingly, we would respectfully request that your personnel be placed on notice that they are subject to criminal liability should they disclose any privileged information. The governing statute in this regard is Title 18, U.S.C., 2232(b), which provides:

(b) **Notice of Search.**- Whoever, having knowledge that any person authorized to make searches and seizures has been authorized or is otherwise likely to make a search or seizure, in order to prevent the authorized seizing or securing of any person, goods, wares, merchandise, or other property, gives notice or attempts to give notice of the possible search and seizure to any person, shall be fined under this title or imprisoned not more than five years, or both.

Again, I greatly appreciate your cooperation in this matter with our agency. If you have any questions or comments, please feel free to call SA [redacted] at [redacted]

Sincerely yours,

Sheri A. Farrar  
Special Agent in Charge

b6  
b7c

By: [redacted]

Supervisory Special Agent



U.S. Department of Justice



Federal Bureau of Investigation

In Reply, Please Refer to  
File No.

550 Main Street, Room 9000  
Cincinnati, Ohio 45202  
November 3, 1998

[Redacted]  
Haverford College  
Academic Computing  
Haverford, PA 19041

RE: Notice to Preserve Evidence Under  
Title 18, U.S.C., 2703(f)

Dear [Redacted]

This letter is to follow up our telephone conversation on October 29, 1998. As I stated at that time, I am a Special Agent for the Federal Bureau of Investigation (FBI), a duly authorized federal law enforcement officer empowered to investigate unauthorized access into private, state, local and federal computer systems. As previously discussed, during the following date(s): September 23 and 24, 1998, an unknown individual illegally entered a state owned academic institutional computer system at sumac.occ.uc.edu, [Redacted]. According to our investigation, this communication originated or passed through your system, io.haverford.edu, [Redacted].

b6  
b7C

(1)  
Lid

b7E

This letter serves to inform you that I will be pursuing the issuance of a subpoena and/or court order under Title 18, U.S.C., 2703(d), respectively, to trace the unknown individual back from your system. Inasmuch that this process can be time consuming, I have requested, pursuant to Title 18, U.S.C., 2703(f), that you take appropriate measures to preserve transactional logs, contents of any relevant communications, back-up files, and any other evidence that pertains to the aforementioned connections.

288-CI-68562-  
36

For ease of reference, Title 18, U.S.C., 2703(f), provides:

Searched \_\_\_\_\_  
Serialized \_\_\_\_\_  
Indexed \_\_\_\_\_  
Filed \_\_\_\_\_

(f) Requirement to preserve evidence.

(1) In general.- A provider of a wire or electronic communication service or a remote computing service, upon the request of a government entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

1 - Addressee  
① - CI (288-CI-68562)/BB:bb (2)

307 6608. 0th

Ru

(2) **Period of retention.**- Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90 day period upon a renewal request by the governmental entity.

Finally, although you have been most cooperative, we have in other situations, experienced some informational leaks. While such leaks may represent misplaced good intentions, they can have serious impact upon our investigation. Accordingly, we would respectfully request that your personnel be placed on notice that they are subject to criminal liability should they disclose any privileged information. The governing statute in this regard is Title 18, U.S.C., 2232(b), which provides:

**(b) Notice of Search.**- Whoever, having knowledge that any person authorized to make searches and seizures has been authorized or is otherwise likely to make a search or seizure, in order to prevent the authorized seizing or securing of any person, goods, wares, merchandise, or other property, gives notice or attempts to give notice of the possible search and seizure to any person, shall be fined under this title or imprisoned not more than five years, or both.

Again, I greatly appreciate your cooperation in this matter with our agency. If you have any questions or comments, please feel free to call SA [redacted], at [redacted]

Sincerely yours,

Sheri A. Farrar  
Special Agent in Charge

b6  
b7c

By: [redacted]  
Supervisory Special Agent

U.S. Department of Justice



Federal Bureau of Investigation

In Reply, Please Refer to  
File No.

550 Main Street, Room 9000  
Cincinnati, Ohio 45202  
November 3, 1998

[Redacted]

University of Texas at Austin  
Office of Telecommunication Services  
Services Building, Room 319  
Austin, TX 78712-1024

RE: Notice to Preserve Evidence Under  
Title 18, U.S.C., 2703(f)

Dear [Redacted]

This letter is to follow up our telephone conversation on October 29, 1998. As I stated at that time, I am a Special Agent for the Federal Bureau of Investigation (FBI), a duly authorized federal law enforcement officer empowered to investigate unauthorized access into private, state, local and federal computer systems. As previously discussed, during the following date(s): September 22, 1998, an unknown individual illegally entered a state owned academic institutional computer system at sumac.occ.uc.edu, [Redacted]. According to our investigation, this communication originated or passed through your system, net.cs.utexas.edu, [Redacted].

b6  
b7c

(7)

b7E

This letter serves to inform you that I will be pursuing the issuance of a subpoena and/or court order under Title 18, U.S.C., 2703(d), respectively, to trace the unknown individual back from your system. Inasmuch that this process can be time consuming, I have requested, pursuant to Title 18, U.S.C., 2703(f), that you take appropriate measures to preserve transactional logs, contents of any relevant communications, back-up files, and any other evidence that pertains to the aforementioned connections.

288-CI-68562-37

For ease of reference, Title 18, U.S.C., 2703(f), provides:

Searched \_\_\_\_\_  
Serialized \_\_\_\_\_  
Indexed \_\_\_\_\_  
Filed \_\_\_\_\_

(f) Requirement to preserve evidence.

(1) In general.- A provider of a wire of electronic communication service or a remote computing service, upon the request of a government entity, shall take all necessary

1 - Addressee

① - CI (288-CI-68562) BB:bb (2)

307 11/7 9. 04h

For

steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

**(2) Period of retention.-** Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90 day period upon a renewal request by the governmental entity.

Finally, although you have been most cooperative, we have in other situations, experienced some informational leaks. While such leaks may represent misplaced good intentions, they can have serious impact upon our investigation. Accordingly, we would respectfully request that your personnel be placed on notice that they are subject to criminal liability should they disclose any privileged information. The governing statute in this regard is Title 18, U.S.C., 2232(b), which provides:

**(b) Notice of Search.-** Whoever, having knowledge that any person authorized to make searches and seizures has been authorized or is otherwise likely to make a search or seizure, in order to prevent the authorized seizing or securing of any person, goods, wares, merchandise, or other property, gives notice or attempts to give notice of the possible search and seizure to any person, shall be fined under this title or imprisoned not more than five years, or both.

Again, I greatly appreciate your cooperation in this matter with our agency. If you have any questions or comments, please feel free to call SA [redacted] at [redacted]

Sincerely yours,

Sheri A. Farrar  
Special Agent in Charge

b6  
b7c

By: [redacted]  
Supervisory Special Agent

U.S. Department of Justice



Federal Bureau of Investigation

In Reply, Please Refer to  
File No.

550 Main Street, Room 9000  
Cincinnati, Ohio 45202  
November 3, 1998

[Redacted]

Auburn University  
Division of Telecommunications/ETV  
Auburn University, AL 36849-5423

RE: Notice to Preserve Evidence Under  
Title 18, U.S.C., 2703(f)

Dear [Redacted]

This letter is to follow up our telephone conversation on October 29, 1998. As I stated at that time, I am a Special Agent for the Federal Bureau of Investigation (FBI), a duly authorized federal law enforcement officer empowered to investigate unauthorized access into private, state, local and federal computer systems. As previously discussed, during the following date(s): September 23, 1998, an unknown individual illegally entered a state owned academic institutional computer system at sumac.occ.uc.edu, [Redacted] According to our investigation, this communication originated or passed through your system, node-57-2.spidle.auburn.edu, [Redacted]

b6  
b7c

(X)  
61

b6  
b7c

This letter serves to inform you that I will be pursuing the issuance of a subpoena and/or court order under Title 18, U.S.C., 2703(d), respectively, to trace the unknown individual back from your system. Inasmuch that this process can be time consuming, I have requested, pursuant to Title 18, U.S.C., 2703(f), that you take appropriate measures to preserve transactional logs, contents of any relevant communications, back-up files, and any other evidence that pertains to the aforementioned connections.

For ease of reference, Title 18, U.S.C., 2703(f), provides:

(f) Requirement to preserve evidence.

(1) In general.- A provider of a wire or electronic communication service or a remote computing service, upon the request of a government entity, shall take all necessary

288-CI-68562-38  
Searched \_\_\_\_\_  
Serialized \_\_\_\_\_  
Indexed \_\_\_\_\_  
Filed \_\_\_\_\_

- 1 - Addressee
- 1 - CI (288-CI-68562) BB:bb (2)

30755/1.0th

R

steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

**(2) Period of retention.-** Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90 day period upon a renewal request by the governmental entity.

Finally, although you have been most cooperative, we have in other situations, experienced some informational leaks. While such leaks may represent misplaced good intentions, they can have serious impact upon our investigation. Accordingly, we would respectfully request that your personnel be placed on notice that they are subject to criminal liability should they disclose any privileged information. The governing statute in this regard is Title 18, U.S.C., 2232(b), which provides:

**(b) Notice of Search.-** Whoever, having knowledge that any person authorized to make searches and seizures has been authorized or is otherwise likely to make a search or seizure, in order to prevent the authorized seizing or securing of any person, goods, wares, merchandise, or other property, gives notice or attempts to give notice of the possible search and seizure to any person, shall be fined under this title or imprisoned not more than five years, or both.

Again, I greatly appreciate your cooperation in this matter with our agency. If you have any questions or comments, please feel free to call SA [redacted] at [redacted]

Sincerely yours,

Sheri A. Farrar  
Special Agent in Charge

b6  
b7c

By: [redacted]  
Supervisory Special Agent

U.S. Department of Justice

Federal Bureau of Investigation



550 Main Street, Room 9000  
Cincinnati, Ohio 45202  
November 3, 1998

In Reply, Please Refer to  
File No.

[Redacted]  
Duke University  
407 North Building  
Durham, NC 27706

RE: Notice to Preserve Evidence Under  
Title 18, U.S.C., 2703(f)

Dear [Redacted]

This letter is to follow up our telephone conversation on October 29, 1998. As I stated at that time, I am a Special Agent for the Federal Bureau of Investigation (FBI), a duly authorized federal law enforcement officer empowered to investigate unauthorized access into private, state, local and federal computer systems. As previously discussed, during the following date(s): September 22 and 24, 1998, an unknown individual illegally entered a state owned academic institutional computer system at sumac.occ.uc.edu, [Redacted]. According to our investigation, this communication originated or passed through your system, bme-www.egr.duke.edu, [Redacted].

b6  
b7c

⊗  
b6  
b7c

b7E

This letter serves to inform you that I will be pursuing the issuance of a subpoena and/or court order under Title 18, U.S.C., 2703(d), respectively, to trace the unknown individual back from your system. Inasmuch that this process can be time consuming, I have requested, pursuant to Title 18, U.S.C., 2703(f), that you take appropriate measures to preserve transactional logs, contents of any relevant communications, back-up files, and any other evidence that pertains to the aforementioned connections.

288-CI-68562-39

For ease of reference, Title 18, U.S.C., 2703(f), provides:

(f) Requirement to preserve evidence.

Searched \_\_\_\_\_  
Serialized \_\_\_\_\_  
Indexed \_\_\_\_\_  
Filed \_\_\_\_\_

(1) In general.- A provider of a wire or electronic communication service or a remote computing service, upon the request of a government entity, shall take all necessary

- 1 - Addressee
- 1 - CI (288-CI-68562) BB:bb (2)

3075610.0th

*[Handwritten signature]*

steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

**(2) Period of retention.**- Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90 day period upon a renewal request by the governmental entity.

Finally, although you have been most cooperative, we have in other situations, experienced some informational leaks. While such leaks may represent misplaced good intentions, they can have serious impact upon our investigation. Accordingly, we would respectfully request that your personnel be placed on notice that they are subject to criminal liability should they disclose any privileged information. The governing statute in this regard is Title 18, U.S.C., 2232(b), which provides:

**(b) Notice of Search.**- Whoever, having knowledge that any person authorized to make searches and seizures has been authorized or is otherwise likely to make a search or seizure, in order to prevent the authorized seizing or securing of any person, goods, wares, merchandise, or other property, gives notice or attempts to give notice of the possible search and seizure to any person, shall be fined under this title or imprisoned not more than five years, or both.

Again, I greatly appreciate your cooperation in this matter with our agency. If you have any questions or comments, please feel free to call SA [redacted] at [redacted]

Sincerely yours,

Sheri A. Farrar  
Special Agent in Charge

b6  
b7c

By: [redacted]  
Supervisory Special Agent



FEDERAL BUREAU OF INVESTIGATION  
FOIPA  
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 238

Page 4 ~ b3

Sealed Court Documents

Page 5 ~ b3

Sealed Court Documents

Page 6 ~ b3

Sealed Court Documents

Page 7 ~ b3

Sealed Court Documents

Page 8 ~ b3

Sealed Court Documents

Page 9 ~ b3

Sealed Court Documents

Page 10 ~ b3

Sealed Court Documents

Page 11 ~ b3

Sealed Court Documents

Page 12 ~ b3

Sealed Court Documents

Page 13 ~ b3

Sealed Court Documents

Page 14 ~ b3

Sealed Court Documents

Page 15 ~ b3

Sealed Court Documents

Page 16 ~ b3

Sealed Court Documents

Page 17 ~ b3

Sealed Court Documents

Page 18 ~ b3

Sealed Court Documents

Page 19 ~ b3

Sealed Court Documents

Page 20 ~ b3

Sealed Court Documents

Page 21 ~ b3

Sealed Court Documents

Page 22 ~ b3

Sealed Court Documents

Page 23 ~ b3

Sealed Court Documents

Page 24 ~ b3

Sealed Court Documents

Page 25 ~ b3

Sealed Court Documents

Page 26 ~ b3  
Sealed Court Documents  
Page 27 ~ b3  
Sealed Court Documents  
Page 28 ~ b3  
Sealed Court Documents  
Page 34 ~ Referral/Direct  
Page 35 ~ Referral/Direct  
Page 36 ~ Referral/Direct  
Page 37 ~ Referral/Direct  
Page 38 ~ Referral/Direct  
Page 39 ~ Referral/Direct  
Page 45 ~ Referral/Consult  
Page 47 ~ Referral/Consult  
Page 48 ~ Referral/Direct  
Page 49 ~ Referral/Direct  
Page 50 ~ Referral/Direct  
Page 51 ~ Referral/Direct  
Page 52 ~ Referral/Direct  
Page 53 ~ Referral/Direct  
Page 54 ~ Referral/Direct  
Page 55 ~ Referral/Direct  
Page 56 ~ Referral/Direct  
Page 57 ~ Referral/Direct  
Page 59 ~ b7E  
Page 60 ~ b7E  
Page 61 ~ b7E  
Page 62 ~ b6, b7C, b7E  
Page 63 ~ b7E  
Page 64 ~ b7E  
Page 65 ~ b7E  
Page 66 ~ b7E  
Page 67 ~ b7E  
Page 68 ~ b6, b7C, b7E  
Page 69 ~ b7E  
Page 70 ~ b7E  
Page 71 ~ b7E  
Page 72 ~ b7E  
Page 73 ~ b7E  
Page 74 ~ b7E  
Page 75 ~ b6, b7C, b7E  
Page 76 ~ b7E  
Page 77 ~ b7E  
Page 78 ~ b7E  
Page 79 ~ b7E  
Page 80 ~ b7E  
Page 81 ~ b7E  
Page 82 ~ b7E  
Page 83 ~ b7E  
Page 84 ~ b7E  
Page 85 ~ b7E

Page 86 ~ b7E  
Page 87 ~ b7E  
Page 88 ~ b7E  
Page 89 ~ b7E  
Page 90 ~ b7E  
Page 91 ~ b7E  
Page 92 ~ b7E  
Page 93 ~ b7E  
Page 105 ~ b3  
Sealed Court Documents  
Page 106 ~ b3  
Sealed Court Documents  
Page 107 ~ b3  
Sealed Court Documents  
Page 108 ~ b3  
Sealed Court Documents  
Page 109 ~ b3  
Sealed Court Documents  
Page 110 ~ b3  
Sealed Court Documents  
Page 111 ~ b3  
Sealed Court Documents  
Page 112 ~ b3  
Sealed Court Documents  
Page 113 ~ b3  
Sealed Court Documents  
Page 114 ~ b3  
Sealed Court Documents  
Page 115 ~ b3  
Sealed Court Documents  
Page 116 ~ b3  
Sealed Court Documents  
Page 117 ~ b3  
Sealed Court Documents  
Page 118 ~ b3  
Sealed Court Documents  
Page 119 ~ b3  
Sealed Court Documents  
Page 120 ~ b3  
Sealed Court Documents  
Page 121 ~ b3  
Sealed Court Documents  
Page 122 ~ b3  
Sealed Court Documents  
Page 123 ~ b3  
Sealed Court Documents  
Page 131 ~ Referral/Consult  
Page 138 ~ b3  
Sealed Court Documents  
Page 139 ~ b3  
Sealed Court Documents

Page 140 ~ b3  
Sealed Court Documents  
Page 141 ~ b3  
Sealed Court Documents  
Page 142 ~ b3  
Sealed Court Documents  
Page 143 ~ b3  
Sealed Court Documents  
Page 144 ~ b3  
Sealed Court Documents  
Page 145 ~ b3  
Sealed Court Documents  
Page 146 ~ b3  
Sealed Court Documents  
Page 147 ~ b3  
Sealed Court Documents  
Page 148 ~ b3  
Sealed Court Documents  
Page 149 ~ b3  
Sealed Court Documents  
Page 150 ~ b3  
Sealed Court Documents  
Page 151 ~ b3  
Sealed Court Documents  
Page 152 ~ b3  
Sealed Court Documents  
Page 153 ~ b3  
Sealed Court Documents  
Page 154 ~ b3  
Sealed Court Documents  
Page 155 ~ b3  
Sealed Court Documents  
Page 156 ~ b3  
Sealed Court Documents  
Page 157 ~ b3  
Sealed Court Documents  
Page 159 ~ b3  
Sealed Court Documents  
Page 160 ~ b3  
Sealed Court Documents  
Page 161 ~ b3  
Sealed Court Documents  
Page 162 ~ b3  
Sealed Court Documents  
Page 163 ~ b3  
Sealed Court Documents  
Page 164 ~ b3  
Sealed Court Documents  
Page 165 ~ b3  
Sealed Court Documents  
Page 166 ~ b3

Sealed Court Documents  
Page 167 ~ b3  
Sealed Court Documents  
Page 168 ~ b3  
Sealed Court Documents  
Page 169 ~ b3  
Sealed Court Documents  
Page 170 ~ b3  
Sealed Court Documents  
Page 171 ~ b3  
Sealed Court Documents  
Page 172 ~ b3  
Sealed Court Documents  
Page 173 ~ b3  
Sealed Court Documents  
Page 174 ~ b3  
Sealed Court Documents  
Page 175 ~ b3  
Sealed Court Documents  
Page 176 ~ b3  
Sealed Court Documents  
Page 177 ~ b3  
Sealed Court Documents  
Page 178 ~ b3  
Sealed Court Documents  
Page 179 ~ b3  
Sealed Court Documents  
Page 180 ~ b3  
Sealed Court Documents  
Page 181 ~ b3  
Sealed Court Documents  
Page 182 ~ b3  
Sealed Court Documents  
Page 183 ~ b3  
Sealed Court Documents  
Page 186 ~ b3  
Sealed Court Documents  
Page 187 ~ b3  
Sealed Court Documents  
Page 188 ~ b3  
Sealed Court Documents  
Page 189 ~ b3  
Sealed Court Documents  
Page 190 ~ b3  
Sealed Court Documents  
Page 191 ~ b3  
Sealed Court Documents  
Page 192 ~ b3  
Sealed Court Documents  
Page 193 ~ b3  
Sealed Court Documents

Page 194 ~ b3  
Sealed Court Documents  
Page 195 ~ b3  
Sealed Court Documents  
Page 196 ~ b3  
Sealed Court Documents  
Page 197 ~ b3  
Sealed Court Documents  
Page 198 ~ Referral/Consult  
Page 199 ~ Referral/Direct  
Page 200 ~ Referral/Direct  
Page 201 ~ Referral/Direct  
Page 210 ~ b3  
Sealed Court Documents  
Page 211 ~ b3  
Sealed Court Documents  
Page 212 ~ b3  
Sealed Court Documents  
Page 213 ~ b3  
Sealed Court Documents  
Page 214 ~ b3  
Sealed Court Documents  
Page 215 ~ b3  
Sealed Court Documents  
Page 216 ~ b3  
Sealed Court Documents  
Page 217 ~ b3  
Sealed Court Documents  
Page 218 ~ b3  
Sealed Court Documents  
Page 219 ~ b3  
Sealed Court Documents  
Page 220 ~ b3  
Sealed Court Documents  
Page 221 ~ b3  
Sealed Court Documents  
Page 222 ~ b3  
Sealed Court Documents  
Page 223 ~ b3  
Sealed Court Documents  
Page 224 ~ b3  
Sealed Court Documents  
Page 225 ~ b3  
Sealed Court Documents  
Page 240 ~ Referral/Direct  
Page 241 ~ Referral/Direct  
Page 242 ~ Referral/Direct  
Page 254 ~ Referral/Direct  
Page 255 ~ Referral/Direct  
Page 256 ~ Referral/Direct  
Page 257 ~ Referral/Direct

Page 258 ~ Referral/Direct  
Page 259 ~ Referral/Direct  
Page 260 ~ Referral/Direct  
Page 261 ~ Referral/Direct  
Page 262 ~ Referral/Direct  
Page 263 ~ Referral/Direct  
Page 264 ~ Referral/Direct  
Page 265 ~ Referral/Direct  
Page 266 ~ Referral/Direct  
Page 267 ~ Referral/Direct  
Page 268 ~ Referral/Direct  
Page 269 ~ Referral/Direct  
Page 270 ~ Referral/Direct  
Page 271 ~ Referral/Direct  
Page 272 ~ Referral/Direct  
Page 273 ~ Referral/Direct  
Page 274 ~ Referral/Direct  
Page 275 ~ Referral/Direct  
Page 276 ~ Referral/Direct  
Page 277 ~ Referral/Direct  
Page 278 ~ Referral/Direct  
Page 279 ~ Referral/Direct  
Page 280 ~ Referral/Direct  
Page 281 ~ Referral/Direct  
Page 282 ~ Referral/Direct  
Page 283 ~ Referral/Direct  
Page 284 ~ Referral/Direct  
Page 285 ~ Referral/Direct  
Page 286 ~ Referral/Direct  
Page 287 ~ Referral/Direct  
Page 288 ~ Referral/Direct  
Page 289 ~ Referral/Direct  
Page 290 ~ Referral/Direct  
Page 291 ~ Referral/Direct  
Page 292 ~ Referral/Direct  
Page 293 ~ Referral/Direct  
Page 294 ~ Referral/Direct  
Page 295 ~ Referral/Direct  
Page 296 ~ Referral/Direct  
Page 297 ~ Referral/Direct  
Page 298 ~ Referral/Direct  
Page 299 ~ Referral/Direct  
Page 300 ~ Referral/Direct  
Page 301 ~ Referral/Direct  
Page 302 ~ Referral/Direct  
Page 303 ~ Referral/Direct  
Page 304 ~ Referral/Direct  
Page 305 ~ Referral/Direct  
Page 306 ~ Referral/Direct  
Page 311 ~ Referral/Direct  
Page 312 ~ Referral/Direct

Page 313 ~ Referral/Direct  
Page 314 ~ b3  
Sealed Court Documents  
Page 315 ~ b3  
Sealed Court Documents  
Page 316 ~ b3  
Sealed Court Documents  
Page 320 ~ b6, b7C, b7E