[redacted]

From: [redacted]
Sent: Thursday, August 02, 2007 3:48 PM
To: [redacted]

b6
b7C

Cc:
Subject: Reminder - Urgent FOIA Request - Deadline - Friday, August 3, 2007

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Just a reminder from UC [redacted] Please be sure to review your files for anything concerning CIPAV technology.

b6
b7C

Thank you,

[redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-16-2008 BY 60322uclp/stp/rds

b6
b7C

-----Original Message-----
From: [redacted]
Sent: Thursday, July 26, 2007 2:06 PM
To: [redacted]

Cc:
Subject: Urgent FOIA Request - Deadline - Friday, August 3, 2007
Importance: High

[redacted]

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
b7C

Good Afternoon,

Per UC [redacted] please provide hard copies of ALL documentation, to include e-mails, concerning CIPAV Technology. All information is to be turned in by COB Friday, August 3rd, 2007. Additionally, it is requested that you please put all documents in chronological order. If I am not in the office that day, please take your documents to [redacted]

Thanks,

[redacted]

[redacted]
Management Assistant
Operational Technology Division (OTD)
Cryptologic and Electronic Analysis Unit (CEAU)
[redacted] (Chantilly)
(Quantico)
(Cell)

b6
b7C
b2

SENSITIVE BUT UNCLASSIFIED

[redacted]

From: [redacted]
Sent: Monday, July 30, 2007 3:23 PM
To: [redacted]
Cc:
Subject: RE: Urgent FOIA Request - Deadline - Friday, August 3, 2007

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

How much, if anything, does CIPAV have to do with the IPAV that was developed in our group back in 2001?

P.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-16-2008 BY 60322uclp/stp/rds

> SENSITIVE BUT UNCLASSIFIED
> NON-RECORD
>
> Good Afternoon,
>
> Per UC [redacted] please provide hard copies of ALL
> documentation, to include e-mails, concerning CIPAV
> Technology. All information is to be turned in by COB
> Friday, August 3rd, 2007. Additionally, it is requested that
> you please put all documents in chronological order. If I am
> not in the office that day, please take your documents to
> [redacted]
>
> Thanks,
>
> [redacted]
>
> [redacted]
> Management Assistant
> Operational Technology Division (OTD)
> Cryptologic and Electronic Analysis Unit (CEAU)
> [redacted] (Chantilly)
> (Quantico)
> (Cell)
>
>
> SENSITIVE BUT UNCLASSIFIED

b6
b7C

b6
b7C
b2

SENSITIVE BUT UNCLASSIFIED

From:
Sent: Friday, July 27, 2007 4:59 PM
To:
Cc:
Subject: FW: Urgent FOIA Request - Deadline - Friday, August 3, 2007

Importance: High

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

I want to clear up any misconceptions you have about and my role here. We are here to provide you with legal advice concerning Science and Technology matters. Also, is my backup for CEAU and my other units, just as I am his backup for his units in his absence. It is improper for you to send general "taskers" to either one of us, and particularly to if I am here.

b6
b7C

Assistant General Counsel
Science and Technology Law Unit
Phone:
Cell phone
Secure phone
Fax

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED b2
DATE 06-16-2008 BY 60322uclp/stp/rds b6
b7C

-----Original Message-----
From:
Sent: Friday, July 27, 2007 4:45 PM
To:
Subject: FW: Urgent FOIA Request - Deadline - Friday, August 3, 2007
Importance: High

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Good Afternoon,

Per a request from CEAU UC he wanted you both to review the Urgent FOIA request below. If you have any questions, please contact me at the below numbers.

b6
b7C

v/r,

-----Original Message-----
From: (OTD) (CON)
Sent: Thursday, July 26, 2007 2:06 PM
To: (OTD) (FBI); (OTD) (CON); (OTD) (CON); (OTD) (FBI); (OTD) (CON); (OTD) (CON); (OTD) (FBI); (OTD) (FBI); (OTD) (FBI); (OTD) (CON); (OTD) (CON); (OTD) (FBI); (OTD) (FBI); (OTD) (CON); (OTD) (CON); (OTD) (FBI); (OTD) (FBI); (OTD) (FBI); (OTD) (CON); (OTD) (CON); (OS) (CON); (OTD) (FBI); (OTD) (FBI); (OTD) (FBI); (OTD) (FBI); (OTD) (CON); (OTD) (FBI); (OTD) (FBI); (OTD) (CON); (OTD) (CON); (OTD) (FBI); (OTD) (CON); (OTD) (CON); (OTD) (FBI); (OTD) (CON); (OS) (CON); (OTD) (FBI); (OTD) (CON); (OS) (CON)

From: [redacted] b6 b7C
Sent: Friday, July 27, 2007 4:56 PM
To: [redacted]
Cc:
Subject: RE: Urgent FOIA Request - Deadline - Friday, August 3, 2007

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

There is nothing to review in your e-mail to the unit concerning the Urgent FOIA request. In fact, if there was a copy of the FOIA attached, there would be nothing for us to review. When a FOIA request goes out from HQ, the persons receiving the request must gather all responsive documents, note any concerns they have about the release of those documents, and send it to the person that sent the request. The FBI has a FOIA unit that, in conjunction with the FOIA Litigation Unit of OGC, reviews what is submitted to them to determine what will must be released and what we will claim an exception for.

[redacted]
Assistant General Counsel
Science and Technology Law Unit
Phone: [redacted]
Cell phone: [redacted]
Secure phone: [redacted]
Fax [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-16-2008 BY 60322uclp/stp/rds

b6 b7C b2

-----Original Message-----
From: [redacted] (OTD) (CON)
Sent: Friday, July 27, 2007 4:45 PM
To: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: FW: Urgent FOIA Request - Deadline - Friday, August 3, 2007
Importance: High

b6 b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Good Afternoon,

Per a request from CEAU UC [redacted] he wanted you both to review the Urgent FOIA request below. If you have any questions, please contact me at the below numbers.

v/r,
[redacted]

-----Original Message-----
From: [redacted] (OTD) (CON)
Sent: Thursday, July 26, 2007 2:06 PM
To: [redacted] (OTD) (FBI); [redacted] (OTD) (CON); [redacted] (OTD) (CON); [redacted] (OTD) (FBI); [redacted] (OTD) (CON); [redacted] (OTD) (FBI); [redacted] (OTD) (FBI); [redacted] (OTD) (CON); [redacted] (OTD) (CON); [redacted] (OTD) (FBI); [redacted] (OTD) (FBI); [redacted] (OTD) (FBI); [redacted] (OTD) (CON); [redacted] (OTD) (CON); [redacted] (OTD) (FBI); [redacted] (OTD) (FBI); [redacted] (OTD) (FBI); [redacted] (OTD) (FBI); [redacted] (OTD) (CON); [redacted] (OS) (CON); [redacted] (OTD) (FBI); [redacted] (OTD) (FBI); [redacted] (OTD) (CON); [redacted] (OTD) (FBI); [redacted] (OTD) (FBI); [redacted] (OTD) (FBI); [redacted] (OTD) (FBI); [redacted] (OTD) (CON); [redacted] (OTD) (CON); [redacted] (OTD) (FBI); [redacted] (OTD) (CON); [redacted] (OTD) (CON); [redacted] (OTD) (FBI); [redacted] (OTD) (CON); [redacted] (OTD) (FBI); [redacted] (OS) (CON); [redacted] (OTD) (FBI); [redacted] (OTD) (CON); [redacted] (OS) (CON)
Cc: [redacted] (OTD) (CON)
Subject: Urgent FOIA Request - Deadline - Friday, August 3, 2007

b6 b7C

Importance: High

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Good Afternoon,

Per UC Pandelides, please provide hard copies of ALL documentation, to include e-mails, concerning CIPAV Technology. All information is to be turned in by COB Friday, August 3rd, 2007. Additionally, it is requested that you please put all documents in chronological order. If I am not in the office that day, please take your documents to Jennifer Ashinhurst.

Thanks,

Leslie

Leslie Delp
Management Assistant
Operational Technology Division (OTD)
Cryptologic and Electronic Analysis Unit (CEAU)
571-223-3509 (Chantilly)
703-985-1252 (Quantico)
202-538-1952 (Cell)

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

[redacted]

From: [redacted]
Sent: Friday, July 27, 2007 8:34 AM
To: [redacted]
Subject: FW: Urgent FOIA Request - Deadline - Friday, August 3, 2007
Importance: High

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-16-2008 BY 60322uclp/stp/rds

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

You might want to send this to [redacted] too.

Since [redacted] was the UC I assume he is also responding to this?

[redacted]
Information Technology Specialist
Operational Technology Division
[redacted]

b6
b7C
b2

-----Original Message-----
From: [redacted](OTD) (CON)
Sent: Thursday, July 26, 2007 2:06 PM
To: [redacted](OTD) (FBI); [redacted](OTD) (CON); [redacted](OTD) (CON); [redacted](OTD) (FBI); [redacted](OTD) (CON); [redacted](OTD) (CON); [redacted](OTD) (FBI); [redacted](OTD) (FBI); [redacted](OTD) (FBI); [redacted](OTD) (CON); [redacted](OTD) (CON); [redacted](OTD) (FBI); [redacted](OTD) (FBI); [redacted](OTD) (FBI); [redacted](OTD) (CON); [redacted](OTD) (CON); [redacted](OTD) (FBI); [redacted](OTD) (FBI); [redacted](OTD) (FBI); [redacted](OTD) (CON); [redacted](OTD) (CON); [redacted](OS) (CON); [redacted](OTD) (FBI); [redacted](OTD) (FBI); [redacted](OTD) (FBI); [redacted](OTD) (FBI); [redacted](OTD) (FBI); [redacted](OTD) (CON); [redacted](OTD) (CON); [redacted](OTD) (FBI); [redacted](OTD) (CON); [redacted](OTD) (CON); [redacted](OTD) (FBI); [redacted](OTD) (FBI); [redacted](OTD) (CON); [redacted](OTD) (FBI); [redacted](OS) (CON); [redacted](OTD) (FBI); [redacted](OTD) (CON); [redacted](OS) (CON)

b6
b7C

Cc: [redacted](OTD) (CON)
Subject: Urgent FOIA Request - Deadline - Friday, August 3, 2007
Importance: High

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Good Afternoon,

Per UC [redacted] please provide hard copies of ALL documentation, to include e-mails, concerning CIPAV Technology. All information is to be turned in by COB Friday, August 3rd, 2007. Additionally, it is requested that you please put all documents in chronological order. If I am not in the office that day, please take your documents to [redacted]

Thanks,

b6
b7C

[redacted]
[redacted]
Management Assistant
Operational Technology Division (OTD)

Cryptologic and Electronic Analysis Unit (CEAU)
[redacted] (Chantilly)
(Quantico)
(Cell)

b2

SENSITIVE BUT UNCLASSIFIED

[redacted]

From: [redacted] b6 b7C
Sent: Monday, June 25, 2007 1:30 PM
To: [redacted]
Cc:
Subject: FW: Traveler Program

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-16-2008 BY 60322uclp/stp/rds

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] I talked to [redacted] about this program, explaining that you would be discussing [redacted] analysis responsibility with [redacted] said that they were looking to evolve this into more aggressive coverage -- what I took to mean CIPAV and RASS - [redacted] analysis. I told her that we and [redacted] should be kept on the ECs as "read and clear" for the time being. b6 b7C b2 b7E

-----Original Message-----
From: [redacted] b6 b7C
Sent: Monday, June 25, 2007 9:25 AM
To: [redacted]
Cc:
Subject: RE: Traveler Program

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

Please give me a call when you get a chance [redacted] The Computer Intrusion Section, National Cyber Investigative Joint Task Force (NCIJTF), Investigative Operations Group (IOG), is in the process of formulating a "standardized" Traveler Program for implementation by FBI Field Divisions in coordination with our Intelligence Community Partners. [redacted] b6 b7C b2 b2 b7E

My past experience working these types of operations (through the Honolulu Division) developed some baseline assessment whereby the following technical personnel assisted: [redacted] OTD, CEAU; [redacted] SOSU; [redacted] SPTU; and [redacted] (former Program Manager). The NCIJTF is working closely with the WFO-NVRA, CR-16, in establishing their traveler operation(s). b6 b7C

I look forward to speaking with you.

SSA [redacted]
CyD/CIS/C3IU-2
NCIJTF / PRC-DET Team Lead
[redacted] (STAO) b6 b7C b2

-----Original Message-----
From: [redacted]
Sent: Wednesday, June 20, 2007 12:04 PM
To: [redacted] b6 b7C
Cc:
Subject: Traveler Program

SENSITIVE BUT UNCLASSIFIED
NON-RECORD b6 b7C

Hi, [redacted]
This is in furtherance of the voice message I left for you this morning. As I understand it, you're managing the Traveler

Program whereby, please correct me if wrong, [redacted]. STAO's Investigative Analysis Unit is discussing technical support of the program with my unit. [redacted] and the expected turnaround time?

Thank you,

[redacted]

SSA [redacted]
Secure Technologies Exploitation Group
Cryptologic and Electronic Analysis Unit (CEAU)
Electronic Surveillance Technology Section
Operational Technology Division
ERF Extension
Quantico, VA
tel: [redacted] (unsecure)
fax [redacted] (unsecure)
tel: [redacted] (secure)
fax [redacted] (secure)

b2
b7E

b6
b7C

b2
b6
b7C

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

[redacted]

From: [redacted]
Sent: Wednesday, July 25, 2007 1:06 PM
To: DICLEMENTE, ANTHONY P. (OTD) (FBI); [redacted]
Subject: RE: FOIA request from Wired News

b6
b7C

DATE: 08-15-2008
CLASSIFIED BY 60322uclp/stp/rds
REASON: 1.4 (c)
DECLASSIFY ON: 08-15-2033

SECRET
RECORD 319

Probably best discussed in person. After our 4:00?

-----Original Message-----
From: DICLEMENTE, ANTHONY P. (OTD) (FBI)
Sent: Wednesday, July 25, 2007 12:34 PM
To: [redacted]
Subject: RE: FOIA request from Wired News

b6
b7C

SECRET
RECORD 319

My understanding is that the tool itself is unclassified. If the tool was classified, we would have had to pursue DAG approval to use it in a criminal investigation.

Anthony P. DiClemente
Chief, Data Acquisition and Intercept Section
Operational Technology Division
[redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b6
b7C
b2

-----Original Message-----
From: [redacted]
Sent: Wednesday, July 25, 2007 11:28 AM
To: [redacted] DICLEMENTE, ANTHONY P. (OTD) (FBI)
Subject: RE: FOIA request from Wired News

SECRET
RECORD 319

b6
b7C

That helps. The FOIA attorney explained that if the tool was Law Enforcement sensitive, that it would not be protected. It could be "watered down", but we might have to provide something. Since, the specifics (which I take to be what is being requested) are SECRET, that should help. Thanks!

[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, July 25, 2007 11:16 AM
To: [redacted] (OTD) (FBI); DICLEMENTE, ANTHONY P. (OTD) (FBI)
Subject: RE: FOIA request from Wired News

SECRET
RECORD 319

If I understand the questions that Mr. Poulsen would like answered, such as how we deliver the system, etc,

(S) the details are classified SECRET. [redacted] etc. are all held SECRET. The actual compiled code, for obvious reasons, cannot be SECRET. However, the workings thereof would, by necessity, as they relate to SECRET source code, etc, are Sensitive. b1

Bill

b6
b7C

-----Original Message-----
From: [redacted]
Sent: Wednesday, July 25, 2007 10:58 AM
To: [redacted] DICLEMENTE, ANTHONY P. (OTD) (FBI)
Subject: RE: FOIA request from Wired News

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Are these details classified SECRET?

-----Original Message-----
From: [redacted]
Sent: Wednesday, July 25, 2007 8:36 AM
To: DICLEMENTE, ANTHONY P. (OTD) (FBI); [redacted]
Subject: RE: FOIA request from Wired News

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

In addition, I have always insisted that the underlying technical details of the CIPAV are classified. Therefore, we should be shielded from this.

[redacted]

-----Original Message-----
From: DICLEMENTE, ANTHONY P. (OTD) (FBI)
Sent: Tuesday, July 24, 2007 5:23 PM
To: [redacted]
Cc: [redacted]
Subject: RE: FOIA request from Wired News

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

Recommend you contact the FBI/OGC FOIA Litigation Unit. We have been able to utilize the FOIA exemption (b) 7(e) successfully to protect law enforcement techniques and methods such as the CIPAV in the past.

b6
b7C

Anthony P. DiClemente
Chief, Data Acquisition and Intercept Section
Operational Technology Division
[redacted]

b6
b7C
b2

-----Original Message-----
From: [redacted]
Sent: Tuesday, July 24, 2007 4:02 PM
To: [redacted] DICLEMENTE, ANTHONY P. (OTD) (FBI)
Subject: FW: FOIA request from Wired News

UNCLASSIFIED
NON-RECORD

[redacted] Tony,

See attached email string. It appears that there was a FOIA request concering the CIPAV used in the Seattle case. Looks like Seattle CDC is looking for assistance. Could you please provide me with guidance. Thanks! b6 b7C

[redacted]

-----Original Mess[redacted] b6
From: [redacted] b7C
Sent: [redacted]
To: [redacted]
Subject: FW: FOIA request from Wired News

~~UNCLASSIFIED~~
~~NON-RECORD~~

FYI.

SSA [redacted]
Operational Technology Division b6
Data Acquisition and Intercept Section b7C
Cryptologic and Electronic Analysis Unit b2
Software Development Group
[redacted] (desk)
(cell)
(fax-unclass)

-----Original Message-----
From: [redacted] b6
Sent: [redacted] b7C
To: [redacted]
Subject: FW: FOIA request from Wired News

~~UNCLASSIFIED~~
~~NON-RECORD~~

[redacted]

FYI, we received the below FOIA request and responded through our CDC SSA [redacted]

I understand there was a flurry of activity last week related to the conviction of the defendant, the subsequent media attention, and misinformation being circulated about the manner by which this case was handled by my squad. b6 b7C

Please let me know if anyone has any pending issues concerning the above.

Thank you [redacted]

b6
b7C

-----Original Message-----
From: [redacted]
Sent: Tuesday, July 24, 2007 10:52 AM
To: [redacted]
Cc: [redacted]
Subject: FW: FOIA request from Wired News

~~UNCLASSIFIED~~
NON-RECORD

~~SECRET~~

[redacted]

Your inquiry was forwarded to me for resolution since I am the Field Office FOIPA Coordinator.
The technique you mention in your e-mail is a sensitive law enforcement technique. The Seattle Field Office does not believe it appropriate to release any information about this technique, beyond that which was contained in the affidavit, and recommends that you consult with the folks in the Cyber Division and/or the Operation Technology Division for their opinion prior to processing the request.
If I may be of further assistance please let me know.
Thank you.

b6
b7C

[redacted]
Supervisory Special Agent
Chief Division Counsel
Seattle Division
[redacted]

b6
b7C
b2

-----Original Message-----
From: [redacted]
Sent: Monday, July 23, 2007 4:18 PM
To: [redacted]
Cc:
Subject: FW: FOIA request from Wired News

b6
b7C

~~UNCLASSIFIED~~
NON-RECORD

-----Original Message-----
From: [redacted]
Sent: Monday, July 23, 2007 12:07 PM
To: [redacted]
Subject: FW: FOIA request from Wired News

b6
b7C

~~UNCLASSIFIED~~
NON-RECORD

-----Original Message-----
From: [redacted]
Sent: Monday, July 23, 2007 11:56 AM
To: [redacted]
Subject: FOIA request from Wired News

b6
b7C

~~UNCLASSIFIED~~
NON-RECORD

[redacted]

We received a FOIA request from Keven Poulsen, Wired News, addressed to FBI HQ, 'seeking any documents, including but not limited to electron records, concerning the FBI's development and utilization of so-called "Computer and Internet Protocol Address Veridier" [CIPAV]'. I already did a ACS search and did not come up with any information.

b6
b7C

I bring this to your attention, because the writer mentioned the following, "A CIPAV is described in a June 12, 2007 application and affidavit filed by FBI Special Agent Norman B. Sanders, Jr of the Seattle Field Office as something that can be transmitted electronically to an investigation target, and , once activated, 'will cause the activating computer to send network level messages, including the activating computer's originating IP address and MAC address, other variables, and certain registry-type information' to a computer under the FBI control."

~~SECRET~~

Do you know where this information is located in order to respond to the FOIA request?

Thanks for your assistance.

[redacted] b6
Legal Administrative Specialist b7C

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign Counterintelligence Investigations
DECLASSIFY ON: 20320725
SECRET

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign Counterintelligence Investigations
DECLASSIFY ON: 20320725
SECRET

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign Counterintelligence Investigations
DECLASSIFY ON: 20320725
SECRET

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign Counterintelligence Investigations
DECLASSIFY ON: 20320725
SECRET

[redacted]

From: [redacted]
Sent: Tuesday, July 24, 2007 3:21 PM
To: [redacted] b6 b7C
Subject: FW: SF Newspaper Ad Response

Importance: High

DATE: 08-15-2008
CLASSIFIED BY 60322uclp/stp/rds
REASON: 1.4 (c)
DECLASSIFY ON: 08-15-2033

SECRET
RECORD [redacted] (S) b1

See the entire thread. This may be fall out from the CIPAV article and news story. In case you didn't know, a complete story appeared on Fox News a day after the story broke. A former AUSA appeared on the show and talked exclusively about the capability of the tool and the legal issues concerning it.

SSA [redacted] b6 b7C b2
Operational Technology Division
Data Acquisition and Intercept Section
Cryptologic and Electronic Analysis Unit
Software Development Group
[redacted] (desk)
(cell)
(fax-unclass)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

-----Original Message-----
From: [redacted]
Sent: Tuesday, July 24, 2007 3:14 PM b6 b7C
To: [redacted]
Subject: FW: SF Newspaper Ad Response
Importance: High

SECRET
RECORD [redacted] (S) b1

fyi

-----Original Message-----
From: [redacted]
Sent: Friday, July 20, 2007 5:00 PM b6 b7C
To: [redacted]
Subject: FW: SF Newspaper Ad Response
Importance: High

SECRET
RECORD [redacted] (S) b1

-----Original Message-----
From: [redacted]
Sent: Tuesday, July 17, 2007 11:17 AM b6 b7C
To: [redacted]
Subject: FW: SF Newspaper Ad Response
Importance: High

SECRET
RECORD [redacted] (S) b1

FYI

-----Original Message-----
From:
Sent: Tuesday, July 17, 2007 9:12 AM
To:
Cc:
Subject: FW: SF Newspaper Ad Response
Importance: High

b6
b7C

SECRET
RECORD (S)

(S) b6 b7C

b1

-----Original Message-----
From:
Sent: Tuesday, July 17, 2007 8:11 AM
To:
Cc:
Subject: FW: SF Newspaper Ad Response
Importance: High

b6
b7C

SECRET
RECORD (S)

b1

FYI (S)

-----Original Message-----
From:
Sent: Monday, July 16, 2007 5:15 PM
To:
Subject: FW: SF Newspaper Ad Response

b6
b7C

SECRET
RECORD

b1

(S)

FYI -

Please see below if you haven't already.

Regards,

-----Original Message-----
From:
Sent: Monday, July 16, 2007 4:55 PM
To:
Subject: FW: SF Newspaper Ad Response

b6
b7C

SECRET
RECORD [redacted] (S)

b1

[redacted]

-----Original Message-----
From: [redacted] (HO) (FBI)
Sent: Monday, July 16, 2007 4:54 PM
To: [redacted]
Subject: RE: SF Newspaper Ad Response

b6
b7C

SECRET
RECORD [redacted] (S)

b1

[redacted]

My replacements are [redacted]

[redacted]
SSA [redacted]
Houston Division
Squad CI-3
[redacted]

b6
b7C
b2

-----Original Message-----
From: [redacted]
Sent: Monday, July 16, 2007 3:34 PM
To: [redacted]
Subject: FW: SF Newspaper Ad Response

(S) SECRET
RECORD [redacted]

b1

[redacted] I know you both have successors but I didn't know who they were.
I'm back in NY and saw this traffic. I don't know if this has any implications for SQ.

b6
b7C

[redacted]

-----Original Message-----
From: [redacted]
Sent: Monday, July 16, 2007 4:26 PM
To: [redacted]
Subject: FW: SF Newspaper Ad Response

b6
b7C

(S) SECRET
RECORD [redacted]

b1

Reporting from CHICAGO ref the LA info I sent around earlier today.
Thanks,

[redacted]

-----Original Message-----
From: [redacted]

b6
b7C

Sent: Monday, July 16, 2007 12:50 PM
To: [redacted] b6 b7C
Subject: RE: SF Newspaper Ad Response

SECRET
RECORD [redacted] (S) b1

[redacted] (S)

SSA [redacted] b6 b7C b2

-----Original Message-----
From: [redacted]
Sent: Monday, July 16, 2007 11:38 AM
To: [redacted] b6 b7C
Subject: SF Newspaper Ad Response

SECRET
RECORD [redacted] (S)

Gents:

(S) [redacted] b1

[redacted]

SSA [redacted]
FBI Los Angeles Squad CI-2
[redacted] (STE)
(cell)
[redacted] b6 b7C b2

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFICATION EXEMPTION 1
SECRET

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign Counterintelligence Investigations
DECLASSIFICATION EXEMPTION 1

~~SECRET~~

[redacted]

From: [redacted] b6 b7C
Sent: Tuesday, July 24, 2007 8:29 AM
To: [redacted]
Cc:

Subject: RE: CIPAV?

DATE: 08-15-2008
CLASSIFIED BY 60322uclp/stp/rds
REASON: 1.4 (c)
DECLASSIFY ON: 08-15-2033

~~SENSITIVE BUT UNCLASSIFIED~~
NON-RECORD

b1

[redacted] (S)

Guy

SSA [redacted]
Acting Unit Chief
Data Intercept Technology Unit
[redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b6
b7C
b2

-----Original Message-----
From: [redacted] b6 b7C
Sent: Tuesday, July 24, 2007 6:27 AM
To: [redacted]
Cc:
Subject: CIPAV?

~~SENSITIVE BUT UNCLASSIFIED~~
NON-RECORD

Hello Guy,

(S) [redacted] b1

[redacted] is tdy here, and he is handling this matter. Can you advise him who he should contact to find out more about CIPAV?

Thanks again,

[redacted] b6 b7C b2
Assistant Legal Attaché
Frankfurt, Germany
[redacted]

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SECRET~~

From:
Sent: Monday, July 23, 2007 2:08 PM
To:
Cc:
Subject: RE: JTF-GNO Request for FBI Tool

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-16-2008 BY 60322uclp/stp/rds

UNCLASSIFIED
NON-RECORD

is correct in his hesitancy, based on liaibility concerns. I don't know of any ponies addressing this issue. Perhaps this would be a good topic for the NCIJTF? Let's look into this after the open house?

b6
b7C
b2

SSA
Cyber / C3IU-2
- Work
- Fax
- Cell

"If you don't learn to laugh at troubles, you won't have anything to laugh at when you grow old." - Edward W. Howe

-----Original Message-----
From:
Sent: Monday, July 23, 2007 12:02 PM
To:
Subject: RE: JTF-GNO Request for FBI Tool

b6
b7C

UNCLASSIFIED
NON-RECORD

On a case-by-case basis, we may be able to assist. But am weary to just hand over our tools to another Gov't agency without any oversight or protection for our tool/technique.

-----Original Message-----
From:
Sent: Monday, July 23, 2007 11:46 AM
To:
Cc:
Subject: FW: JTF-GNO Request for FBI Tool

b6
b7C

UNCLASSIFIED
NON-RECORD

b6
b7C

b2

The NCIS and JTF-GNO has asked for assistance from the FBI in obtaining different FBI tools for use . I talked with (OTD) this morning and he said the FBI can't share FBI tools with other agencies without an MOU between the two agencies. Do you know of any MOU ponies - I could use in drafting up an MOU?

Any assistance will be appreciated.

Thanks!

-----Original Message-----
From: [redacted]
Sent: Monday, July 23, 2007 11:11 AM
To: [redacted]
Subject: JTF-GNO Request for FBI Tool

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted]

The Joint Task Force - Global Network Operations (JTF-GNO) has asked the FBI for a copy of a tool called "Computer Internet Protocol Address Verifier" (CIPAV). Please advise where I could go to find this tool for release [redacted].

Thanks!

b6
b7C
b2

[redacted]
NCIS Liaison - FBI Cyber Division
[redacted]

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

[redacted]

From: [redacted]
Sent: Wednesday, July 18, 2007 6:11 PM
To: [redacted]
Subject: RE: Seattle CIPAV Case

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-16-2008 BY 60322uclp/stp/rds

[redacted]

I have forwarded this e-mail to management and the press officers, along with a link to the wired.com story. I have also verbally briefed management.

b6
b7C

[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, July 18, 2007 2:35 PM
To: [redacted] (SE) (FBI)
Cc: [redacted] (OTD) (FBI); DICLEMENTE, ANTHONY P. (OTD) (FBI) [redacted] (OTD) (FBI)
Subject: Seattle CIPAV Case

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

I just wanted to reiterate our telephonic discussion, so that you can pass this information on to your Executive Management. As we are all aware, the Seattle bomb threat case has gone public on several news and technical websites, providing detailed information on some of the capabilities of this particular tool. This obviously causes us some concern as we try to make every effort possible to protect the FBI's sensitive tools and techniques. That being said, with a good possibility that future inquiries will be forthcoming to Seattle Division regarding how the FBI was able to collect the information that ultimately helped solve this case, we want to ensure that the capabilities of the CIPAV are minimized, if discussed at all. This and many tools deployed by the FBI are law enforcement sensitive and, as such, we request that as little information as possible be provided to as few individuals as possible. Thanks and please let me know if you have any questions.

b6
b7C

[redacted]
Unit Chief
Cryptologic and Electronic Analysis Unit (CEAU)

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

[redacted]

From: [redacted] b6 b7C
Sent: Wednesday, July 18, 2007 3:57 PM
To: [redacted]
Subject: FW: FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats

UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-16-2008 BY 60322uclp/stp/rds

Wow you're good!

-----Original Message-----
From: [redacted]
Sent: Wednesday, July 18, 2007 2:13 PM
To: [redacted]
Subject: FW: FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats

UNCLASSIFIED
NON-RECORD

b6 b7C b2

When did we get tools like this? Oh wait, now I remember. Anyway, glad to see it all spelled out in Wired.

[redacted]

-----Original Message-----
From: [redacted] b6 b7C
Sent: Wednesday, July 18, 2007 11:03 AM
To: [redacted]
Subject: FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats

UNCLASSIFIED
NON-RECORD

This looks like "the good stuff" that the criminal people never get to use. Interesting that it's in an criminal affidavit.

FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats

Wired.com

2:00 AM

By Kevin Poulsen

July 18, 2007

SEATTLE, WA – FBI agents trying to track the source of e-mailed bomb threats against a Washington high school last month sent the suspect a secret surveillance program designed to surreptitiously monitor him and report back to a government server, according to an FBI affidavit obtained by Wired News.

The court filing offers the first public glimpse into the bureau's long-suspected spyware capability, in which the FBI adopts techniques more common to online criminals. The software was sent to the owner of an anonymous MySpace profile linked to bomb threats against Timberline High School near Seattle. The code led the FBI to 15-year-old Josh Glazebrook, a student at the school, who on Monday pleaded guilty to making bomb threats, identity theft and felony harassment. In an affidavit seeking a search warrant to use the software, filed last month in U.S. District Court in the Western District of Washington, FBI agent Norman Sanders describes the software as a "computer and internet protocol address verifier," or CIPAV.

FBI Spyware In A Nutshell

The full capabilities of the FBI's "computer and internet protocol address verifier" are closely guarded secrets, but here's some of the data the malware collects from a computer immediately after infiltrating it, according to a bureau affidavit acquired by Wired News.

- **IP address**
- **MAC address of ethernet cards**
- **A list of open TCP and UDP ports**
- **A list of running programs • The operating system type, version and serial number**
- **The default internet browser and version**
- **The registered user of the operating system, and registered company name, if any**
- **The current logged-in user name**
- **The last visited URL**

Once that data is gathered, the CIPAV begins secretly monitoring the computer's internet use, logging every IP address to which the machine connects. All that information is sent over the internet to an FBI computer in Virginia, likely located at the FBI's technical laboratory in Quantico. Sanders wrote that the spyware program gathers a wide range of information, including the computer's IP address; MAC address; open ports; a list of running programs; the operating system type, version and serial number; preferred internet browser and version; the computer's registered owner and registered company name; the current logged-in user name and the last-visited URL. The CIPAV then settles into a silent "pen register" mode, in which it lurks on the target computer and monitors its internet use, logging the IP address of every computer to which the machine connects for up to 60 days.

Under a ruling this month by the 9th U.S. Circuit Court of Appeals, such surveillance -- which does not capture the content of the communications -- can be conducted without a wiretap warrant, because internet users have no "reasonable expectation of privacy" in the data when using the internet. According to the affidavit, the CIPAV sends all the data it collects to a central FBI server located somewhere in eastern Virginia. The server's precise location wasn't specified, but previous FBI internet surveillance technology -- notably its Carnivore packet-sniffing hardware -- was developed and run out of the bureau's technology laboratory at the FBI Academy in Quantico, Virginia.

The FBI's national office referred an inquiry about the CIPAV to a spokeswoman for the FBI Laboratory in Quantico, who declined to comment on the technology. The FBI has been known to use PC-spying technology since at least 1999, when a court ruled the bureau could break into reputed mobster Nicodemo Scarfo's office to plant a covert keystroke logger on his computer. But it wasn't until 2001 that the FBI's plans to use hacker-style computer-intrusion techniques emerged in a report by

MSNBC.com. The report described an FBI program called "Magic Lantern" that uses deceptive e-mail attachments and operating-system vulnerabilities to infiltrate a target system. The FBI later confirmed the program, and called it a "workbench project" that had not been deployed.

No cases have been publicly linked to such a capability until now, says David Sobel, a Washington, D.C., attorney with the Electronic Frontier Foundation. "It might just be that the defense lawyers are not sufficiently sophisticated to have their ears perk up when this methodology is revealed in a prosecution," says Sobel. "I think it's safe to say the use of such a technique raises novel and unresolved legal issues." The June affidavit doesn't reveal whether the CIPAV can be configured to monitor keystrokes, or to allow the FBI real-time access to the computer's hard drive, like typical Trojan malware used by computer criminals. It notes that the "commands, processes, capabilities and ... configuration" of the CIPAV is "classified as a law enforcement sensitive investigative technique, the disclosure of which would likely jeopardize other ongoing investigations and/or future use of the technique."

The document is also silent as to how the spyware infiltrates the target's computer. In the Washington case, the FBI delivered the program through MySpace's messaging system, which allows HTML and embedded images. The FBI might have simply tricked the suspect into downloading and opening an executable file, says Roger Thompson, CTO of security vendor Exploit Prevention Labs. But the bureau could also have exploited one of the legion of web browser vulnerabilities discovered by computer-security researchers and cybercrooks -- or even used one of its own. "It's quite possible the FBI knows about vulnerabilities that have not been disclosed to the rest of the world," says Thompson. "If they had discovered one, they would not have disclosed it, and that would be a great way to get stuff on people's computer. Then I guess they can bug whoever they want."

The FBI's 2008 budget request hints at the bureau's efforts in the hacking arena, including $220,000 sought to "purchase highly specialized equipment and technical tools used for covert (and) overt search and seizure forensic operations.... This funding will allow the technology challenges (sic) including bypass, defeat or compromise of computer systems." With the FBI in the business of hacking, security companies are in a tight place. Thompson's LinkScanner product, for example, scans web pages for security exploits, and warns the customer if one is found. How would his company respond if the FBI asked him to turn a blind eye to CIPAV? He says he's never fielded such a request. "That would put us in a very difficult position," Thompson says. "I don't know what I'd say."

The Washington case unfolded May 30, when a handwritten bomb threat prompted the evacuation of Timberline High School in Lacey, Washington. No bomb was found. On June 4, a second bomb threat was e-mailed to the school from a Gmail account that had been newly created under the name of an innocent student. "I will be blowing up your school Monday, June 4, 2007," the message read. "There are 4 bombs planted throughout Timberline high school. One in the math hall, library hall, main office and one portable. The bombs will go off in 5 minute intervals at 9:15 AM." In addition, the message promised, "The e-mail server of your district will be offline starting at 8:45 am."

The author made good on the latter threat, and a denial-of-service attack smacked the North Thurston Public Schools computer network, generating a relatively modest 1 million packets an hour. Responding to the bomb threat, school administrators ordered an evacuation of the high school, but, once again, no explosives were found. That began a bizarre cat-and-mouse game between law enforcement and school officials and the ersatz cyberterrorist, who e-mailed a new hoax bomb threat every day for several days, each triggering a new evacuation. Each threat used the same pseudonym, but was sent from a different, newly created Gmail account to complicate tracing efforts.

On June 7, the hoaxer started issuing threats through other online mediums. In his most brazen move, he set up a MySpace profile called Timberlinebombinfo and sent friend requests to 33 classmates. The whole time he was daring law enforcement officials to trace him. "The e-mail was sent over a newly made Gmail account, from overseas in a foreign country," he wrote in one message. "Seeing as you're too stupid to

trace the e-mail back lets (sic) get serious," he taunted in another. "Maybe you should hire Bill Gates to tell you that it is coming from Italy. HAHAHA. Oh wait. I already told you that it's coming from Italy." As promised, attempts to trace the hoaxer dead-ended at a hacked server in Grumello del Monte, Italy.

The FBI's Seattle Division contacted the FBI legal attaché in Rome, who provided an official request to the Italian national police for assistance. But on June 12, perhaps fed up with the mocking, the FBI applied for and obtained a search warrant authorizing the bureau to send the CIPAV to the Timberlinebombinfo MySpace profile. Court documents reveal the search warrant was "executed" June 13 at 5:49 p.m. Though the CIPAV provided a wealth of information, Glazebrook's IP address would have been enough to guide the FBI to the teen's front door. John Sinclair, Glazebrook's attorney, says his client never intended to blow anything up -- "it was a prank from the get-go" -- but admits he hacked into computers in Italy to launder his activities, and that he launched the denial-of-service attack against the school district's network.

Glazebrook was sentenced Monday to 90 days in custody, and given credit for 32 days he's spent behind bars since his arrest. When he's released he'll be on two years' probation with internet and computer restrictions, and he's been expelled from high school. The teen is being held at the Thurston County Juvenile Detention Center, where he will serve out his sentence, says Sinclair. Sinclair says he was told that the FBI had tracked down his client in response to a request from local police -- but that he didn't know exactly how the bureau did it.

"The prosecutor made it clear that they wouldn't indicate how this device works or how they do it," says Sinclair. "For obvious reasons." Larry Carr, a spokesman with the FBI's Seattle field office, couldn't confirm that the CIPAV is the same software previously known as Magic Lantern, but emphasized that the bureau's technological capabilities have grown since the 2001 report. The case shows that FBI scientists are equipped to handle internet threats, says Carr. "It sends a message that, if you're going to try and do stuff like this online, that we have the ability to track individuals' movements online and bring the case to resolution."

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

~~SECRET~~

[redacted]

From: [redacted] b6 b7C
Sent: Monday, July 16, 2007 4:35 PM
To: [redacted]
Cc: [redacted] b1
Subject: (S) RE: [redacted]

~~SENSITIVE BUT UNCLASSIFIED~~
NON-RECORD

DATE: 08-15-2008
CLASSIFIED BY 60322uclp/stp/rds
REASON: 1.4 (c)
DECLASSIFY ON: 08-15-2033

I think we have a problem.

[redacted]

[redacted]
Information Technology Specialist
Operational Technology Division
Office [redacted] b6 b7C b2
Mobile
Pager

-----Original Message-----
From: [redacted] b6 b7C
Sent: Monday, July 16, 2007 4:33 PM
To: [redacted]
Cc: [redacted]
Subject: RE: [redacted] (S)

~~SENSITIVE BUT UNCLASSIFIED~~
NON-RECORD b1

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Only the IP address and then only once.

[redacted]

[redacted] b6 b7C
Assistant General Counsel
Science and Technology Law Unit
Office of the General Counsel
Federal Bureau of Investigation
Ph [redacted] b2
Cel [redacted] b6
Ph (Secure) [redacted] b7C
Fax [redacted]

-----Original Message-----
From: [redacted] b6 b7C
Sent: Monday, July 16, 2007 4:30 PM
To: [redacted]
Cc: [redacted]
(S) **Subject:** [redacted] b1

~~SENSITIVE BUT UNCLASSIFIED~~
NON-RECORD

~~SECRET~~

[redacted] the pony we sent stated b6 b7C

(S) [redacted] b1

[redacted] b6 b7C
Information Technology Specialist
Operational Technology Division
[redacted]

-----Original Message-----
From: [redacted] b6 b7C
Sent: Monday, July 16, 2007 3:52 PM
To: [redacted]
Cc: [redacted] (FBI)
(S) **Subject:** [redacted] b1

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] b6 b7C

(S) [redacted] b1

[redacted]
Assistant General Counsel
Science and Technology Law Unit
Office of the General Counsel
Federal Bureau of Investigation
[redacted] b6 b7C

[redacted] b6 b7C b2

SENSITIVE BUT UNCLASSIFIED

~~SECRET~~

From:
Sent: Monday, July 02, 2007 9:26 AM
To:
Subject: RE: Traveler Program

DATE: 08-15-2008
CLASSIFIED BY 60322uclp/stp/rds
REASON: 1.4 (c)
DECLASSIFY ON: 08-15-2033

b6
b7C

~~SENSITIVE BUT UNCLASSIFIED~~
NON-RECORD

How do you feel about asking CyD for $ to implement this effort?

-----Original Message-----
From:
Sent: Monday, July 02, 2007 9:18 AM
To:
Subject: RE: Traveler Program

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b6
b7C

~~SENSITIVE BUT UNCLASSIFIED~~
NON-RECORD

Thanks Can we request that do an EC with all the parties involved explaining exactly what the traveler program is and the scope of it. This should include etc. After speaking with this morning, neither of us have the resources or are even sure whether the FBI should be doing this, but we need a little more info. I can call if you are busy, but not sure what your schedule is with the Director.

b6
b7C
b2
b7E

Thanks!

-----Original Message-----
From:
Sent: Monday, June 25, 2007 1:30 PM
To:
Cc:
Subject: FW: Traveler Program

b6
b7C

~~SENSITIVE BUT UNCLASSIFIED~~
NON-RECORD

b1

(S)

-----Original Message-----
From:
Sent: Monday, June 25, 2007 9:25 AM
To:
Cc:
Subject: RE: Traveler Program

b6
b7C

~~SENSITIVE BUT UNCLASSIFIED~~
NON-RECORD

Please give me a call when you get a chance The Computer Intrusion Section, National

b6
b7C
b2

~~SECRET~~

~~SECRET~~

From: [redacted]
Sent: Monday, June 26, 2006 6:44 AM
To: [redacted] b6 b7C
Cc:
Subject: RE [redacted] (S) b1

DATE: 08-15-2008
CLASSIFIED BY 60322uclp/stp/rds
REASON: 1.4 (c)
DECLASSIFY ON: 08-15-2033

SECRET//NOFORN
RECORD [redacted] (S) b1

(S)

[redacted] b1

Hope this info helps.

Sincerely,

[redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b6
b7C

-----Original Message-----
From: [redacted]
Sent: Thursday, April 27, 2006 6:02 PM
To: [redacted] b6 b7C
Cc:
Subject: FW: [redacted] (S) b1
Importance: High

SECRET//NOFORN
RECORD [redacted] b1

b6
b7C

[redacted] (S) b1

~~SECRET~~

Thanks
[redacted]

b6
b7C

SSA [redacted]
FBIHQ/CTD/LX1
ITOS 1/CONUS 1
[redacted]

b2
b6
b7C

-----Original Message-----
From: [redacted]
Sent: Thursday, April 27, 2006 4:46 PM
To: [redacted]
Cc:
Subject: [redacted] (S)

b6
b7C

b1

SECRET//NOFORN
RECORD [redacted]

(S)

b1

Gentlemen:

[redacted]

~~SECRET~~

(S)

b1

Your input is appreciated.

b6
b7C
b2

SA
Philadelphia FBI - Cyber Squad (8)

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign Counterintelligence Investigations
DECLASSIFICATION EXEMPTION 1
SECRET//NOFORN

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign Counterintelligence Investigations
DECLASSIFICATION EXEMPTION 1
SECRET//NOFORN

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign Counterintelligence Investigations
DECLASSIFICATION EXEMPTION 1
SECRET//NOFORN

~~SECRET~~

DATE: 08-15-2008
CLASSIFIED BY 60322uclp/stp/rds
REASON: 1.4 (c)
DECLASSIFY ON: 08-15-2033

From: [redacted] b6 b7C
Sent: Thursday, June 21, 2007 3:56 PM
To: [redacted]
Subject: RE: NIP Request for Quarter 3 - DUE COB Thrsday 06/21

SECRET
RECORD [redacted] b2

(S)

[redacted] b1

[redacted]

SSA [redacted] b6 b7C b2
Operational Technology Division (OTD)
Cryptologic and Electronic Analysis Unit (CEAU)
[redacted] (cell)
(desk)
(fax)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b6 b7C

-----Original Message-----
From: [redacted]
Sent: Wednesday, June 20, 2007 9:58 AM
To: [redacted]
Subject: NIP Request for Quarter 3 - DUE COB Thrsday 06/21

SECRET
RECORD [redacted] b2

b6 b7C

(S)

[redacted] b1

I need by COB Thursday. Thanks!

[redacted] b6 b7C

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign Counterintelligence Investigations
DECLASSIFICATION EXEMPTION 1
SECRET

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign Counterintelligence Investigations
DECLASSIFICATION EXEMPTION 1

~~SECRET~~

[redacted]

From: [redacted] b6 b7C
Sent: Wednesday, June 20, 2007 1:18 PM
To: [redacted]
Subject: RE: NIP Request for Quarter 3 - DUE COB Thrsday 06/21

SECRET
RECORD [redacted] b2

DATE: 08-15-2008
CLASSIFIED BY 60322uclp/stp/rds
REASON: 1.4 (c)
DECLASSIFY ON: 08-15-2033

[redacted] (S) b1

-----Original Message-----
From: [redacted]
Sent: Wednesday, June 20, 2007 9:58 AM
To: [redacted]
Subject: NIP Request for Quarter 3 - DUE COB Thrsday 06/21

b6 b7C

SECRET
RECORD [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b2

b6 b7C

[redacted]

(S) [redacted] b1

I need by COB Thursday. Thanks!

[redacted] b6 b7C

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign Counterintelligence Investigations
DECLASSIFICATION EXEMPTION 1
SECRET

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign Counterintelligence Investigations
DECLASSIFICATION EXEMPTION 1
SECRET

~~SECRET~~

[redacted] b6 b7C

From: [redacted]
Sent: Tuesday, June 19, 2007 5:29 PM
To: [redacted]
Subject: RE: Reminder

DATE: 08-15-2008
CLASSIFIED BY 60322uclp/stp/rds
REASON: 1.4 (c)
DECLASSIFY ON: 08-15-2033

~~UNCLASSIFIED~~
~~NON-RECORD~~

[redacted] b1 (S)

SSA [redacted]
Operational Technology Division
Digital Evidence Section
Cryptologic and Electronic Analysis Unit
Software Development Group
[redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT b6 b7C b2
WHERE SHOWN OTHERWISE

-----Original Message-----
From: [redacted] b6 b7C
Sent: Tuesday, June 19, 2007 12:55 PM
To: [redacted]
Subject: Reminder

~~UNCLASSIFIED~~
~~NON-RECORD~~

Sorry to be a pain. But please let me know when you have had a chance to go through the leads so I can look at and have answers to remaining by Thursday. Thanks!

[redacted] b6 b7C

~~UNCLASSIFIED~~

~~UNCLASSIFIED~~

~~SECRET~~

[redacted]

From: [redacted]
Sent: Thursday, June 14, 2007 3:23 PM
To: [redacted]
Subject: Seattle Case Summary

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 09-22-2008
CLASSIFIED BY 60322 uc lp/stp/rds
REASON: 1.4 (c)
DECLASSIFY ON: 09-22-2033

UNCLASSIFIED
NON-RECORD

[redacted]

b6
b7C

Per your request, the following is a synopsis of the Seattle Division's investigation:

On 06/06/2007, the Seattle Division was contacted by the Lacey Police Department (LPD), Lacey, WA, regarding numerous bomb threats and DDOS attacks received at the Timberline School District, Lacey, WA. The threats began on 05/30/2007 and persisted through 06/04/2007. The threats necessitated the daily evacuation of Timberline High School. The LPD and the Washington State Patrol (WSP) performed school evacuations and bomb sweeps with negative results. Parents and school district employees informed local television stations and newspapers, which aired the story on June 6, 2007. As a result, the LPD requested investigative assistance from the Northwest Cyber Crime Task Force (NCCTF) headed by the Seattle Division. In turn, the Seattle Field Office requested assistance from the CEAU with geophysically locating the UNSUB.

[redacted] (S)
b1

information obtained from Comcast confirmed the suspicions of Law Enforcement and led to the issuing of a search warrant and arrest warrant. A 15 year old male student from Timberline High School was taken into custody without incident at his home at approximately 2 A.M. this date. The minor confessed to issuing the bomb threats. Bomb threats dated this date were found on the minor's computer. The minor's computer equipment was seized and the arrest was made without incident. Following an interview with the minor, the LPD was able to clear another threat case, as the minor confessed to issuing telephone death threats to teachers and others, including his parents, earlier this year.

SSA [redacted]
Operational Technology Division
Digital Evidence Section
Cryptologic and Electronic Analysis Unit
Software Development Group

b6
b7C
b2

[redacted]

~~SECRET~~

~~SECRET~~

[redacted]

From: [redacted]
Sent: Friday, June 08, 2007 2:15 PM
To: [redacted]
Subject: FW: 288A-SE-93709

b6
b7C

DATE: 08-15-2008
CLASSIFIED BY 60322uclp/stp/rds
REASON: 1.4 (c)
DECLASSIFY ON: 08-15-2033

~~UNCLASSIFIED~~
~~NON-RECORD~~

Here is the opening EC for the Seattle Case.

SSA [redacted]
Operational Technology Division
Digital Evidence Section
Cryptologic and Electronic Analysis Unit
Software Development Group
[redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b6
b7C
b2

b6
b7C

-----Original Message-----
From: [redacted]
Sent: Thursday, June 07, 2007 5:12 PM
To: [redacted]
Cc: [redacted]
Subject: 288A-SE-93709

~~UNCLASSIFIED~~
~~NON-RECORD~~

158nbs01.ec (15 KB)

[redacted]

b1
(S)

SA [redacted]
FBI Seattle
[redacted]

b6
b7C
b2

~~UNCLASSIFIED~~

~~UNCLASSIFIED~~

~~SECRET~~

[redacted]

b6
b7C

From: [redacted]
Sent: Friday, June 08, 2007 12:37 PM
To: [redacted]
Cc:

Subject: RE: Second IP Address

~~UNCLASSIFIED~~
NON-RECORD

DATE: 08-18-2008
CLASSIFIED BY 60322uclp/stp/rds
REASON: 1.4 (c)
DECLASSIFY ON: 08-18-2033

(S)

[redacted]

b1

[redacted]

Can you confirm your fax number and I will get the emails to you also.

b6
b7C

Thanks for your help.

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, June 08, 2007 4:37 AM
To: [redacted]
Cc:
Subject: RE: Second IP Address

b6
b7C

~~UNCLASSIFIED~~
NON-RECORD

[redacted]

[redacted] out today but I am in and available to help. Our fax number here is [redacted] Thanks --

b6
b7C
b2

[redacted]

SSA [redacted]
Behavioral Analysis Unit 1
CIRG/NCAVC

[redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b6
b7C

-----Original Message-----
From: [redacted]
Sent: Thursday, June 07, 2007 11:09 PM
To: [redacted]
Cc:
Subject: Second IP Address

~~SECRET~~

~~UNCLASSIFIED~~
~~NON-RECORD~~

All,

(S) [redacted] b1

Thanks, [redacted]

SSA [redacted] b6 b7C
Seattle Field Office
Cyber Squad 11 b2
[redacted]

~~UNCLASSIFIED~~

~~UNCLASSIFIED~~

~~UNCLASSIFIED~~

~~SECRET~~

[redacted]

From: [redacted]
Sent: Friday, June 08, 2007 11:02 AM
To: [redacted]
Subject: FW: 288A-SE-93709

b6
b7C

DATE: 08-18-2008
CLASSIFIED BY 60322uclp/stp/rds
REASON: 1.4 (c)
DECLASSIFY ON: 08-18-2033

~~UNCLASSIFIED~~
~~NON-RECORD~~

[redacted]

b6
b7C

You are assigned this case. Please keep me updated. Thanks!

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, June 08, 2007 10:51 AM
To: [redacted]
Cc: [redacted]
Subject: FW: 288A-SE-93709

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b6
b7C

~~UNCLASSIFIED~~
~~NON-RECORD~~

[redacted] - Here is the Opening EC we forwarded to [redacted] yesterday. Thanks, [redacted]

b6
b7C

-----Original Message-----
From: [redacted]
Sent: Thursday, June 07, 2007 2:12 PM
To: [redacted]
Cc: [redacted]
Subject: 288A-SE-93709

b6
b7C

~~UNCLASSIFIED~~
~~NON-RECORD~~

158nbs01.ec (15 KB)

b1

[redacted] (S)

SA [redacted]
FBI Seattle

[redacted]

b6
b7C
b2

~~SECRET~~

[redacted]

From: [redacted]
Sent: Friday, June 08, 2007 11:01 AM
To: DICLEMENTE, ANTHONY P. (OTD) (FBI)
Subject: RE: UR5214/SE/THREAT INVESTIGATION

b6
b7C

DATE: 08-18-2008
CLASSIFIED BY 60322uclp/stp/rds
REASON: 1.4 (c)
DECLASSIFY ON: 08-18-2033

~~UNCLASSIFIED~~
~~NON-RECORD~~

We're on it. Will advise with updates.

-----Original Message-----
From: DICLEMENTE, ANTHONY P. (OTD) (FBI)
Sent: Friday, June 08, 2007 10:02 AM
To: [redacted]
Cc:
Subject: FW: UR5214/SE/THREAT INVESTIGATION

b6
b7C

~~UNCLASSIFIED~~
~~NON-RECORD~~

[redacted]

Pls reach out to Seattle Field Office and offer CEAU assistance relative to CIPAVs and advise.

b6
b7C
b2

Anthony P. DiClemente
Chief, Electronic Surveillance Technology Section
Operational Technology Division
[redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

-----Original Message-----
From: MOTTA, THOMAS GREGORY (OTD) (FBI)
Sent: Friday, June 08, 2007 9:17 AM
To: [redacted]
Cc:
Subject: FW: UR5214/SE/THREAT INVESTIGATION

b6
b7C

~~UNCLASSIFIED~~
~~NON-RECORD~~

(S) [redacted]

b1

Thos. Gregory Motta
Section Chief, Digital Evidence Section (DES)
Operational Technology Division (OTD)
Engineering Research Facility
[redacted]

b2

[redacted] b2

-----Original Message-----
From: [redacted] b6 b7C
Sent: Friday, June 08, 2007 12:38 AM
To: [redacted] MOTTA, THOMAS GREGORY (OTD) (FBI)
Subject: FW: UR5214/SE/THREAT INVESTIGATION

UNCLASSIFIED
NON-RECORD

UNCLASSIFIED
NON-RECORD

Being forwarded for your information is Urgent Report 5214 from FBI-Seattle regarding email bomb threats.

SSA [redacted] b6 b7C
Watch Supervisor - SIOC
[redacted] b2

-----Original Message-----
From: [redacted] b6 b7C
Sent: Thursday, June 07, 2007 11:46 PM
To: FBI_URGENT REPORTS
Cc: SE All Supervisors
Subject: UNSUB TIMBERLINE HIGH SCHOOL - VICTIM, COMPUTER INTRUSION - THREAT; 288A-SE-93709

UNCLASSIFIED
NON-RECORD

Please see the attached Urgent Report. If you have any questions, please feel free to contact me.

[redacted] b6 b7C

<< File: 158brf02.ec >>

[redacted] b6 b7C
A/ASAC Seattle Division
SSA - Squad 5
Gang/Criminal Enterprise Program;
Organized Crime Program;
Violent Crimes Program;
[redacted] b2

UNCLASSIFIED

UNCLASSIFIED

[redacted]

From: [redacted]
Sent: Friday, June 08, 2007 10:53 AM
To: [redacted]
Cc:
Subject: CIPAV and Local Info

DATE: 08-18-2008
CLASSIFIED BY 60322uclp/stp/rds
REASON: 1.4 (c)
DECLASSIFY ON: 08-18-2033

b6
b7C

SENSITIVE BUT ~~UNCLASSIFIED~~
NON-RECORD

(S)

[redacted]

b1

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b1

(S)

b1

~~SENSITIVE BUT UNCLASSIFIED~~

~~SECRET~~

[redacted]

From: [redacted]
Sent: Thursday, May 31, 2007 12:52 PM
To: [redacted]
Cc:
Subject: [redacted] (S)

b6
b7C
b1

~~**SENSITIVE BUT UNCLASSIFIED**~~
NON-RECORD

DATE: 08-18-2008
CLASSIFIED BY 60322uclp/stp/rds
REASON: 1.4 (c)
DECLASSIFY ON: 08-18-2033

Hi, [redacted] As promised, here's a copy of the OTD STE policy, including the LEGAT and OPS Plan ECs mentioned in the policy:

STE Policy.WPD (52 KB) | Legat EC.wpd (17 KB) | OPERATIONS PLAN.wpd (8 KB)

Read this guidance in context. A lot of it is written for overseas deployment of physical equipment and personnel at the request of the foreign government. Disregard those entries that don't make sense to your situation.

[redacted]

b1

Contrary to what I told you, please address the EC to the CEAU Chief, SSA [redacted]

Good talking with you!

[redacted]

b6
b7C

~~**SENSITIVE BUT UNCLASSIFIED**~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

CEAU Assistance to Seattle Case:

UNSUB(s);
TIMBERLINE SCHOOL DISTRICT (VICTIM);
COMPUTER INTRUSION – INTERNET EXTORTION

Background

On June 6, 2007, the Seattle Division was contacted by the Lacey Police Department (LPD), Lacey, WA, regarding numerous bomb threats and Distributed Denial of Service (DDOS) attacks received at the Timberline School District, Lacey, WA. The threats began on May 30, 2007 and persisted through June 4, 2007. The threats necessitated the daily evacuation of Timberline High School. The LPD and the Washington State Patrol (WSP) performed school evacuations and bomb sweeps with negative results. Parents and school district employees informed local television stations and newspapers, which aired the story on June 6, 2007. As a result, the LPD requested investigative assistance from the Northwest Cyber Crime Task Force (NCCTF), headed by the FBI Seattle Division. In turn, the Seattle Field Office requested assistance from the OTD/CEAU to attempt to geo-physically locate the UNSUB(s).

Assistance Provided

CEAU deployed a Computer Internet Protocol Address Verifier (CIPAV) to a MySpace account identified as possibly belonging to the UNSUB. The CIPAV returned several IP addresses, one of which resolved back to Comcast Cable in Seattle, Washington. Subscriber information obtained from Comcast led to the issuing of a search and arrest warrant. A 15 year old male student from Timberline High School was taken into custody without incident at his home at approximately 2 A.M. June 14, 2007. The minor confessed to issuing the bomb threats. Future bomb threats, dated June 14, 2007, were found on the minor's computer. The minor's computer equipment was seized and the arrest was made without incident. Following an interview with the minor, the LPD was able to solve another threat case, as the minor confessed to issuing telephone death threats to teachers and others, including his parents, earlier in 2007.

Pittsburgh II Investigation (Different case then original ongoing one)

- 01/04/2007 - SPU referred case to OTD/CEAU
- 01/31/2007 - ITOS requests OTD/CEAU if remote computer attack can be conducted against target
- 02/07/2007 - SPU contacted CEAU to offer assistance regarding case. CEAU advised that it may require [redacted] which falls in SPU's arena. If so, CEAU will coordinate with SPU for the task. b2 b7E
- Present - Per Case Agent, CEAU advised Pittsburgh that they could assist with [redacted] SPU has not heard anything from OTD regarding this.

Cincinnati Investigation

[redacted] Acting Unit Chief, Special Technologies Operations Unit (STOU) was contacted on the evening of February 15, 2007 by Special Agent [redacted] (Squad 13 - Cincinnati Division) requesting urgent support . SA [redacted] advised that he was working on a case (288A-CI-76037-WB) in which he needed immediate assistance from STOU in analyzing data obtained from a Computer and Internet Protocol Address Identifier ("CIPAV") inserted in five different [redacted] b6 b7C b2 b7D b7E

Acording to the Cincinnati's EC, "The CIPAV was previously exposed to hackers from 01/30/2007 to 02/09/2007 but no information was gathered because [redacted]

"During the period of the current search warrant, the Unsub hacker(s) accessed [redacted] *on 02/13/2007 at 12:23:08 Eastern Standard Time ("EST").* ***The Unsub(s) then proceeded to visit the site 29 more times. In these instances, the CIPAV did not deliver its' payload because of system incompatibility.*** On 02/15/2007 at 5:29:21 EDT, the system was able to deliver a CIPAV and the CIPAV returned data."

SA [redacted] requested STOU immediately begin analyzing all data recovered by the CIPAV and continue to perform analysis on an ongoing basis until the termination of CIPAV operations on 02/22/2007. SA [redacted] expressed the valid concern that the Unsub hackers would be "spooked" [redacted] According to SA [redacted] the hackers are responsible for [redacted] b2 b7E b6 b7C

STOU engineers immediately engaged in the case and began providing data back to SA [redacted] the very next day. STOU continued to provide daily support until the analysis was complete.