

[redacted] (OTD) (FBI)

From: [redacted] (OTD) (FBI)
Sent: Tuesday, July 24, 2007 3:57 PM
To: [redacted] (OTD) (FBI)
Subject: FW: FOIA request from Wired News

b6
b7C

UNCLASSIFIED
NON-RECORD

FYI.

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

b6
b7C
b2

-----Original Message-----

From: [redacted] (SE) (FBI)
Sent: Tuesday, July 24, 2007 3:54 PM
To: [redacted] (CyD) (FBI); [redacted] (OTD) (FBI)
Subject: FW: FOIA request from Wired News

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted] and [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]

-----Original Message-----

From: [redacted] (SE) (FBI)
Sent: Tuesday, July 24, 2007 10:52 AM
To: [redacted] (RMD) (FBI)
Cc: [redacted] (SE) (FBI); [redacted] (SE) (FBI); [redacted] (SE) (FBI)
Subject: FW: FOIA request from Wired News

b6
b7C

UNCLASSIFIED
NON-RECORD

[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.

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

b6
b7C
b2

-----Original Message-----

From: [redacted] (SE) (FBI)
Sent: Monday, July 23, 2007 4:18 PM
To: [redacted] (SE) (FBI); [redacted] (SE) (FBI)
Cc: [redacted] (SE) (FBI)
Subject: FW: FOIA request from Wired News

UNCLASSIFIED
NON-RECORD

b6
b7C

-----Original Message-----

From: [redacted] (SE) (FBI)
Sent: Monday, July 23, 2007 12:07 PM
To: [redacted] (SE) (FBI)
Subject: FW: FOIA request from Wired News

UNCLASSIFIED
NON-RECORD

-----Original Message-----

From: [redacted] (RMD) (FBI)
Sent: Monday, July 23, 2007 11:56 AM
To: [redacted] (SE) (FBI)
Subject: FOIA request from Wired News

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.

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."

b6
b7C

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

Thanks for your assistance.

[redacted]
Legal Administrative Specialist

UNCLASSIFIED

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (OTD) (FBI)
Sent: Tuesday, July 24, 2007 3:25 PM
To: [redacted] (OTD) (FBI)
Subject: RE: SF Newspaper Ad Response

b6
b7C

SECRET
RECORD 134M

Thanks for info

-----Original Message-----

1-Orig [redacted] (OTD) (FBI)
nal i Tuesday, July 24, 2007 3:21 PM
MOi [redacted] (OTD) (FBI)
nesDaA i FW: SF Newspaper Ad Response
VrIO- SIAai High

b6
b7C

SECRET
RECORD [redacted]

b2

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

b6
b7C
b2

-----Original Message-----

1-Orig [redacted] (OTD) (FBI)
nal i Tuesday, July 24, 2007 3:14 PM
MOi [redacted] (OTD) (FBI)
nesDaA i FW: SF Newspaper Ad Response
VrIO- SIAai High

b6
b7C

SECRET
RECORD [redacted]

b2

fyi

-----Original Message-----

1-Orig [redacted] (OTD) (FBI)
nal i Friday, July 20, 2007 5:00 PM
MOi [redacted] (OTD) (FBI)
nesDaA i FW: SF Newspaper Ad Response
VrIO- SIAai High

b6
b7C

SECRET
RECORD [redacted]

DATE: 10-15-2008
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 10-15-2033

b2

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

1

~~SECRET~~

~~SECRET~~

Please see below if you haven't already.

Regards,

[Redacted]

-----Original Message-----

1-Orig [Redacted] (CD) (FBI)
nal i Monday, July 16, 2007 4:55 PM
MOi [Redacted] (CD) (FBI) [Redacted] (CD) (FBI)
nesDaA i FW: SF Newspaper Ad Response

b6
b7C

SECRET
RECORD [Redacted]

[Redacted]

-----Original Message-----

1-Orig [Redacted] (HO) (FBI)
nal i Monday, July 16, 2007 4:54 PM
MOi [Redacted] (CD) (FBI)
nesDaA i RE: SF Newspaper Ad Response

b6
b7C

SECRET
RECORD [Redacted]

[Redacted]

My replacements are [Redacted]

[Redacted]

SSA [Redacted]
Houston Division
Squad CI-3

[Redacted] (Office)
[Redacted] (Blackberry)

b2

-----Original Message-----

1-Orig [Redacted] (CD) (FBI)
nal i Monday, July 16, 2007 3:34 PM
MOi [Redacted] (OTD) (FBI) [Redacted] (HO) (FBI)
nesDaA i FW: SF Newspaper Ad Response

SECRET
RECORD [Redacted]

[Redacted] and [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-----

1-Orig [Redacted] (NY) (FBI)
nal i Monday, July 16, 2007 1:26 PM
MOi [Redacted] (NY) (FBI); [Redacted] (NY) (FBI); [Redacted] (NY) (FBI); [Redacted] (NY) (FBI);
[Redacted] (NY) (FBI); [Redacted] (NY) (FBI); [Redacted] (NY) (FBI); [Redacted] (NY) (FBI);
[Redacted] (NY) (FBI); [Redacted] (CD) (FBI); [Redacted] (NY) (FBI); [Redacted] (NY) (FBI); [Redacted] (NY) (FBI);

~~SECRET~~

~~SECRET~~

nesDaA i FW: SF Newspaper Ad Response

SECRET
RECORD [redacted]

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

[redacted]

-----Original Message-----

1-Orig [redacted] (CG) (FBI)
nal i Monday, July 16, 2007 12:50 PM
MOi [redacted] (LA) (FBI); [redacted] (CD) (FBI); [redacted] (HO) (FBI); [redacted] (WF) (FBI); [redacted] (FBI); [redacted] (NY) (FBI); [redacted] (CD) (FBI); [redacted] (SF) (FBI)

nesDaA i RE: SF Newspaper Ad Response

SECRET
RECORD [redacted]

b2

[Large redacted block]

b1
(S)

SSA [redacted]
[redacted]

b6
b7C
b2

-----Original Message-----

1-Orig [redacted] (LA) (FBI)
nal i Monday, July 16, 2007 11:38 AM
MO [redacted] (CD) (FBI); [redacted] (HO) (FBI); [redacted] (CG) (FBI); [redacted] (WF) (FBI); [redacted] (NY) (FBI); [redacted] (CD) (FBI); [redacted] (SF) (FBI)

nesDaA i SF Newspaper Ad Response

SECRET
RECORD [redacted]

Gents:

b1

(S)

[Large redacted block]

[redacted]

SSA [redacted]
FBI Los Angeles Squad CI-2

[redacted] (STE)
[redacted] (cell)
[redacted] (JWICS)
[redacted] (SIPRNET)

b6
b7C
b2

~~SECRET~~

~~SECRET~~

~~(Internet Cafe)~~

b2
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~~

~~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~~

~~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~~

~~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~~

~~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~~

~~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
SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (OTD) (FBI) b6
Sent: Tuesday, July 24, 2007 8:29 AM b7C
To: [redacted] (FR) (FBI)
Cc: [redacted] (FR) (FBI); [redacted] (OTD) (FBI); [redacted]
Subject: (OTD) (FBI)
RE: CIPAV?

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

CIPAV is handled by the unit next door to us, the Cryptologic and Electronic Analysis Unit (CEAU). Their UC is [redacted] and the SSA over that program is [redacted]. I have cc'd them on this e-mail.

[redacted]

b2
b6
b7C

[redacted]

SSA [redacted]
Acting Unit Chief
Data Intercept Technology Unit

b6
b7C

[redacted] (STU)

-----Original Message-----

From: [redacted] (FR) (FBI)
Sent: Tuesday, July 24, 2007 6:27 AM
To: [redacted] (OTD) (FBI)
Cc: [redacted] (FR) (FBI)
Subject: CIPAV?

b6
b7C
b2

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Hello [redacted]

I am embarrassed to be approaching you again with a request from the Germans (after your previous help and offers of assistance that have not yet been follow-ed up on by our German colleagues), but they now have asked us about CIPAV (Computer Internet Protocol Address Verifier) software, allegedly used by the Bu?

[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]
Assistant Legal Attaché
Frankfurt, Germany
[redacted]

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

[redacted] (OTD) (FBI)

b6
b7C

From: [redacted] (OTD) (FBI)
Sent: Wednesday, July 18, 2007 5:35 PM
To: [redacted] (SE) (FBI)
Cc: [redacted] (OTD) (FBI); DICLEMENTE, ANTHONY P. (OTD) (FBI); [redacted]
[redacted] (OTD) (FBI)
Subject: Seattle CIPAV Case

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
b7C

[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.

[redacted]

Unit Chief
Cryptologic and Electronic Analysis Unit (CEAU)

SENSITIVE BUT UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-12-2008 BY 60322UC/LP/STP/gjg

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (OTD) (FBI)
Sent: Monday, July 16, 2007 5:25 PM
To: [redacted] (NY) (FBI)
Subject: FW: [redacted]

b6
b7C

b1

(S)

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

[redacted]

Please read the email from the bottom up.

SSA [redacted]
Operational Technology Division
Data Acquisition and Intercept Section
Cryptologic and Electronic Analysis Unit
Software Development Group

b6
b7C
b2

[redacted] (desk)
[redacted] (cell)
[redacted] (fax-unclass)

b6
b7C

-----Original Message-----

From: [redacted] (OGC) (FBI)
Sent: Monday, July 16, 2007 4:33 PM
To: [redacted] (OTD) (FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OGC) (FBI); [redacted] (OTD) (FBI); [redacted] (OTD) (FBI)
Subject: RE: [redacted]

b1

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

(S)

[redacted]

b1

(S)

Assistant General Counsel
Science and Technology Law Unit
Office of the General Counsel
Federal Bureau of Investigation
Ph - [redacted]
Cell [redacted]
Ph (Secure) - [redacted]
Fax - [redacted]

b6
b7C
b2

-----Original Message-----

From: [redacted] (OTD) (FBI)
Sent: Monday, July 16, 2007 4:30 PM
To: [redacted] (OGC) (FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OGC) (FBI)
Subject: RE: [redacted]

b6
b7C

b1

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

(S)

DATE: 09-12-2008
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 09-12-2033

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

[redacted] the pony we sent stated

(S) [redacted] b1

[redacted]

b2
b7E

(S)

(S)

[redacted]

Information Technology Specialist
Operational Technology Division

Office [redacted]
Mobile [redacted]
Pager [redacted]

b6
b7C
b2

-----Original Message-----

b6
b7C

From: [redacted] (OGC) (FBI)
Sent: Monday, July 16, 2007 3:52 PM
To: [redacted] (OTD) (FBI); [redacted] (OTD) (FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OTD) (FBI)
Subject: [redacted]

b1

SENSITIVE BUT UNCLASSIFIED (S)
NON-RECORD

[redacted]

(S) [redacted] Once again the case agent and/or the AUSA went their own direction [redacted]

b2
b7E

search would be done with the assistance of [redacted]

[redacted]

(S) [redacted] b1

It may be that the case agent believes that he can get sufficient evidence from [redacted] Maybe but if not, to get more details about the target computer, a second order will be necessary. I still suggest a

b2
b7E

(S) [redacted]

[redacted]

Assistant General Counsel
Science and Technology Law Unit
Office of the General Counsel
Federal Bureau of Investigation

Ph - [redacted]
Cell [redacted]
Ph (Secure) - [redacted]
Fax - [redacted]

b2
b6
b7C

SENSITIVE BUT UNCLASSIFIED

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (OTD) (FBI)
Sent: Monday, July 16, 2007 5:06 PM
To: [redacted] (OTD) (FBI)
Cc: [redacted] (OTD) (FBI)
Subject: [redacted]

b6
b7C

b1

(S)

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

What are we going to do here?

-----Origin | Message-----

From: [redacted] (OTD) (FBI)
Sent: Monday, July 16, 2007 4:35 PM
To: [redacted] (OGC) (FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OGC) (FBI); [redacted] (OTD) (FBI); [redacted] (OTD)
Subject: RE: Re: [redacted]

b6
b7C

b1

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

(S)

I think we have a problem.

J...

[redacted]
Information Technology Specialist
Operational Technology Division
Office - [redacted]
Mobile - [redacted]
Pager - [redacted]

b6
b7C
b2

-----Origin | Message-----

From: [redacted] (OGC) (FBI)
Sent: Monday, July 16, 2007 4:33 PM
To: [redacted] (OTD) (FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OGC) (FBI); [redacted] (OTD) (FBI); [redacted] (OTD)
Subject: RE: [redacted]

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

(S)

b1

[redacted] (S)
[redacted]
Assistant General Counsel
Science and Technology Law Unit
Office of the General Counsel
Federal Bureau of Investigation
Ph - [redacted]
Cell - [redacted]
Ph (Secure) - [redacted]
Fax - [redacted]

DATE: 09-29-2008
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 09-29-2033

b6
b7C
b2

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

-----Origin | Mess ge-----

From: [redacted] (OTD) (FBI)
Sent: Monday, July 16, 2007 4:30 PM
To: [redacted] (OGC) (FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OGC) (FBI)
Subject: RE: [redacted]

b1
b6
b7C

~~SENSITIVE BUT UNCLASSIFIED~~ (S)
~~NON-RECORD~~

[redacted] the pony we sent stated

(S)

[redacted]

(S)

[redacted]

b1
b7E

[redacted]
Information Technology Specialist
Operational Technology Division
Office - [redacted]
Mobile - [redacted]
Pager - [redacted]

b6
b7C
b2

b6
b7C

-----Origin | Mess ge-----

From: [redacted] (OGC) (FBI)
Sent: Monday, July 16, 2007 3:52 PM
To: [redacted] (OTD) (FBI); [redacted] (OTD) (FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted]
Subject: [redacted]

b1

~~SENSITIVE BUT UNCLASSIFIED~~ (S)
~~NON-RECORD~~

b6
b7C

[redacted]
Once again the case agent and/or the AUSA went their own direction [redacted]

b1

(S)

[redacted]

(S)
(S)

[redacted]

It may be that the case agent believes that he can get sufficient evidence from [redacted] Maybe but if not, to get more details about the target computer, a second order will be necessary. I still suggest a search [redacted]

b1

(S)

[redacted]
Assistant General Counsel

b6
b7C

~~SECRET~~

Science and Technology Law Unit
Office of the General Counsel
Federal Bureau of Investigation
Ph - [redacted]
Cell - [redacted]
Ph (Secure) - [redacted]
Fax - [redacted]

b6
b7C
b2

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SECRET~~

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (OGC) (FBI)
Sent: Thursday, July 12, 2007 10:17 AM
To: [redacted] (OTD) (FBI)
Cc: [redacted] (OTD) (FBI)
Subject: FW: Lead 12/22/2005 - Banner

b6
b7C

SECRET
RECORD 288B-SI-54759

Attached is the banner that [redacted] and [redacted] designed back in late 2005/early 2006.

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

b6
b7C
b2

-----Original Message-----

From: [redacted] (OGC) (FBI)
Sent: Friday, March 10, 2006 3:31 PM
To: [redacted] (OTD) (FBI); [redacted] (CyD) (FBI)
Cc: [redacted] (OGC) (FBI)
Subject: FW: Lead 12/22/2005 - Banner

b6
b7C

SECRET
RECORD 288B-SI-54759

b1

(S)

[Large redacted area]

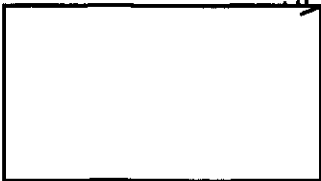
Assuming that [redacted] concurs, request that you approve the use of this banner. You have the background and email strings associated with this request but if it will be helpful, I'll package them and send them to you. I've attached the proposed banner for your convenience.

DATE: 10-16-2008
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 10-16-2033

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~



(S)

b1



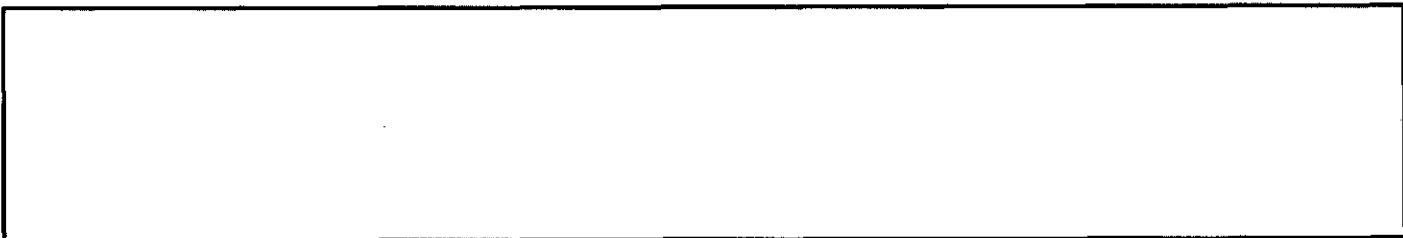
Assistant General Counsel
Science and Technology Law Unit
Office of the General Counsel
Federal Bureau of Investigation
Phone [Redacted]
Fax [Redacted]

b6
b7C
b2

-----Original Message-----

From: [Redacted] (OTD)
Sent: Friday, March 10, 2006 2:14 PM
To: [Redacted] (OGC) (FBI)
Subject: RE: Lead 12/22/2005 - Banner

SECRET
RECORD 288B-SI-54759



(S)
b1

SSA [Redacted]
Cryptologic & Electronic Analysis Unit
Digital Evidence Section, Operational Technology Division
Quantico, VA



o
p
f
secure voice
secure fax

b6
b7C
b2

-----Original Message-----

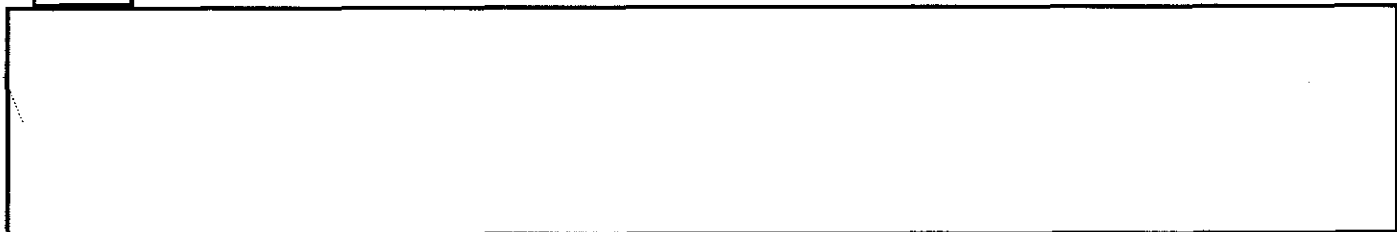
From: [Redacted] (OGC) (FBI)
Sent: Friday, March 10, 2006 11:31 AM
To: [Redacted] (OTD)
Subject: FW: Lead 12/22/2005 - Banner

SECRET
RECORD 288B-SI-54759

b1



(S)



~~SECRET~~

~~SECRET~~

(S) [Redacted]

b1

Thanks

[Redacted]
Assistant General Counsel
Science and Technology Law Unit
Office of the General Counsel
Federal Bureau of Investigation
Phone [Redacted]
Fax - [Redacted]

b6
b7C
b2

-----Original Message-----

From: [Redacted] (OGC) (FBI)
Sent: Friday, March 10, 2006 11:13 AM
To: [Redacted] (OGC) (FBI)
Subject: RE: Lead 12/22/2005 - Banner

SECRET
RECORD 288B-SI-54759

(S) [Redacted]

b1

Let me know if you agree, feel otherwise, etc.

Thanks,
[Redacted]

-----Original Message-----

From: [Redacted] (OGC) (FBI)
Sent: Friday, March 10, 2006 8:32 AM
To: MOTTA, THOMAS GREGORY (OGC) (FBI); [Redacted] (OGC) (FBI)
Subject: RE: Lead 12/22/2005 - Banner

SECRET
RECORD 288B-SI-54759

b6
b7C
b2

[Redacted]

You have seen this. I can send you a copy of your emails if it will help.

[Redacted]
Assistant General Counsel
Science and Technology Law Unit
Office of the General Counsel
Federal Bureau of Investigation
Phone [Redacted]
Fax - [Redacted]

~~SECRET~~

~~SECRET~~

-----Original Message-----

From: [redacted]
Sent: Thursday, March 09, 2006 5:28 PM
To: [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: FW: Lead 12/22/2005 - Banner

SECRET
RECORD 288B-SI-54759

b6
b7C

I had previously referred [redacted] call to [redacted] while you were away. [redacted] has had extensive Banner review experience including some prior DoD Banners. [redacted] can you review and comment.

Thanks.

[redacted]

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

[redacted]

Associate General Counsel - Unit Chief
Science & Technology Law Unit
Engineering Research Facility
Bldg 27958A, Room A-207
Quantico, VA 22135

b6
b7C
b2

Tel. [redacted]
Fax. [redacted]

-----Original Message-----

From: [redacted] (OGC) (FBI)
Sent: Thursday, March 09, 2006 2:51 PM
To: [redacted] (SI) (FBI)
Cc: [redacted] (CyD) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: RE: Lead 12/22/2005 - Banner

b6
b7C

SECRET
RECORD 288B-SI-54759

b1

(S) [redacted]
[redacted]

(S) [redacted]

[redacted]
Assistant General Counsel
Science and Technology Law Unit
Office of the General Counsel
Federal Bureau of Investigation
Phone - [redacted]
Fax - [redacted]

b6
b7C
b2

~~SECRET~~

~~SECRET~~

-----Original Message-----

From: [redacted] (SI) (FBI)
Sent: Thursday, January 05, 2006 4:21 PM
To: [redacted] (OGC) (FBI)
Subject: RE: Lead 12/22/2005

b6
b7C

SECRET
RECORD 288B-SI-54759

[redacted]

AFOSI has not gotten the "Official" approval from the appropriate Air Force General yet to deploy CIPAV. The General asked for an official OPS plan to include CIPAV basic information, how we will gather and share the appropriate data and how long we expect to deploy the tool. He requested the OPS plan include the FBI's recommended banner changes before he approves so his DOD attorneys can review our changes before he signs off.

I know it's a chicken or egg thing.....but he wants to see our recommendations before signing off. Thanks again.

SA [redacted]
U.S. Bank Building
6701 North Illinois
Suite 200
Fairview Heights, Illinois 62208
Tel: [redacted]
Fax: [redacted]

b6
b7C
b2

-----Original Message-----

From: [redacted] (OGC) (FBI)
Sent: Thursday, January 05, 2006 2:24 PM
To: [redacted] (SI) (FBI)
Cc: [redacted] (OTD); [redacted] (OGC) (FBI)
Subject: RE: Lead 12/22/2005

SECRET
RECORD 288B-SI-54759

[redacted]

We are putting the final touches on the draft Banner language now but I will have to coordinate the language thru OGC before I can provide it to you via EC. Before I take the next step I need to know that the Air Force has agreed to make the recommended changes and to use of the CIPAV tool. Please let me know ASAP.

Thanks

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

b6
b7C
b2

-----Original Message-----

From: [redacted] (SI) (FBI)
Sent: Thursday, December 29, 2005 12:57 PM

~~SECRET~~

~~SECRET~~

To: [redacted] (OGC) (FBI)
Subject: RE: Lead 12/22/2005

SECRET
RECORD 288B-SI-54759

Yes, that is the only thing we have found to date.

SA [redacted]
U.S. Bank Building
6701 North Illinois
Suite 200
Fairview Heights, Illinois 62208
Tel: [redacted]
Fax: [redacted]

b6
b7C
b2

-----Original Message-----

From: [redacted] (OGC) (FBI)
Sent: Thursday, December 29, 2005 7:24 AM
To: [redacted] (SI) (FBI)
Subject: RE: Lead 12/22/2005

SECRET
RECORD 288B-SI-54759

[redacted]

Thanks and my understanding is that in your investigation you've determined that [redacted]

b2
b7E

[redacted]
Assistant General Counsel
Science and Technology Law Unit
Office of the General Counsel
Federal Bureau of Investigation
Phone - [redacted]
Fax - [redacted]

b6
b7C

-----Original Message-----

From: [redacted] (SI) (FBI)
Sent: Wednesday, December 28, 2005 7:41 PM
To: [redacted] (OGC) (FBI)
Subject: RE: Lead 12/22/2005

SECRET
RECORD 288B-SI-54759

[redacted] I am not sure about that. I'll be out of the office until next week and if you want me to check with the Air Force on it I will. [redacted]

b2
b7E

[redacted]

~~SECRET~~

~~SECRET~~

SA [redacted]
U.S. Bank Building
6701 North Illinois
Suite 200
Fairview Heights, Illinois 62208
Tel: [redacted]
Fax: [redacted]

-----Original Message-----

From: [redacted] (OGC) (FBI)
Sent: Wednesday, December 28, 2005 3:32 PM
To: [redacted] (SI) (FBI)
Subject: RE: Lead 12/22/2005

b6
b7C

SECRET
RECORD 288B-SI-54759

Thanks [redacted]

b2
b7E

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

-----Original Message-----

From: [redacted] (SI) (FBI)
Sent: Wednesday, December 28, 2005 3:56 PM
To: [redacted] (OGC) (FBI)
Subject: RE: Lead 12/22/2005

b6
b7C

SECRET
RECORD 288B-SI-54759

Good Afternoon [redacted]

b2
b7E

[redacted] I am not,
however, currently aware of that to be happening.

SA [redacted]
U.S. Bank Building
6701 North Illinois
Suite 200
Fairview Heights, Illinois 62208
Tel: [redacted]
Fax: [redacted]

b6
b7C
b2

-----Original Message-----

From: [redacted] (OGC) (FBI)
Sent: Wednesday, December 28, 2005 1:11 PM
To: [redacted] (SI) (FBI)
Subject: FW: Lead 12/22/2005

~~SECRET~~

~~SECRET~~

SECRET
RECORD 288B-SI-54759

[Redacted]

Now I have your EC officially. I'm coordinating as I type to get ideas from my colleagues. The concern seems to be that while we may be able to proceed

(S)

[Redacted]

b1

[Redacted]

Assistant General Counsel
Science and Technology Law Unit
Office of the General Counsel b6
Federal Bureau of Investigation b7C
Phone [Redacted] b2
Fax [Redacted]

-----Original Message-----

From: [Redacted] (OGC) (FBI)
Sent: Thursday, December 22, 2005 2:29 PM
To: [Redacted] (OGC) (FBI)
Cc: MOTTA, THOMAS GREGORY (OGC) (FBI); [Redacted] (OGC)
Subject: Lead 12/22/2005

Happy Holidays all,

Please find attached a lead for [Redacted] that has a deadline of 1/31/2006.

Thanks,

[Redacted] << File: 12222005.wpd >>

~~**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**~~

~~**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] (OTD) (FBI)

From: [redacted] (SI) (FBI)
Sent: Tuesday, July 10, 2007 6:24 PM
To: [redacted] (OTD) (FBI)
Subject: RE: CIPAV reminder

b6
b7C

UNCLASSIFIED
NON-RECORD

Per our conversation, we'll talk to you (and your engineers) at 3:30 pm EST (2:30 pm central)

-----Original Message-----

From: [redacted] (OTD) (FBI)
Sent: Tuesday, July 10, 2007 4:59 PM
To: [redacted] (SI) (FBI)
Subject: RE: CIPAV reminder

UNCLASSIFIED
NON-RECORD

How does 2pm EST sound?

SSA [redacted]
Operational Technology Division
Digital Evidence Section
Cryptologic and Electronic Analysis Unit
Software Development Group
[redacted] (desk)
[redacted] (cell)
[redacted] (fax-unclass)

b6
b7C
b2

-----Original Message-----

From: [redacted] (SI) (FBI)
Sent: Tuesday, July 10, 2007 5:31 PM
To: [redacted] (OTD) (FBI)
Subject: RE: CIPAV reminder

UNCLASSIFIED
NON-RECORD

Miscommunication. We thought you were calling us. What time works?

-----Original Message-----

From: [redacted] (OTD) (FBI)
Sent: Tuesday, July 10, 2007 4:15 PM
To: [redacted] (SI) (FBI)
Subject: RE: CIPAV reminder

b6
b7C

UNCLASSIFIED
NON-RECORD

Yes, I will be able to discuss the issues tomorrow. I waited patiently for you to call yesterday. Did I get my wires crossed? Was I suppose to call you or were you going to call me?

SSA [redacted]
Operational Technology Division

Digital Evidence Section
Cryptologic and Electronic Analysis Unit
Software Development Group

[redacted] (desk)
[redacted] (cell)
[redacted] (fax-unclass)

-----Original Message-----

From: [redacted] (SI) (FBI)
Sent: Tuesday, July 10, 2007 2:24 PM
To: [redacted] (OTD) (FBI)
Subject: FW: CIPAV reminder

UNCLASSIFIED
NON-RECORD

Are you going to be available to discuss these issues tomorrow?

b6
b7C
b2

-----Original Message-----

From: [redacted] (SI) (FBI)
Sent: Friday, July 06, 2007 1:13 PM
To: [redacted] (OTD) (FBI)
Subject: CIPAV reminder

UNCLASSIFIED
NON-RECORD

Per our discussion today, you are checking with you engineers and [redacted] regarding our matter here. We are going to talk again Monday assuming you get your answers (tentatively scheduled for after 2 pm). Call with questions.

[redacted]
D [redacted]
C [redacted]

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 07/05/2007

To: Seattle

Attn: SA [redacted]

Cyber

Attn: SSA [redacted]
C3IU-2

b6
b7C

From: Operational Technology Division/
Electronic Surveillance Technology Section/
Cryptologic and Electronic Analysis Unit

Approved By: [redacted]
DiClemente Anthony P

[redacted]
[redacted]

b6
b7C

Drafted By: [redacted]

Case ID #: [redacted] (Pending)
288E-SE-93709 (Pending)

b2

Title: CRYPTOLOGIC ELECTRONIC ANALYSIS UNIT (CEAU)
ASSISTANCE TO THE SEATTLE FIELD OFFICE

UNSUB(S);
TIMBERLINE SCHOOL DISTRICT (VICTIM);
COMPUTER INTRUSION - INTERNET EXTORTION

Synopsis: After Action Report for effectuating remote delivery of a Computer Internet Protocol Address Verifier (CIPAV) to geophysically locate a subject who has issued multiple bomb threats against a local high school.

Details: On 06/06/2007, 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 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 locating the UNSUB.

To: Seattle From: Operational Technology Division/
Re: [REDACTED] 07/05/2007

b2

OBJECTIVE

The objective of this operation was to deploy a CIPAV to locate the subject issuing bomb threats to the Timberline High School, Lacey, Washington. The CIPAV was deployed in the usual way.

SUMMARY OF EVENTS

Concurrence for the operation was obtained from Case Agent [REDACTED] and [REDACTED] Assistant United States Attorney, Western District of Washington. In addition, [REDACTED] Office of the General Counsel, concurred with the operation following his review of the affidavit and warrant, signed by James P. Donohue, United States Magistrate Judge, United States District Court, Western District of Washington, dated 6/12/2007.

b6
b7C

CONCLUSION

CEAU deployed a CIPAV to a MySpace account identified as possibly belonging to the UNSUB. The CIPAV returned several IP Addresses, one resolving back to Comcast Cable in Seattle, Washington. Subscriber 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. on 6/14/2007. The minor confessed to issuing the bomb threats. Bomb threats dated 6/14/2007, 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 clear another threat case, as the minor confessed to issuing telephone death threats to teachers and others, including his parents, earlier this year.

To: Seattle From: Operational Technology Division/
Re: [REDACTED] 07/05/2007

b2

LEAD(s):

Set Lead 1: (Action)

SEATTLE

AT SEATTLE, WA

Lead covered at OTD/ESTS/CEAU. Read and Clear

Set Lead 2: (Action)

CYBER

AT WASHINGTON, DC

Read and Clear.

◆◆

S:/DES/CEAU/Upload/AARSEATTLE06kld1407.wpd

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (OGC) (FBI) b6
Sent: Monday, July 02, 2007 10:52 AM b7C
To: [redacted] (SE) (FBI)
Cc: [redacted] (SE) (FBI); [redacted] (SE) (FBI); [redacted] (SE) (FBI); [redacted] (SE) (FBI)
Subject: RE: [redacted] (OTD) (FBI) b2
b7E

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

I spoke with [redacted] of our office on this issue. We agree that you probably should get a search warrant in order to conduct this investigation. It is just not well settled in the law that we can rely on the trespasser exception to the search requirement. I'm told that [redacted] has a pony for an affidavit for a situation such as this. It needs to be fairly detailed as to what we are going to do. I have copied [redacted] on this response. It was a [redacted] [redacted] [redacted] can refresh your memory if you don't know the one I am referring to. b6
b7C
b2
b7E

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

b6
b7C
b2

-----Original Message-----

From: [redacted] (SE) (FBI)
Sent: Monday, June 25, 2007 11:53 AM
To: [redacted] (O C) (FBI)
Cc: [redacted] (SE) (FBI); [redacted] (SE) (FBI); [redacted] (SE) (FBI)
Subject: RE: [redacted]

b6
b7C
b2
b7E

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Thanks [redacted] - Hoping to hear a decision soon. [redacted]
[redacted] Thanks for all your help. [redacted]

b2
b7E

SA [redacted]
FBI Seattle
[redacted] (Fax)
[redacted] (Nextel) DC: [redacted]
[redacted]

b6
b7C
b2

DATE: 02-24-2009
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 02-24-2034

-----Original Message-----

From: [redacted] (O C) (FBI)
Sent: Monday, June 25, 2007 7:55 AM
To: [redacted] (SE) (FBI)
Subject: [redacted]

b2
b7E

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

[Redacted]

(S)

[Redacted]

b1

been resolved by the courts. A colleague recently raised the same question with a DOJ attorney in the Criminal Division. The response was that they didn't have a written position on it, but they did think it would reduce the litigation risks associated with this type of action. Not a very good response. The attorney did mention that there is a pending case in the Eastern District of California that may answer this question, but who knows when that will be decided. There are two people I want to discuss this with, but they are both out this week. I'm afraid this is all I can tell you for now, but I will keep working it.

[Redacted]

Assistant General Counsel
Science and Technology Law Unit

Phone: [Redacted]

Secure phone [Redacted]

Fax: [Redacted]

b6
b7C
b2

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

AFFIDAVIT

1
2
3 STATE OF WASHINGTON
4 COUNTY OF KING

}
} ss:

5
6 Norman B. Sanders Jr., being duly sworn on oath, deposes and says:

7 1. I am a Special Agent for the Federal Bureau of Investigation ("FBI"), and
8 have been such for the past five years. Prior to becoming a Special Agent, I was
9 employed by the FBI as a Computer Forensic Examiner, for six and one-half years. I
10 am currently assigned to the Seattle Office's Cyber Crime Squad, which investigates
11 various computer, and Internet-related federal crimes.

12 2. My experience as an FBI Agent has included the investigation of cases
13 involving Computer Intrusions, Extortion, Internet Fraud, Identity Theft, Crimes
14 Against Children, Intellectual Property Rights, and other federal violations involving
15 computers and the Internet. I have also received specialized training and gained
16 experience in interviewing and interrogation techniques, arrest procedures, search
17 warrant applications, the execution of searches and seizures, cyber crimes computer
18 evidence identification, computer evidence seizure and forensic processing, and various
19 other criminal laws and procedures. I have personally participated in the execution of
20 arrest warrants and search warrants involving the search and seizure of computers and
21 electronic evidence, as well as paper documents and personal belongings.

22 3. I am an investigative or law enforcement officer of the United States
23 within the meaning of Section 2510(7) of Title 18, United States Code, in that I am
24 empowered by law to conduct investigations and to make arrests for federal felony
25 offenses.

26 4. Relative to this investigation, my duties include the investigation of
27 offenses including violations of Title 18, United States Code, Sections 875(c) (Interstate
28 Transmission of Communication Containing Threat to Injure), and 1030(a)(5)(A)(i) and

Affidavit of Norm Sanders for CIPAV
USAO# 2007R00791

1 (B)(iv) (Computer Intrusion Causing a Threat to Public Safety).

2 5. I submit this affidavit in support of the application of the United States for
3 a search warrant. This search warrant pertains to the Government's planned use of a
4 specialized technique in a pending criminal investigation. Essentially, if a warrant is
5 approved, a communication will be sent to the computer(s) being used to administer
6 www.myspace.com¹ ("MySpace") user account "Timberlinebombinfo".

7 The communication to be sent is designed to cause the above referenced
8 computer(s) to transmit data, in response, that will identify the computer(s) and/or the
9 user(s) of the computer(s). In this manner, the FBI may be able to identify the
10 computer(s) and/or user of the computer(s) that are involved in committing criminal
11 violations of United States Code²; specifically, Title 18, United States Code, Sections
12 875(c) (Interstate Transmission of Communication Containing Threat to Injure), and
13 1030(a)(5)(A)(i) and (B)(iv) (Computer Intrusion Causing a Threat to Public Safety).

14 More specifically, the United States is applying for a search warrant authorizing:

15
16 a. the use of a Computer & Internet Protocol Address³ ("IP address")

17
18 ¹ MySpace is a international free service that uses the Internet for online communication through
19 an interactive social network of photos, videos, weblogs, user profiles, blogs, e-mail, instant
20 messaging, web forums, and groups, as well as other media formats. MySpace users are capable of
21 customizing their user webpage and profile. Users are also capable of searching or browsing other
MySpace webpages and adding other users as "friends". If the person identified approves your
"friend" request, he or she will be added to your list of friends. Users are capable of sending MySpace
messages and posting comments on other user's MySpace webpages.

22 ² In submitting this request, the Government respectfully does not concede that a reasonable
23 expectation of privacy exists in the internet protocol address assigned by a network service provider or
24 other provider to a specific user and used to address and route electronic communications to and from
25 that user. Nor does the government concede that a reasonable expectation of privacy is abridged by the
use of this communication technique, or that the use of this technique to collect a computer's IP
address, MAC address or other variables that are broadcast by the computer whenever it is connected
to the Internet, constitutes a search or seizure.

26 ³ Conceptually, IP addresses are similar to telephone numbers, in that they are used to identify
27 computers that exchange information over the Internet. An IP address is a unique numeric address
28 used to direct information over the Internet and is a series of four numbers, each in the range 0-255,
separated by periods (e.g., 121.56.97.178). In general, information sent over the Internet must
contain an originating IP address and a destination IP address, which identify the computers sending

1 Verifier ("CIPAV") in conjunction with any computer that administers MySpace user
2 account "Timberlinebombinfo" (<http://www.myspace.com/timberlinebombinfo>) ,
3 without prior announcement within ten days from the date this Court authorizes the use
4 of the CIPAV;

5 b). that the CIPAV may cause any computer - wherever located - that
6 activates any CIPAV authorized by this Court (an "activating computer") to send
7 network level messages⁴ containing the activating computer's IP address and/or MAC
8 address,⁵ other environment variables, and certain registry-type information⁶ to a
9 computer controlled by the FBI;

10 c). that the FBI may receive and read within ten days from the date
11 this Court authorizes the use of the CIPAV, at any time of day or night, the information
12 that any CIPAV causes to be sent to the computer controlled by the FBI; and

13
14 and receiving the information. Section 216 of the USA Patriot Act (P.L. 107-56) amended 18 U.S.C.
15 §§3121 *et seq* to specifically authorize the recovery of "addressing" and "routing" information of
16 electronic As used here, a network-level message refers to an exchange of technical information
17 between computers. communications by a pen register/trap & trace order.

17 ⁴ Such messages work in established network protocols, determining, for example, how a given
18 communication will be sent and received. Every time a computer connected to a local area network
19 (LAN) or to the Internet connects to another computer on the LAN or the Internet, it broadcasts
20 network-level messages, including its IP address, and/or media access control (MAC) address, and/or
21 other "environment variables." A MAC address is a unique numeric address of the network interface
22 card in a computer. Environment variables that may be transmitted include: operating system type and
23 version, browser type and version, the language the browser is using, etc. These network-level
24 messages also often convey network addressing information, including origin and destination
25 information. Network-level messages are used to make networks operate properly, transparently, and
26 consistently.

23 ⁵ Computers that access, and communicate on LANs do so via a network interface card (NIC)
24 installed in the computer. The NIC is a hardware device and every NIC contains its own unique MAC
25 address. Every time a computer connected to a LAN communicates on the LAN, the computer
26 broadcasts its MAC address.

26 ⁶ As used here, "registry-type information" refers to information stored on the internal hard drive
27 of a computer that defines that computer's configuration as it relates to a user's profile. This
28 information includes, for example, the name of the registered owner of the computer and the serial
number of the operating system software installed. Registry information can be provided by a
computer connected to the Internet, for example, when that computer connects to the Internet to request
a software upgrade from its software vendor.

1 d). that, pursuant to 18 U.S.C. §3103a(b)(3), to satisfy the notification
2 requirement of Federal Rule of Criminal Procedure 41(f)(3), the FBI may delay
3 providing a copy of the search warrant and the receipt for any property taken until no
4 more than thirty (30) days after such time as the name and location of the owner or user
5 of the activating computer is positively identified or a latter date as the court may, for
6 good cause shown, authorize. Provision of a copy of the search warrant and receipt
7 may, in addition to any other methods allowed by law, be effectuated by electronic
8 delivery of true and accurate electronic copies (e.g. Adobe PDF file) of the fully
9 executed documents.

10 6. I am thoroughly familiar with the information contained in this Affidavit,
11 which I have learned through investigation conducted with other law enforcement
12 officers, review of documents, and discussions with computer experts. Because this an
13 application for a search warrant and pen register, not every fact known about the
14 investigation is set forth, but only those that are pertinent to the application. As a result
15 of the investigation, I submit there is probable cause to believe the MySpace
16 "Timberlinebombinfo" account, e-mail account "dougbriggs123@gmail.com"; e-mail
17 account "dougbrigs@gmail.com"; e-mail account "dougbriggs234@gmail.com"; e-mail
18 account "thisisfromitaly@gmail.com"; and e-mail account
19 "timberline.sucks@gmail.com" have been used to transmit interstate communications
20 containing threats to injure and involve computer intrusion causing a threat to public
21 safety in violation of Title 18, United States Code, Sections 875(c) and 1030(a)(5)(A)(i)
22 and (B)(iv). I further submit that there is probable cause to believe that using a CIPAV
23 in conjunction with the target MySpace account (Timberlinebombinfo) will assist in
24 identifying the individual(s) using the activating computer to commit these violations of
25 the United States Code.

26 7. In general, a CIPAV utilizes standard Internet computer commands
27 commonly used commercially over local area networks (LANs) and the Internet to
28 request that an activating computer respond to the CIPAV by sending network level

1 | messages, and/or other variables, and/or registry information, over the Internet⁷ to a
2 | computer controlled by the FBI. The exact nature of these commands, processes,
3 | capabilities, and their configuration is classified as a law enforcement sensitive
4 | investigative technique, the disclosure of which would likely jeopardize other on-going
5 | investigations and/or future use of the technique. As such, the property to be accessed
6 | by the CIPAV request is the portion of the activating computer that contains
7 | environmental variables and/or certain registry-type information; such as the
8 | computer's true assigned IP address, MAC address, open communication ports, list of
9 | running programs, operating system (type, version, and serial number), internet
10 | browser and version, language encoding, registered computer name, registered
11 | company name, current logged in user name, and Uniform Resource Locator (URL)
12 | that the target computer was previously connected to.

13 | 8. An Internet Service Provider (ISP) normally controls a range of several
14 | hundred (or even thousands) IP addresses, which it uses to identify its customers'
15 | computers. IP addresses are usually assigned "dynamically": each time the user
16 | connects to the Internet, the customer's computer is randomly assigned one of the
17 | available IP addresses controlled by the ISP. The customer's computer retains that IP
18 | address until the user disconnects, and the IP address cannot be assigned to another
19 | user during that period. Once the user disconnects, however, that IP address becomes
20 | available to other customers who connect thereafter. ISP business customers will
21 | commonly have a permanent, 24-hour Internet connection to which a "static" (i.e.,
22 | fixed) IP address is assigned. Practices for assigning IP addresses to Internet users
23 | vary, with many providers assigning semi-persistent numbers that may be allocated to a
24 | single user for a period of days or weeks.

26 | ⁷ The "Internet" is a global computer network, which electronically connects computers and
27 | allows communications and transfers of data and information across state and national boundaries. To
28 | gain access to the Internet, an individual utilizes an Internet Service Provider (ISP). These ISP's are
available worldwide.

1 e-mail from sender: "dougbriggs123@gmail.com". The Unknown Subject(s) (UNSUB)
2 stated in the e-mail "I will be blowing up your school Monday, June 4, 2007. There
3 are 4 bombs planted throughout timberline high school. One in the math hall, library
4 hall, main office and one portable. The bombs will go off in 5 minute intervals at 9:15
5 AM." In addition, the UNSUB(s) stated, "The email server of your district will be
6 offline starting at 8:45 am". The UNSUB(s) launched a Denial-of-Service (DOS)⁸
7 attack on the Lacey School District computer network, which caused over 24,000,000
8 hits on the system within a 24 hour period. School administrators ordered an
9 evacuation of the school on June 4, 2007.

10
11 b). On June 5, 2007, the UNSUB(s) sent an e-mail from
12 "dougbrigs@gmail.com" stating the following:

13 <<Read This ASAP>>

14 Now that the school is scared from yesturdays fake bomb threat
15 it's now time to get serious. One in a gym locker, the girls. It's
16 in a locker hidden under a pile of clothes. The other four I will
17 only say the general location. One in the Language Hall, One in
18 the math hall, One underneath a portable taped with strong
19 ducktape. This bomb will go off if any vibrations are felt. And
20 the last one, Is in a locker. It is enclosed in a soundproof package,
21 and litteraly undetectable. I have used a variety of chemicals to
22 make the bombs. They are all different kinds.

23 They will all go off at 10:15AM. Through remote detonation.
24 Good Luck. And if that fails, a failsafe of 5 minutes later.

25 The UNSUB(s) goes on to state:

26 Oh and for the police officers and technology idiots at
27 the district office trying to track this email and yesturdays email's
28 location. I can give you a hint. The email was sent over a newly made
29 gmail account, from overseas in a foreign country. The gmail account
30 was created there, and this email and yesturdays was sent from there.
31 So good luck talking with Italy about getting the identify of the person
32 who owns the 100Mbit dedicated server"

26
27 ⁸ A DOS attack is an Internet based computer attack in which a compromised system attacks a
28 single target, thereby causing a denial of service for users of the targeted computer system. The flood
29 of incoming messages to the target system essentially forces it to shut down, thereby denying service to
30 the system to legitimate users. The DOS attack is generally targeted at a particular network service,
31 such as e-mail or web access.

1 c). In another email from sender "dougbriggs234@gmail.com"
2 the UNSUB(s) states the following:

3 Hello Again. Seeing as how you're too stupid to trace the email back
4 lets get serious." [The UNSUB(s) mentions 6 bombs set to detonate
5 between 10:45-11:15 AM, and adds] Seriously, you are not going to catch
6 me. So just give up. Maybe you should hire Bill Gates to tell you that it
7 is coming from Italy. HAHAHA Oh wait I already told you that. So stop
8 pretending to be "tracing it" because I have already told you it's coming
9 from Italy. That is where trace will stop so just stop trying. Oh and this
10 email will be behind a proxy behind the Italy server.

11 d). School administrators ordered an evacuation of the school on June
12 5, 2007.

13 e). On June 6, 2007, Principle Dave Lehnis of Timberline High
14 School received an e-mail from sender: "dougbriggs911@gmail.com". The e-mail
15 contained the following text: "ENJOY YOUR LIFE ENDING".

16 f). In another e-mail from "dougbriggs911@gmail.com," the
17 UNSUB(s) states the following,

18 Well hello Timberline, today is June 6, 2007 and I'M just emailing you
19 today to say that school will blow up and that's final! There are 2 bombs this time
20 (Iran short on money to buy things at home depot). They will go off at exactly 10:45:00
21 AM. One is on located on a portable. And the other is somewhere else. Keep trying
22 to 'trace' this email. The only thing you will be able to track is that it came from
23 Italy. There is no other information that leads it back to the United States in any way
24 so get over it.
25 You should hire Bill Gates to track it for you. HAHAHAAAA. He will just tell you that
26 it came from over seas, so if you have close relations with the POPE you might get
27 some information. But other than that, have fun looking in Italy. :-)
28 Also, stop advising teachers to no show this email to classmates. Everyone would be
29 ammused by this email and I might stop if you do. Funny how I can trick you all into
30 thinking that I included my name to show that it isn't me, because who the hell would
31 put their name? Or is that just what I want you to think.
32 And yet again, this email was sent from overseas to a newly made email account that
33 has
34 already been deleted of all information by the time you read this email. Get your ass
35 on a plane to Italy if you want it to stop.

36 g). School administrators ordered an evacuation fo the school on June
37 6, 2007

38 h). On June 7, 2007, Timberline High School received an e-mail from
39 sender "thisisfromitaly@gmail.com." The UNSUB(s) states "There

1 are 3 bombs planted in the school and they're all different kinds. I
2 have premade these weeks in advance and tested the timers to make sure
3 they work to exact millisecond. Locking the doors is a good plan,
4 but too late."

5
6 i). School administrators ordered an evacuation of the school on June
7 7, 2007.

8
9 j). On June 7, 2007, the UNSUB(s) posted three of the threatening e-
10 mails in the comments section of the online news publication
11 service, "theolympian". The administrator from "theolympian.com"
12 removed the threatening e-mail postings. Shortly thereafter, the
13 UNSUB(s) re- posted the threatening e-mails. Eventually, the
14 administrator of "theolympian.com" disabled the "Comments" section.

15
16 k). On June 7, 2007, Detective Jeremy Knight, Lacey Police
17 Department (LPD), received information from the Thurston County Sheriff's Office,
18 which had revealed a complaint from a person identified as AG. AG stated that she
19 received an invitation through Myspace.com from the MySpace profile of
20 "Timberlinebombinfo" wanting her to post a URL link to
21 <http://bombermails.hyperphp.com> on her Myspace.com webpage. The UNSUB(s)
22 advised her that failure to comply would result in her name being associated with future
23 bomb threats. Similarly, Knight received a phone call from a parent alleging that her
24 son received the same request from the UNSUB(s). According to Knight, 33 students
25 received a request from the UNSUB(s) to post the link on their respective Myspace.com
26 webpages. Subsequent interviews performed by Knight yielded limited information.

27
28 l). On June 7, 2007, VW and BP received MySpace private invitations

1 from an individual utilizing the MySpace moniker "Timberlinebombinfo". VW
2 accepted the invitation from "Timberlinebombinfo" and received an America Online
3 Instant Message (AIM) from an individual utilizing AIM screen name
4 "Alexspi3ring_09." Communication ceased with "Alexspi3ring_09" after VW requested
5 additional information related to the bomb threats. VW believed screen name
6 "Alexspi3ring_09" was associated to ALEX SPIERING, a student at Timberline High
7 School. VW stated "Alexspi3ring_09" and "Timberlinebombinfo" used to have the
8 identical graphic on their MySpace webpage. "Timberlinebombinfo" recently changed
9 his/her graphic from a picture of guns to a picture of a bomb.

10
11 m). On June 7, 2007, Thurston County School District reported ALEX
12 SPIERING resides at 6133 Winnwood Loop SE, Olympia, WA, 98513, telephone (360)
13 455-0569, date of birth February 6, 1991.

14
15 n). On June 8, 2007, Comcast Internet, Thorofare, New Jersey,
16 reported residential address 6133 Winnwood Loop SE, Olympia, WA, 98513 received
17 Comcast Internet services for the following subscriber:

18 Sara Spiering
19 6133 Winnwood Loop SE, Lacey, WA 98513
20 Telephone (360) 455-0569
21 Dynamically Assigned Active Account
22 Account Number: 8498380070269681

23
24 o). On June 8, 2007, Thurston County School District received two
25 additional bomb threat e-mails from "Timberline.Sucks@gmail.com." which resulted in
26 the evacuation of the Timberline High School.

27
28 12. On June 4, 2007, Google provided subscriber, registration, and IP Address

1 log history for e-mail address "dougbriggs123@gmail.com" with the following results:

2 Status: Enabled (user deleted account)

3 Services: Talk, Search History, Gmail

4 Name: Doug Briggs

5 Secondary Email:

6 Created on: 03-Jun-2007

7 Lang: en

8 IP: 80.76.80.103

9 LOGS: All times are displayed in UTC/GMT

10 dougbriggs123@gmail.com

11 Date/Time	IP
12 04-Jun-2007 05:47:29 am	81.27.207.243
13 04-Jun-2007 05:43:14 am	80.76.80.103
14 03-Jun-2007 06:19:44 am	80.76.80.103

15

16 a). On June 6, 2007, a SmartWhoIs lookup of IP Address 80.76.80.103

17 resolved to Sonic S.R.L, Via S.Rocco 1, 24064, Grumello Del Monte, Italy,

18 Phone: +390354491296, E-mail: Staff@sonic.it. Your affiant connected to

19 http://sonic.it, which displayed an Italian business webpage for Sonic SRL Internet

20 Service Provider.

21

22 b). On June 7, 2007, a request to MySpace for subscriber and IP

23 Address logs for MySpace user "Timberlinebombinfo" provided the following results:

24 User ID: 199219316

25 First Name: Doug

26 Last Name: Briggs

27 Gender: Male

28 Date of Birth: 12/10/1992

1 Age: 14
2 Country: US
3 City: Lacey
4 Postal Code: 985003
5 Region: Western Australia
6 Email Address: timberline.sucks@gmail.com
7 User Name: timberlinebombinfo
8 Sign up IP Address: 80.76.80.103
9 Sign up Date: June 7, 2007 7:49PM
10 Delete Date: N/A
11 Login Date June 7, 2007 7:49:32:247 PM IP Address 80.76.80.103
12

13 c). FBI Seattle Division contacted FBI Legate Attache Rome, Italy and
14 an official request was provided to the Italian National Police requesting assistance in
15 contacting Sonic SRL and locating the compromised computer utilizing IP Address
16 80.76.80.103.
17

18 d). On June 7, 2007, the System Administrator for the
19 www.theolympian.com advised the posting of the bomb threat e-mails originated
20 from IP Address 192.135.29.30. A SmartWhois lookup resolved 192.135.29.30
21 to "The National Institute of Nuclear Physics (INFN), LNL - Laboratori
22 Nazionali di Legnaro, Italy".
23

24 13. Based on my training, experience, and the investigation described herein, I
25 know the following among other things:

26 e). that network level messages, including the originating IP address
27 and MAC address, other variables, and certain registry-type information of a computer
28 can be used to assist in identifying the individual(s) using that computer; and

1 f). the individual(s) using the aforementioned activated computer
2 utilized compromised computers to conceal their true originating IP address and thereby
3 intentionally inhibiting the individual(s)' identification. Compromised computers are
4 generally infected with computer viruses, trojans, or other malevolent programs, which
5 can allow a user the ability to control computer(s) on the Internet or particular services
6 of compromised computer(s) without authorization. It is common for individuals
7 engaged in illegal activity to access and control compromised computer(s) to perform
8 malicious acts in order to conceal their originating IP addresses.

9 14. Based on training, experience, and the investigation described herein, I
10 have concluded that using a CIPAV on the target MySpace Timberlinebombinfo account
11 may assist the FBI to determine the identities of the individual(s) using the activating
12 computer. A CIPAV's activation will cause the activating computer to send network
13 level messages, including the activating computer's originating IP address and MAC
14 address, other variables, and certain registry-type information. This information may
15 assist the FBI in identifying the individual(s) using the activating computers.

16 15. The CIPAV will be deployed through an electronic messaging program from
17 an account controlled by the FBI. The computers sending and receiving the CIPAV data
18 will be machines controlled by the FBI. The electronic message deploying the CIPAV
19 will only be directed to the administrator(s) of the Timberlinebombinfo account.

20 a). Electronic messaging accounts commonly require a unique user
21 name and password.

22 b). Once the CIPAV is successfully deployed, it will conduct a one-
23 time search of the activating computer and capture the information
24 described in paragraph seven.

25 c). The captured information will be forwarded to a computer
26 controlled by the FBI located within the Eastern District of
27 Virginia.

28 d). After the one-time search, the CIPAV will function as a pen register

1 device and record the routing and destination addressing information
2 for electronic communications originating from the activating
3 computer.

- 4 e). **The pen register will record IP address, dates, and times of the**
5 **electronic communications, but not the contents of such**
6 **communications or the contents contained on the computer, and**
7 **forward the IP address data to a computer controlled by the**
8 **FBI, for a period of (60) days.**

9
10 **CONCLUSION**

11 16. Based upon my review of the evidence, my training and experience, and
12 information I have gathered from various computer experts, I have probable cause to
13 believe that deploying a CIPAV in an electronic message directed to the administrator(s)
14 of the MySpace Timberlinebombinfo account will assist in identifying a computer and
15 individual(s) using the computer to transmit bomb threats and related communications in
16 violation of Title 18, United States Code Sections 875(c) and 1030(a)(5)(A)(i) and
17 (B)(iv).

18 17. Because notice as required by Federal Rule of Criminal Procedure
19 41(f)(3) would jeopardize the success of the investigation, and because the investigation
20 has not identified an appropriate person to whom such notice can be given, I hereby
21 request authorization to delay such notice until an appropriate person is identified.
22 Further, assuming providing notice would still jeopardize the investigation after an
23 appropriate person to receive notice is identified, I request permission to ask this Court
24 to authorize an additional delay in notification. In any event, the United States
25 government will notify this Court when it identifies an appropriate person to whom to
26 give notice, so that this Court may determine whether notice shall be given at that time.

27 18. Because there are legitimate law enforcement interests that justify an
28 unannounced use of the CIPAV and review of the messages generated by the activating

1 computer in this case,⁹ I ask this Court to authorize the proposed use of a CIPAV
2 without the prior announcement of its use. One of these legitimate law enforcement
3 interests is that announcing the use of the CIPAV would assist a person controlling the
4 activating computer(s) to evade revealing its true IP address, other variables, and
5 certain registry-type information - thereby defeating the CIPAV's purpose.

6 19. Rule 41(e)(2) requires that (A) the warrant command the FBI "to execute
7 the warrant within a specified time no longer than 10 days" and (B) "execute the warrant
8 during the daytime unless the judge for good cause expressly authorizes execution at
9 another time..." In order to comply with Rule 41, the Government will only deploy
10 CIPAV between the hours of 6:00 a.m. and 10:00 p.m. (PST) during an initial 10-day
11 period. However, the Government seeks permission to read any messages generated by
12 the activating computer as a result of a CIPAV at any time of day or night during the
13 initial 10-day period. This is because the individuals using the activating computer(s)
14 may activate the CIPAV after 10:00 p.m. or before 6:00 a.m., and law enforcement
15 would seek to read the information it receives as soon as it is aware of the CIPAV
16 response given the emergent nature of this investigation. If the CIPAV is not activated
17 within the initial 10-day period, the Government will seek further authorization from the
18 Court to read any information sent to the computer controlled by the FBI as a result of
19 that CIPAV after the 10th day from the date the Court authorizes the use of the first
20 CIPAV.

21 20. Because the FBI cannot predict whether any particular formulation of a
22 CIPAV to be used will cause a person(s) controlling the activating computers to activate
23 a CIPAV, I request that this Court authorize the FBI to use multiple CIPAV's in
24 conjunction with the target MySpace account within 10 days of this Court authorizing
25 the use of the first CIPAV.

27 ⁹ See Wilson v. Arkansas, 514 U.S. 927, 936 (1995) (recognizing that "law enforcement
28 interests may . . . establish the reasonableness of an unannounced entry.")

1 21. Accordingly, it is respectfully requested that this Court issue a search
2 warrant authorizing the following:

3 e). the use of multiple CIPAVs in conjunction with the target MySpace
4 Timberlinebombinfo account, without prior announcement, within 10 days from the date
5 this Court authorizes the use of the first CIPAV;

6 f). the CIPAV may cause an activating computer - wherever located -
7 to send network level messages containing the activating computer's IP address, and/or
8 MAC address, and/or other variables, and/or certain registry-type information to a
9 computer controlled by the FBI and located within the Eastern District of [Virginia];

10 g). that the FBI may receive and read, at any time of day or night,
11 within 10 days from the date the Court authorizes of use of the CIPAV, the information
12 that any CIPAV causes to be sent to the computer controlled by the FBI; and

13 h). that, pursuant to 18 U.S.C. §3103a(b)(3), to satisfy the notification
14 requirement of Federal Rule of Criminal Procedure 41(f)(3), the FBI may delay
15 providing a copy of the search warrant and the receipt for any property taken until no
16 more than thirty (30) days after such time as the name and location of the individual(s)
17 using the activating computer(s) is positively identified or a latter date as the court may,
18 for good cause shown, authorize. Provision of a copy of the search warrant and receipt
19 may, in addition to any other methods allowed by law, be effectuated by electronic
20 delivery of true and accurate electronic copies (e.g. Adobe PDF file) of the fully
21 executed documents.

22 22. It is further requested that this Application and the related documents be
23 filed under seal. The information to be obtained is relevant to an on-going investigation.
24 Premature disclosure of this Application and related documents may jeopardize the
25 success of the above-described investigation.

26 WHEREFORE, Affiant respectfully requests that a warrant be issued authorizing
27 the FBI to utilize a CIPAV and receive the attendant information according to the terms
28 set forth in this Affidavit.

1 **THIS APPLICATION DOES NOT SEEK AUTHORIZATION TO OBTAIN**
2 **THE CONTENT OF ANY ELECTRONIC COMMUNICATIONS, AND THE**
3 **WARRANT WILL SO SPECIFY.**

4 _____
5 Norman B. Sanders
6 Special Agent
7 Federal Bureau of Investigation

8 Sworn to and subscribed before
9 me this _____ day of June, 2007

10 _____
11 Hon. James P. Donohue
12 United States Magistrate Judge

[redacted] (OTD) (FBI)

From: [redacted] (OTD) (FBI)
Sent: Monday, June 25, 2007 1:30 PM
To: [redacted] (OTD) (FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OTD) (FBI)
Subject: FW: Traveler Program

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

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

b2
b7E

b6
b7C

-----Original Message-----

From: [redacted] (CyD) (FBI)
Sent: Monday, June 25, 2007 9:25 AM
To: [redacted] (OTD) (FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OTD) (FBI); [redacted] (CyD) (FBI); [redacted] (FBI); [redacted] (CyD) (FBI); [redacted] (CyD) (FBI)
Subject: RE: Traveler Program

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]
Please give me a call when you get a chance ([redacted] STAO). 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. Topics, such as the scope of assessment, number and make/model of the laptops, as well as the projected turn around time needs to be established with those supporting the technical side of the house.

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).

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] (OTD) (FBI)
Sent: Wednesday, June 20, 2007 12:04 PM
To: [redacted] (CyD) (FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OTD) (FBI)
Subject: Traveler Program

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

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, laptops of our overseas traveling personnel are assessed for compromise. STAO's Investigative Analysis Unit is discussing technical support of the program with my unit. Can you characterize the number of laptops and other specimens needing such assessments, the scope of the assessment (i.e. do you want complete hardware, firmware, BIOS, and OS check on each specimen), 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
b6
b7C

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

[redacted] (OTD) (FBI)

b6
b7C

From: [redacted] (OTD) (FBI)
Sent: Wednesday, June 20, 2007 9:58 AM
To: [redacted] (OTD) (FBI); [redacted] (OS) (FBI); [redacted]
Subject: A. (OS) (FBI)
NIP Request for Quarter 3 - DUE COB Thursday 06/21

~~SECRET~~
~~RECORD 62-0~~

[redacted]

Please provide me the number of successful ops and unsuccessful ops (penetrations) we have had in the month of April, May, and June.

b2
b7E

So...if we attempted to penetrate a target computer [redacted] I need number of attempts and number of successes/failures.

b6
b7C

I need by COB Thursday. Thanks!

[redacted]

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

DECLASSIFIED BY 60322UC/LP/STP/gjg
ON 09-29-2008

[redacted] (OTD) (FBI)

b6
b7C

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

UNCLASSIFIED
NON-RECORD

All leads have been covered and cleared from ACS.

Two of the leads, Detroit (315N-DE-94979) and New Orleans (288A-NO-71030) have been assessed and we are staging to conduct the operations.

Phoenix [redacted] was cancelled by the FO due to [redacted]

b7A
b2

[redacted] I covered the lead in accordance with this information.

Cincinnati [redacted] was comprised of information received from the FO following our deployment of a

b7A
b2

CIPAV [redacted] is evaluating the received information and once he has completed his evaluation, I will forward a response to the FO. As a side note, this is not high on the priority list as we are concentrating on developing solutions for CT cases.

b2
b7E

The remaining leads from Sacramento and St. Louis consisted of read and clear leads.

SSA [redacted]
Operational Technology Division
Digital Evidence Section
Cryptologic and Electronic Analysis Unit
Software Development Group
[redacted] (desk)
[redacted] (cell)
[redacted] (fax-unclass)

b6
b7C
b2

-----Original Message-----

From: [redacted] (OTD) (FBI)
Sent: Tuesday, June 19, 2007 12:55 PM
To: [redacted] (OTD) (FBI); [redacted] (OTD) (FBI)
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]

UNCLASSIFIED

UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-10-2009 BY 60322UC/LP/STP/gjg

[redacted] (OTD) (FBI)

From: [redacted] (OTD) (FBI)
Sent: Tuesday, June 19, 2007 3:19 PM
To: [redacted] (OTD) (FBI)
Subject: FW: SAR Input

b6
b7C

UNCLASSIFIED
NON-RECORD

SSA [redacted]
Operational Technology Division
Digital Evidence Section
Cryptologic and Electronic Analysis Unit
Software Development Group
[redacted] (desk)
[redacted] (cell)
[redacted] (fax-unclass)

b6
b7C
b2

-----Original Message-----

From: [redacted] (OTD) (FBI)
Sent: Tuesday, June 19, 2007 12:20 PM
To: [redacted] (OTD) (FBI)
Subject: SAR Input

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted]

Here is my SAR contribution for last week or this week.

Unclass
288E-SE-93709

On 06/14/2007, CEAU/SDG in conjunction with the Seattle Division deployed a CIPAV to assist with the geophysical locating of a subject whom had issued numerous bomb threats and launched a DDOS attack against a local high school. The CIPAV provided information leading to the identity and arrest of a 15 year old male student from the victim high school who 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.

On 06/08/2007, CEAU presented at the Cyber Online Undercover Course at Calverton RA. Topics addressed were cryptography, remote access search and surveillance, and the voice changer.

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

b6
b7C
b2

[redacted] (desk)
[redacted] (cell)
[redacted] (fax-unclass)

UNCLASSIFIED

UNCLASSIFIED

[redacted] (OTD) (FBI)

From: [redacted] (OTD) (FBI)
Sent: Tuesday, June 19, 2007 1:39 PM
To: [redacted] (OTD) (FBI)
Subject: RE: SAR Input

Importance: High

b6
b7C

UNCLASSIFIED
NON-RECORD

Case ID # needed. Also, assume case is U/FOUO?

[redacted]

-----Original Message-----

From: [redacted] (OTD) (FBI)
Sent: Tuesday, June 19, 2007 12:20 PM
To: [redacted] (OTD) (FBI)
Subject: SAR Input

UNCLASSIFIED
NON-RECORD

b6
b7C

[redacted]

Here is my SAR contribution for last week or this week.

On 06/14/2007, CEAU/SDG in conjunction with the Seattle Division deployed a CIPAV to assist with the geophysical locating of a subject whom had issued numerous bomb threats and launched a DDOS attack against a local high school. The CIPAV provided information leading to the identity and arrest of a 15 year old male student from the victim high school who 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.

On 06/08/2007, CEAU presented at the Cyber Online Undercover Course at Calverton RA. Topics addressed were cryptography, remote access search and surveillance, and the voice changer.

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

[redacted] (desk)
[redacted] (cell)

[redacted] (OTD) (FBI)

From: [redacted] (OTD) (FBI)
Sent: Tuesday, June 19, 2007 1:28 PM
To: [redacted] (OTD) (FBI)
Subject: RE: SAR Input

UNCLASSIFIED
NON-RECORD

b6
b7C

May want to change your signature line to ESTS vs. DES (I've made the same mistake).

Regards.

-----Original Message-----

From: [redacted] (OTD) (FBI)
Sent: Tuesday, June 19, 2007 12:20 PM
To: [redacted] (OTD) (FBI)
Subject: SAR Input

UNCLASSIFIED
NON-RECORD

[redacted]

Here is my SAR contribution for last week or this week.

On 06/14/2007, CEAU/SDG in conjunction with the Seattle Division deployed a CIPAV to assist with the geophysical locating of a subject whom had issued numerous bomb threats and launched a DDOS attack against a local high school. The CIPAV provided information leading to the identity and arrest of a 15 year old male student from the victim high school who 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.

On 06/08/2007, CEAU presented at the Cyber Online Undercover Course at Calverton RA. Topics addressed were cryptography, remote access search and surveillance, and the voice changer.

SSA [redacted]
Operational Technology Division
Digital Evidence Section
Cryptologic and Electronic Analysis Unit
Software Development Group
[redacted] (desk)
[redacted] (cell)
[redacted] (fax-unclass)

b6
b7C

~~SECRET~~

[Redacted] (OTD) (FBI)

From: [Redacted] (OTD) (FBI)
Sent: Thursday, June 14, 2007 7:48 PM
To: [Redacted] (MO) (FBI)
Subject: Affidavit of CIPAV

UNCLASSIFIED
NON-RECORD

b6
b7C
b2

[Redacted]

Sorry for the delay in getting this out to you. Attached are two affidavits. One was used in a Cincinnati case to

[Redacted]

b1

[Redacted] hope they help. I will be out of the office tomorrow. If you need to reach out to me, call me on my cell phone.

(S)

(S)

Sincerely,

SSA [Redacted]
Operational Technology Division
Digital Evidence Section
Cryptologic and Electronic Analysis Unit
Software Development Group
[Redacted] (desk)
[Redacted] (cell)
[Redacted] (fax-unclass)



Web Bug
ffidavit.wpd (61 KB



Revised Affidavit
for Norm San...

UNCLASSIFIED

DATE: 02-24-2009
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 02-24-2034

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

[redacted] (OTD) (FBI)

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

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted]

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.

CEAU deployed a CIPAV to a MySpace account identified as possibly belonging to the UNSUB. The CIPAV returned several IP Addresses, one resolving back to Comcast Cable in Seattle, Washington. Subscriber 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] (desk)
[redacted] (cell)
[redacted] (fax-unclass)

~~SECRET~~

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 06/13/2007

To: Operational Technology Division

From: Operational Technology Division
Electronic Surveillance Technology Section/
Cryptologic and Electronic Analysis Unit

Contact: SSA [REDACTED]

b6
b7C

Approved By: [REDACTED]
[REDACTED]

Drafted By: [REDACTED]

Case ID #: 268-HQ-1305912-SDG

Title: CRYPTOLOGIC ELECTRONIC ANALYSIS UNIT (CEAU)
ASSISTANCE TO THE SEATTLE FIELD OFFICE

Synopsis: Operations Order to assist the Seattle Field Office with effectuating remote delivery of a Computer Internet Protocol Address Verifier (CIPAV) to geophysically locate a subject who has issued multiple bomb threat against a local high school.

Details: The Seattle Field Office has requested assistance from the CEAU with geophysically locating a subject engaged in issuing bomb threats via the Internet to Timberline High School, Lacey, Washington. The objective of the operation is to remotely deploy a CIPAV to geophysically locate the subject.

BACKGROUND

On 06/06/2007, the Seattle Division was contacted by Lacey Police Department (LPD), Lacey, WA, regarding numerous bomb threats and DDOS attacks received at the Timberline School District, Lacey, WA. Below are a time-line of events:

05/30/2007 - Timberline High School evacuation due to hand written bomb threat note.

06/04/2007 - Timberline High School evacuation due to bomb threat email from sender: [REDACTED] UNSUB(s) also b6
b7C

DATE: 02-24-2009
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 02-24-2034

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

~~SECRET~~

To: Operational Technology From: Operational Technology
Re: 268-HQ-1305912-SDG, 06/13/2007

advised a computer attack will hit the Lacey School District, which resulted in a DDOS attack totaling over 80,000,000 hits.

06/05/2007 - Timberline High School evacuation due to bomb threat email from sender: [REDACTED]

b6
b7C

06/06/2007 - Timberline High School evacuation due to bomb threat email from sender: [REDACTED]

06/07/2007 - Timberline High School received additional email from UNSUB(s). Details unknown at present time.

LPD and the Washington State Patrol (WSP) continue to perform school evacuations and bomb sweeps with negative results. Parents and school district employees have informed local television stations and newspapers, which aired the story on June 6, 2007. LPD has requested investigative assistance from the Northwest Cyber Crime Task Force.

LPD has conducted numerous thorough interviews of a student at Timberline High School, [REDACTED]. [REDACTED] appears not to be the subject responsible for bomb threats. [REDACTED] and teachers from Timberline High School provided a list of other students who may be responsible for the threats and DDOS attack. [REDACTED] received a text message from [REDACTED] [REDACTED] DOB [REDACTED] FBI Number [REDACTED] on 06/03/2007, advising "Keep your head up." [REDACTED] is described by teachers as a self proclaimed computer hacker that routinely bypasses the school computer security measures. [REDACTED] computer is in LPD custody and forensic results are pending. Initial interview of [REDACTED] provided negative results.

b6
b7C

[REDACTED]

b1

(S)

On 06/07/2007, Detective [REDACTED] WSP, and SA [REDACTED] Seattle Division, contacted AUSA Kathryn Warma, Western District of Washington, who agreed to prosecute captioned matter.

b6
b7C

~~SECRET~~

~~SECRET~~

To: Operational Technology From: Operational Technology
Re: 268-HQ-1305912-SDG, 06/13/2007

CONCEPT OF THE OPERATION

Deployment Operations Personnel (DOC) will deploy a CIPAV to geophysically locate the subject issuing bomb threats to the Timberline High School, Lacey, Washington. The CIPAV will be deployed [redacted]

b1

[redacted] in MySpace.com (a popular social networking website).

(S)

(S)

EXECUTION



(S)

b1

◆◆

S:/DES/CEAU/Upload/Seattle0613kld07.wpd

SECRET

[redacted] (OTD) (FBI)

From: [redacted] (OTD) (FBI)
Sent: Tuesday, June 12, 2007 3:03 PM
To: [redacted] (SE) (FBI)
Cc: [redacted] (OTD) (FBI)
Subject: RE: Associated Press Article2

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted]

b2
b7E

Let me know what you think

J...

[redacted]
Information Technology Specialist
Operational Technology Division
Office - [redacted]
Mobile - [redacted]
Pager - [redacted]

b6
b7C

-----Original Message-----

From: [redacted] (SE) (FBI)
Sent: Tuesday, June 12, 2007 2:34 PM
To: [redacted] (OTD) (FBI); [redacted] (OTD) (CON); [redacted] (OTD) (FBI)
Cc: [redacted] (SE) (FBI); [redacted] (SE) (OGA)
Subject: FW: Associated Press Article

UNCLASSIFIED
NON-RECORD

[redacted] below is the news article we would like to send containing the CIPAV. I am meeting with the judge at 1:30PST and hope to deploy afterwards. Thanks, [redacted]

SA [redacted]
FBI Seattle

b6
b7C

[redacted] (Fax)
[redacted] (Nextel) [redacted]
[redacted]

-----Original Message-----

From: [redacted] (SE) (FBI)
Sent: Tuesday, June 12, 2007 11:18 AM
To: [redacted] (SE) (FBI)
Subject: Associated Press Article

UNCLASSIFIED
NON-RECORD

Here is the email link in the style of the Seattle Times

>

>

> **Bomb threat at high school downplayed by local police department**

>

> Technology savvy student holds Timberline High School hostage....

>

> Full story:

> http://seattletimes.nwsourc.com/html/nationworld/2003743231_webteensex11.html

>

>

>

>

> TO SUBSCRIBE TO THE SEATTLE TIMES PRINT EDITION

> Call (206) 464-2121 or 1-800-542-0820, or go to

> <http://seattletimes.com/subscribe>

>

> HOW TO ADVERTISE WITH THE SEATTLE TIMES COMPANY ONLINE

> For information on advertising in this e-mail newsletter,

> or other online marketing platforms with The Seattle Times Company,

> call (206) 464-2361 or e-mail websales@seattletimes.com

>

> TO ADVERTISE IN THE SEATTLE TIMES PRINT EDITION

> Please go to <http://seattletimes.nwsourc.com/contactus/adsales>

> for information.

>

>

> For news updates throughout the day, visit <http://www.seattletimes.com>

>

>

>

>

>

>

Copyright (c) 2007 The Seattle Times Company

www.seattletimes.com

Here is the full article.

Friday, June 8, 2007

Bomb threat at high school downplayed by local police department.

The Associated Press

LACEY Wash. — Technology savvy student holds Timberline High School hostage. The suspect is still unknown after several bomb threats and 5 days of school evacuations. Anonymous bomb threats to high schools are a growing trend in rural America.

~~SECRET~~

[Redacted] (OTD) (FBI)

From: [Redacted] (SE) (FBI) b6
Sent: Tuesday, June 12, 2007 1:28 AM b7C
To: [Redacted] (OGC) (FBI); [Redacted] (OTD) (FBI)
Cc: [Redacted] (SE) (FBI); [Redacted] (SE) (OGA); [Redacted] (SE) (FBI); [Redacted] (FBI); [Redacted] (SE) (FBI); [Redacted] (SE) (FBI); [Redacted] (SE) (FBI); [Redacted] (SE) (FBI); [Redacted] (SE) (FBI)
Subject: CIPAV Affidavit - Seattle Division

UNCLASSIFIED
NON-RECORD

[Large Redacted Block]

b1



Revised Affidavit
for [Redacted]

SA [Redacted]
FBI Seattle

[Redacted] (Fax) [Redacted]
[Redacted] (Nextel) [Redacted]
[Redacted]

b6
b7C
b2

UNCLASSIFIED

DATE: 02-24-2009
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 02-24-2034

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (OGC) (FBI) b6
Sent: Tuesday, June 12, 2007 11:06 AM b7C
To: [redacted] (SE) (FBI); [redacted] (OTD) (FBI)
Cc: [redacted] (SE) (FBI); [redacted] (SE) (OGA); [redacted] (SE) (FBI); [redacted] (SE) (FBI); [redacted] (SE) (FBI); [redacted] (OGC) (FBI)
Subject: RE: CIPAV Affidavit - Seattle Division

~~UNCLASSIFIED
NON-RECORD~~

Here are my comments on my legal review of the application for a search warrant in this case. This application is much better than the previous version, and there are only a few issues that I believe need to be addressed or clarified.

Not a legal point, but check your formatting in para 11. The way the document printed on my computer there were some problems.

[redacted]

(S)
b1

In f. (probably should be b.) , Remove the brackets from around Virginia, and you need to add language that makes it clear that the information you are saying may be collected will [redacted] and that after that it will only be collecting addressing, routing, etc. (the stuff covered by a pen register, trap and trace).

b2
b7E

That's all that I have. I have spoken with [redacted] and he has no technical issues that need addressing. Let me know how we can be of further help.

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

b2
b6
b7C

DATE: 02-09-2009
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 02-09-2034

-----Original Message-----

From: [redacted] (SE) (FBI) b6
Sent: Tuesday, June 12, 2007 1:28 AM b7C
To: [redacted] (OGC) (FBI); [redacted] (OTD) (FBI)
Cc: [redacted] (SE) (FBI); [redacted] (SE) (OGA); [redacted] (SE) (FBI); [redacted] (SE) (FBI); [redacted] (SE) (FBI)
Subject: CIPAV Affidavit - Seattle Division

~~UNCLASSIFIED
NON-RECORD~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

[redacted]

(S)
b1

<< File: Revised Affidavit for [redacted] CIPAV.wpd >>

~~SECRET~~

SA [redacted]
FBI Seattle

[redacted] (Fax) [redacted]
(Nextel) [redacted]
[redacted]

b6
b7C
b2

~~UNCLASSIFIED~~

~~UNCLASSIFIED~~

~~SECRET~~

~~SECRET~~

[Redacted] (OTD) (FBI)

From: [Redacted] (OTD) (FBI) b6
Sent: Monday, June 11, 2007 3:38 PM b7C
To: [Redacted] (OGC) (FBI)
Subject: FW: 288A-SE-93709

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

FYI.

SSA [Redacted]
Operational Technology Division
Digital Evidence Section
Cryptologic and Electronic Analysis Unit
Software Development Group
[Redacted] (desk)
[Redacted] (cell)
[Redacted] (fax-unclass)

b6
b7C
b2

-----Original Message-----

From: [Redacted] (OTD) (FBI)
Sent: Friday, June 08, 2007 7:04 PM
To: [Redacted] (SE) (FBI)
Cc: [Redacted] (OTD) (FBI)
Subject: RE: 288A-SE-93709

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

[Redacted]

(S)
b1
b2
b7E

[Large Redacted Area]

~~SECRET~~

DATE: 10-16-2008
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 10-16-2033

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

I cannot stress enough the importance of telling the Judge that the tool will stay persistent on the compromised computer and that ever time the computer connects to the Internet, we will capture the information associated with the PRTT.

I have also attached four documents. The WordPad document [redacted] contains the information that will be returned via the Search Warrant and the PRTT. The other three documents are copies of an application for a mobile tracking order, a mobile tracking/PRTT order, and the affidavit supporting the two that ST. Louis drafted for a similar type order.

Please contact me at the below listed numbers if you have any questions.

Sincerely,

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

[redacted] (desk)
[redacted] (cell)
[redacted] (fax-unclass)

b6
b7C
b2

(S)

[redacted]

b1

-----Original Message-----

From: [redacted] (SE) (FBI)
Sent: Thursday, June 07, 2007 5:12 PM
To: [redacted] (OID) (FBI)
Cc: [redacted] (SE) (OGA)
Subject: 288A-SE-93709

b6
b7C

UNCLASSIFIED
NON-RECORD

b1

<< File: 158pbc01.ec >>

(S)

[redacted]

SA [redacted]
FBI Seattle

[redacted] (Fax)
[redacted] (Nextel) [redacted]
[redacted]

b6
b7C
b2

UNCLASSIFIED

~~UNCLASSIFIED~~

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (SE) (FBI) b6
Sent: Monday, June 11, 2007 10:49 AM b7C
To: [redacted] (OTD) (FBI)
Cc: [redacted] (SE) (OGA); [redacted] (SE) (FBI); [redacted]
Subject: (SE) (FBI)
CIPAV Affidavit

UNCLASSIFIED
NON-RECORD



AFFIDAVIT [redacted]
SFORCIPAV.wpd (...)

[redacted] - AUSA's secretary is cleaning up margins as her version of WP was different at her residence. Content will obviously be the same. Hoping to get it signed this morning. Thanks again for all your help. [redacted]

AUSA is Katheryn Warma [redacted] if DOJ attorney has questions for her.

b6
b7C
b2

SA [redacted]
FBI Seattle

[redacted] (Fax)
[redacted] (Nextel) [redacted]
[redacted]

UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 03-09-2009 BY 60322UC/LP/STP/gjg

~~SECRET~~

[redacted] (OTD) (FBI)

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

DATE: 02-09-2009
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 02-09-2034

b6
b7C

~~SENSITIVE BUT UNCLASSIFIED
NON-RECORD~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

[redacted] we basically have 3 tools to locate a computer. Basic IPAV, Local Info and Local Info with
Getter.

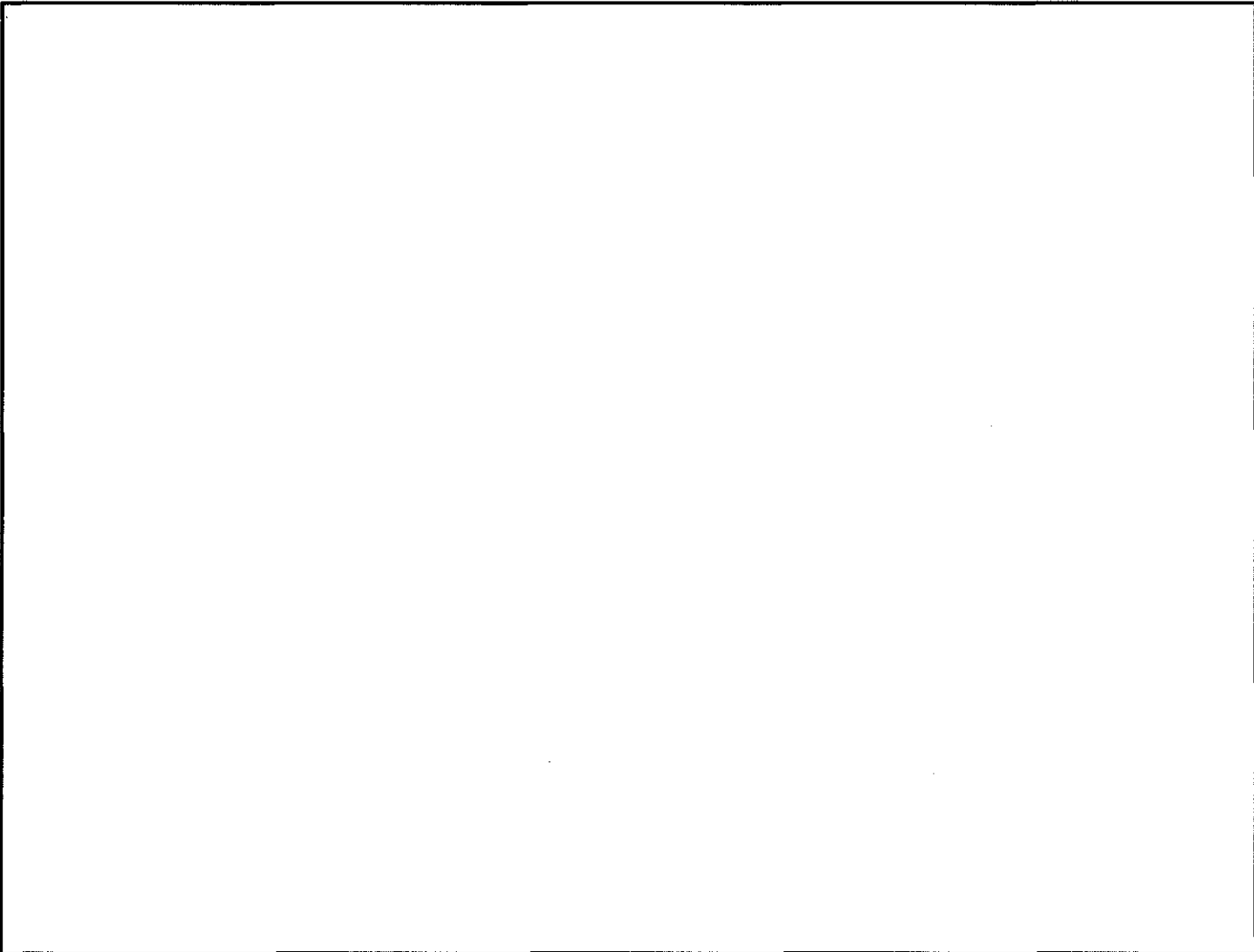
b6
b7C

Give me a call if you have any questions.

J...

b1

Computer Internet Protocol Address Verifier (CIPAV)

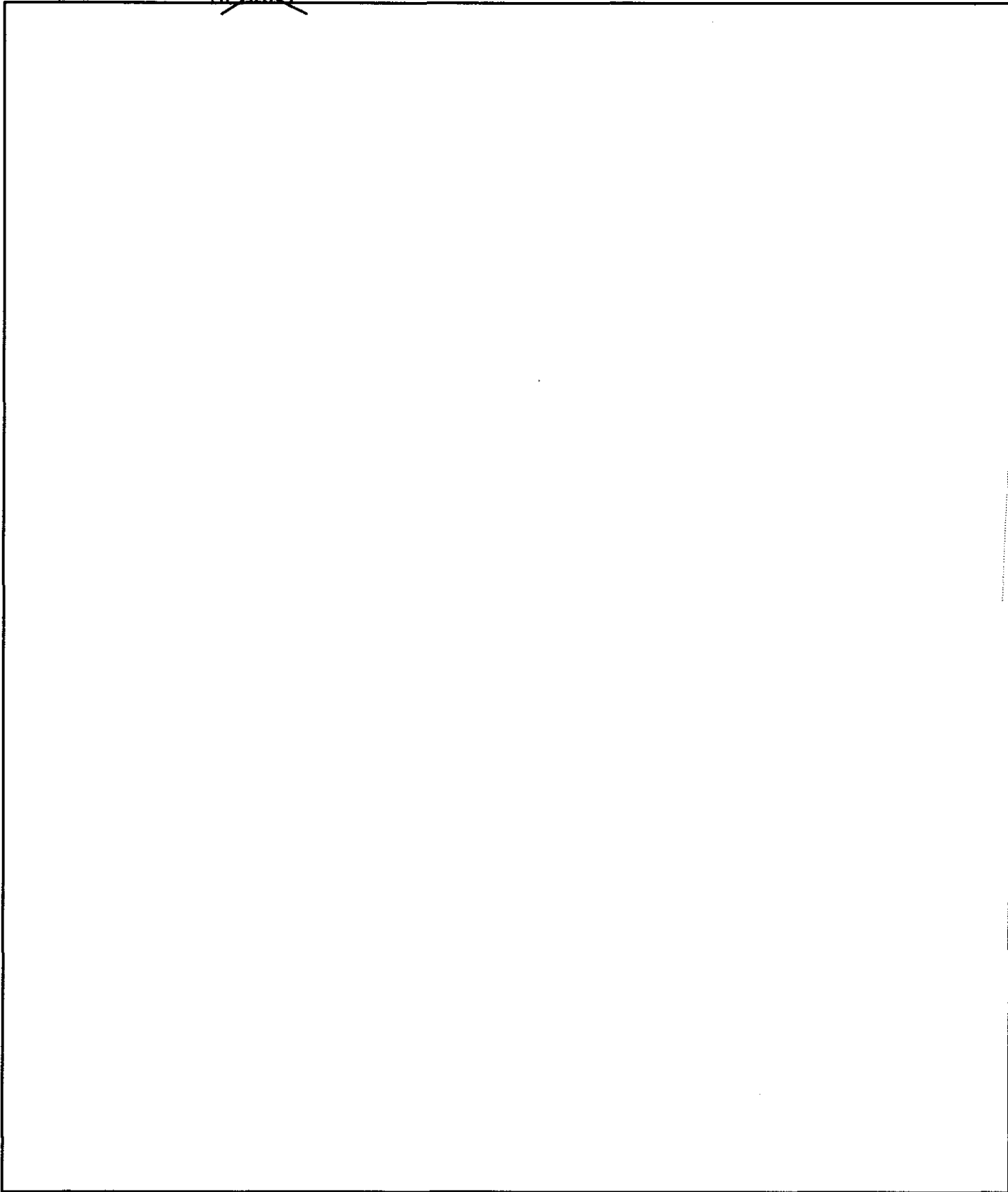


~~SECRET~~

~~SECRET~~

(S)

b1



See Local Info above for further information

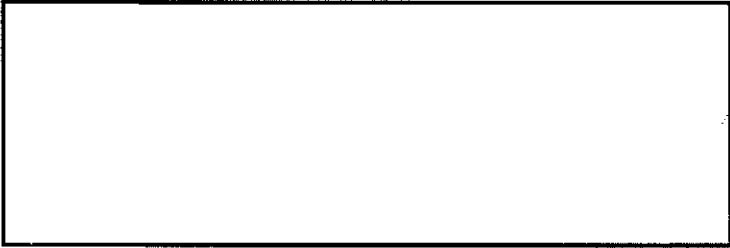
b1



~~SECRET~~

(S)

~~SECRET~~



(S)

b1

~~SENSITIVE BUT UNCLASSIFIED~~

~~SECRET~~

~~SECRET~~

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY

Date: 06/07/2007

To: Cyber

Attn: SSA [redacted]
C3IU-2

International Operations

Attn: UC [redacted]
Europe Unit

b6
b7C

Rome

Attn: Legat [redacted]
ALAT [redacted]

Operational Technology

Attn: CEAU
UC [redacted]
SSA [redacted]

From: Seattle

Squad 11 - Cyber
Contact: Detective [redacted]
SA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]:nbs

Case ID #: 288A-SE-NEW (Pending)

Title: UNSUB(S);
TIMBERLINE SCHOOL DISTRICT (VICTIM);
COMPUTER INTRUSION - INTERNET EXTORTION

Synopsis: Request to open captioned investigation.

Administrative: Reference the following communications:

06/07/2007 telcal between Detective [redacted]
Seattle Division Cyber Task Force, and ROME ALAT [redacted]
[redacted].

b6
b7C

06/07/2007 telcal between SA [redacted],
Seattle Division, and SSA [redacted], CACU.

Details: On 06/06/2007, Seattle Division was contacted by Lacey
Police Department (LPD), Lacey, WA, regarding numerous bomb
threats and DDOS attacks received at the Timberline School
District, Lacey, WA. Below are a time-line of events:

05/30/2007 - Timberline High School evacuation due to
hand written bomb threat note.

DATE: 10-16-2008
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 10-16-2033

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

To: Cyber From: Seattle
Re: 288A-SE-NEW, 06/07/2007

06/04/2007 - Timberline High School evacuation due to bomb threat email from sender: [REDACTED] UNSUB(s) also advised a computer attack will hit the Lacey School District, which resulted in a DDOS attack totaling over 80,000,000 hits.

b6
b7C

06/05/2007 - Timberline High School evacuation due to bomb threat email from sender: [REDACTED]

06/06/2007 - Timberline High School evacuation due to bomb threat email from sender: [REDACTED]

06/07/2007 - Timberline High School received additional email from UNSUB(s). Details unknown at present time.

LPD and the Washington State Patrol (WSP) continue to perform school evacuations and bomb sweeps with negative results. Parents and school district employees have informed local television stations and newspapers, which aired the story on June 6, 2007. LPD has requested investigative assistance from the Northwest Cyber Crime Task Force.

LPD has conducted numerous thorough interviews of a student at Timberline High School, [REDACTED]. [REDACTED] appears not to be the subject responsible for bomb threats. [REDACTED] and teachers from Timberline High School provided a list of other students who may be responsible for the threats and DDOS attack. [REDACTED] received a text message from [REDACTED] [REDACTED] DOB [REDACTED] FBI Number [REDACTED], on 06/03/2007, advising "Keep your head up." [REDACTED] is described by teachers as a self proclaimed computer hacker that routinely bypasses the school computer security measures. [REDACTED] computer is in LPD custody and forensic results are pending. Initial interview of [REDACTED] provided negative results.

b6
b7C

(S)

[REDACTED]

b1

On 06/07/2007, Detective [REDACTED] WSP, and SA [REDACTED], Seattle Division, contacted AUSA Kathryn Warma, Western District of Washington, who agreed to prosecute captioned matter.

b6
b7C

~~SECRET~~

~~SECRET~~

To: Cyber From: Seattle
Re: 288A-SE-NEW, 06/07/2007

~~SECRET~~

~~SECRET~~

To: Cyber From: Seattle
Re: 288A-SE-NEW, 06/07/2007

LEAD(s):

Set Lead 1: (Info)

CYBER

AT WASHINGTON, DC

For information.

Set Lead 2: (Info)

INTERNATIONAL OPERATIONS

AT WASHINGTON, DC

For information.

Set Lead 3: (Action)

ROME

AT ROME, ITALY

(S)



b1

Set Lead 4: (Info)

OPERATIONAL TECHNOLOGY

AT QUANTICO, VA

For information.

◆◆

~~SECRET~~

~~SECRET~~

[Redacted] (OTD) (FBI)

From: [Redacted] (SE) (FBI)
Sent: Thursday, June 07, 2007 5:12 PM
To: [Redacted] (OTD) (FBI)
Cc: [Redacted] (SE) (OGA)
Subject: 288A-SE-93709

b6
b7C

UNCLASSIFIED
NON-RECORD



158nbs01.ec (16 KB)

(S)

[Large redacted block]

b1

SA [Redacted]
FBI Seattle

[Redacted] (Fax)
[Redacted] (Nextel)
[Redacted]

b6
b7C
b2

UNCLASSIFIED

DATE: 02-24-2009
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 02-24-2034

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (OTD) (FBI)
Sent: Thursday, May 31, 2007 12:52 PM
To: [redacted] (NY) (FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OTD) (FBI)
Subject: CIPAV request

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

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] asked that you cover the following in your request: Summary of the case, details of the target and his/her equipment (as much as you know, such as OS, network topology, IP address(es), MACs, Internet connection type, security hardware/software, technical sophistication), legal authority and means of constraining to intended target, and what it is you want from our support (not the technical wants, but what you expect to get from this collection).

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

b6
b7C

Good talking with you!

[redacted]

SENSITIVE BUT UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-30-2008 BY 60322UC/LP/STP/gjg

~~SECRET~~

SECRET // NOFORN // ORCON // 20320621

OPERATIONAL TECHNOLOGY DIVISION (OTD)

SIGNIFICANT MONTHLY ACCOMPLISHMENTS

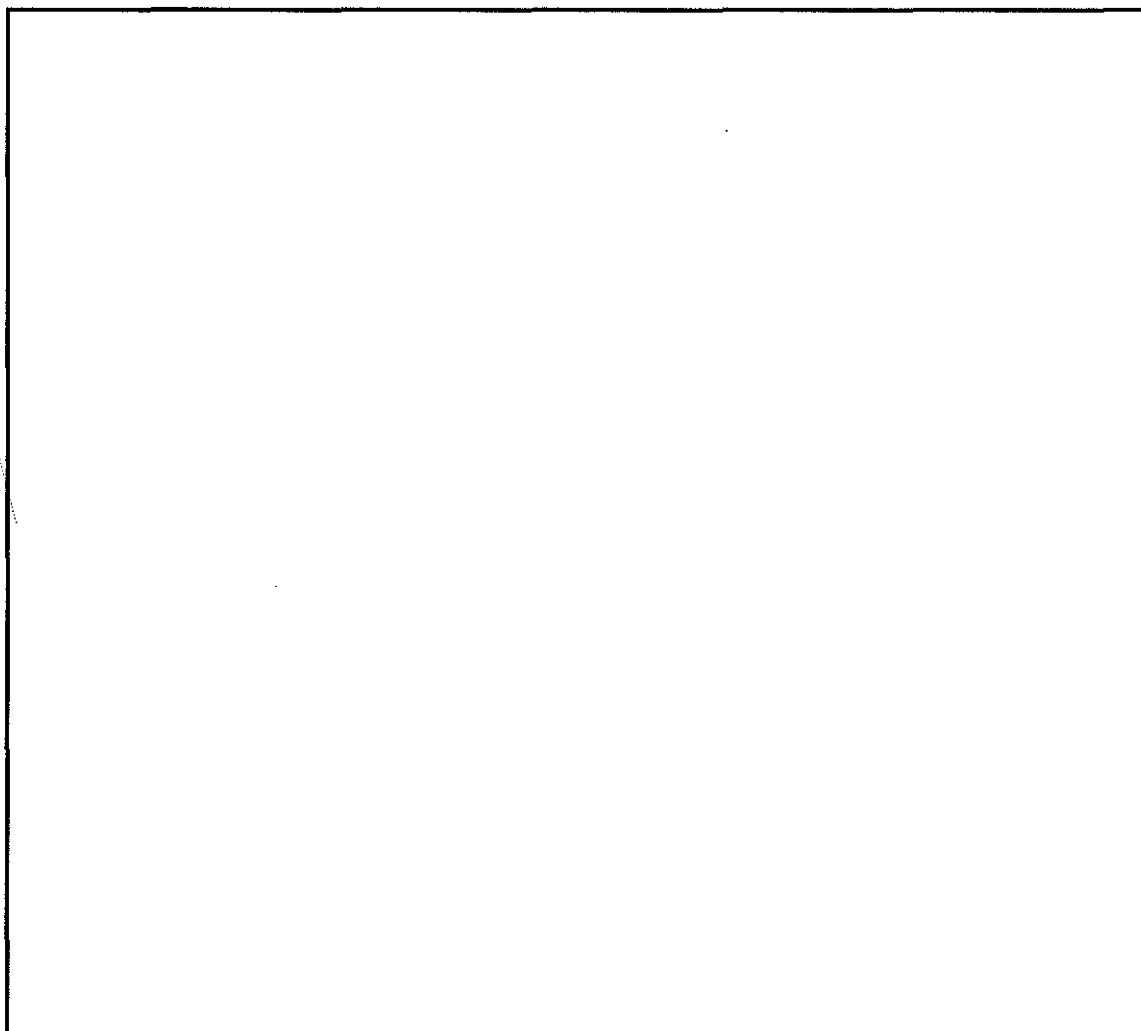
May 24 - June 21, 2007

Electronic Surveillance Technology Section

The Cryptologic and Electronic Analysis Unit (CEAU) reports the following:

(S//NOFORN//ORCON) FIELD SUPPORT:

(S)



b1

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 09-30-2008
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 09-30-2033

~~Derived From: G-3~~
~~Declassify On: 06/21/2032~~

~~SECRET~~

SECRET // NOFORN // ORCON // 20320621

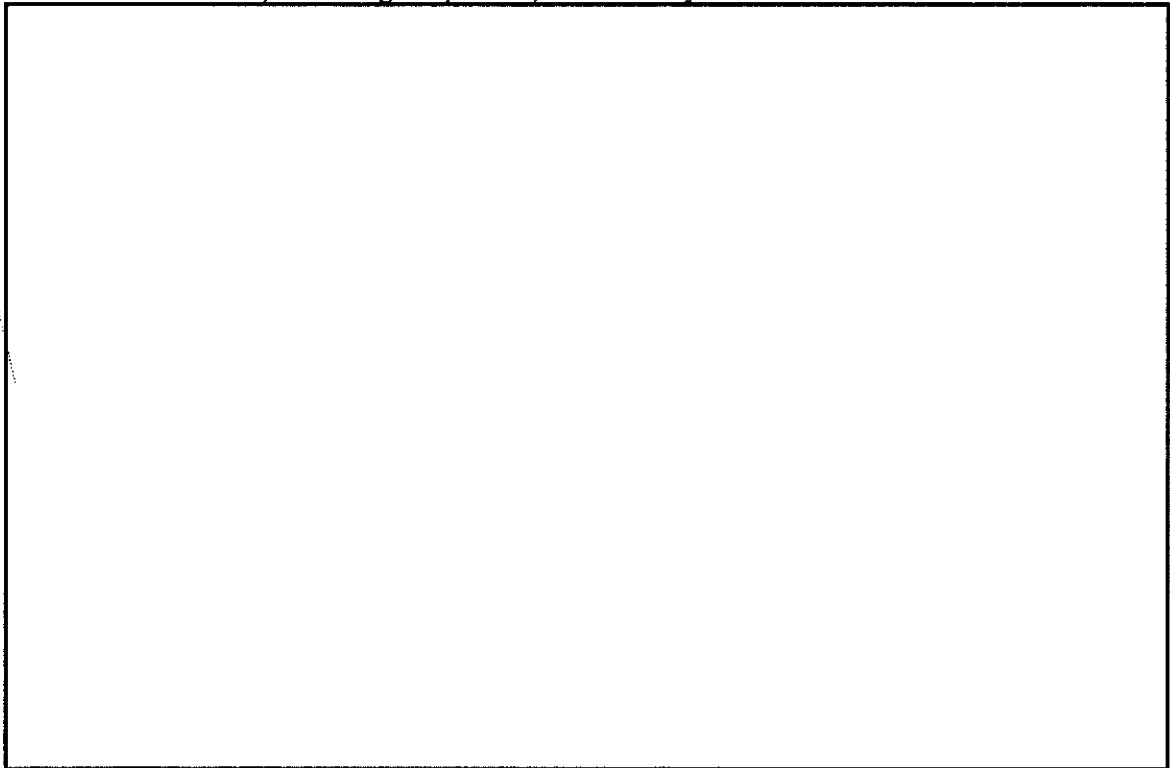
(S)



b1

- (U//FOUO) 288E-SE-93709. On June 14, 2007, CEAU's SDG, in conjunction with the Seattle Field Office, deployed a Computer Internet Protocol Address Verifier (CIPAV) to assist with the geophysical locating of a subject whom had issued numerous bomb threats and launched a Directed-Denial-of-Service (DDOS) attack against a local high school. The CIPAV provided information leading to the identity and arrest of a 15 year old male student from the victim high school who 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 Lacey Washington Police Department (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.

(S)



b1

(U//FOUO) HEADQUARTERS SUPPORT:

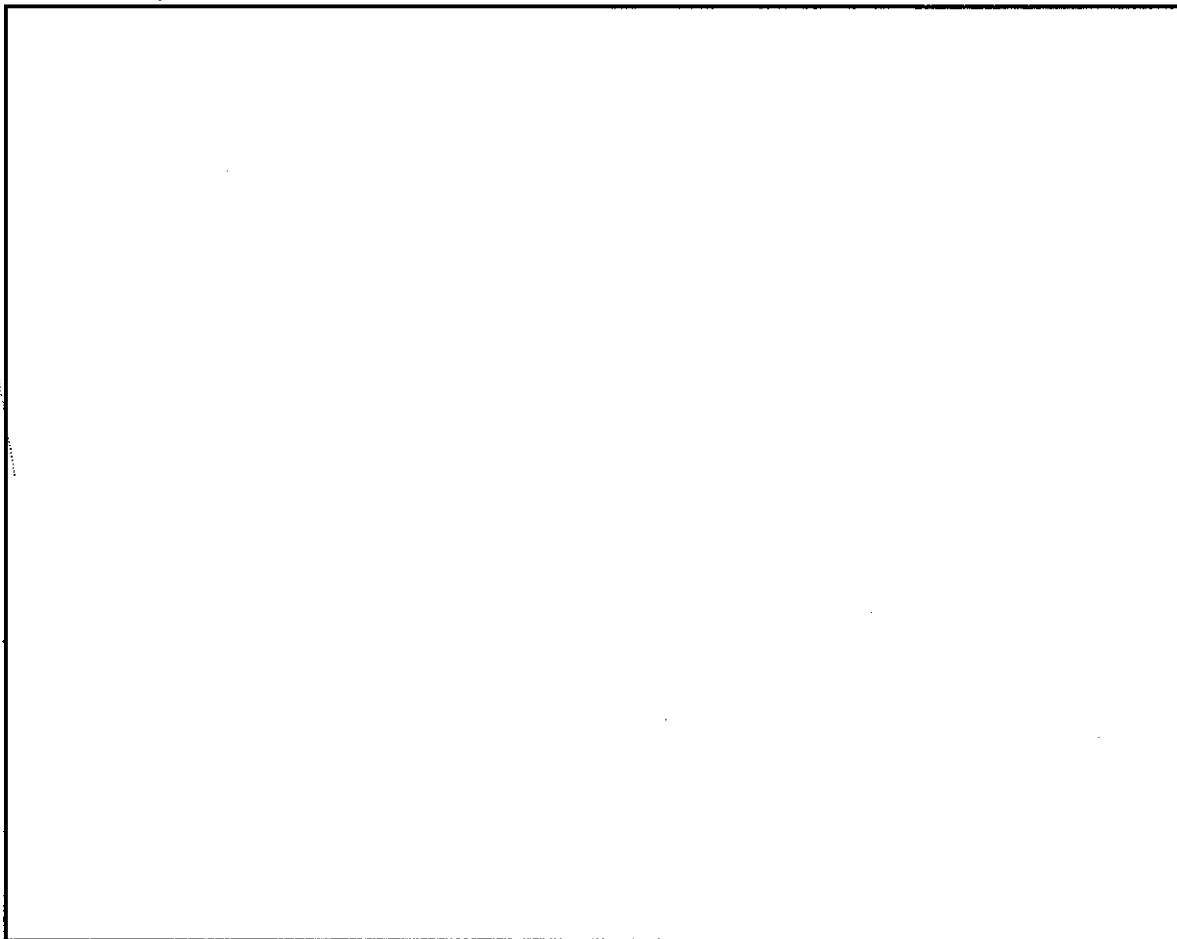
- (U//FOUO) On Friday, June 1, 2007, two (2) members of CEAU traveled to LX1 and answered technical questions during a FISA renewal board. This was necessary to

SECRET // NOFORN // ORCON // 20320621

successfully renew a CTD FISA requesting Hybrid Search and Surveillance authority. OGC expressed their appreciation for this effort.

(S//NOFORN) LIAISON:

(S)



b1

- **(U//FOUO)** June 12, 2007: In response to a request by the Digital Evidence Section (DES)/Forensic Audio/Video Image Analysis Unit (FAVIAU), a tour of [redacted] [redacted] was given to [redacted] personnel who have an interest in Personal Digital Assistant (PDA) passwords and defeats.

b2
b7E

(U//FOUO) TRAINING CONDUCTED:

- **(U//FOUO)** June 6, 2007: CEAU's STEG Manager, SSA [redacted] presented "FBI cell phone forensics" to New Jersey prosecutors and investigators at the New Jersey Regional Computer Forensic Laboratory, Hamilton, New Jersey.

b6
b7C

SECRET // NOFORN // ORCON // 20320621

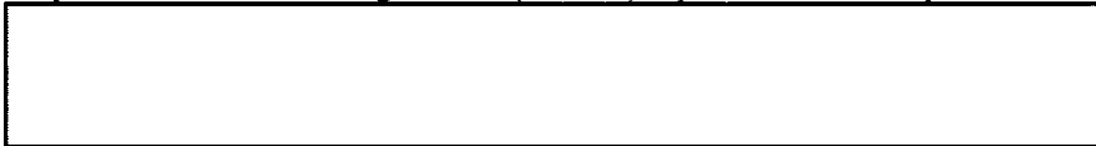
~~SECRET~~

SECRET // NOFORN // ORCON // 20320621

- (U//FOUO) June 8, 2007: CEAU's Software Development Group Manager, SSA [redacted] delivered a presentation to the Online Undercover Course attendees at the Baltimore Field Office's Calverton Resident Agency in Calverton, MD. Topics addressed were cryptography, remote access search and surveillance, and the Voicechanger device. b6 b7c
- (U//FOUO) June 13, 2007: CEAU's STEG Manager, SSA [redacted] presented an hour block on encryption and the Voicechanger device to the Innocent Images National Initiative (IINI) Basic Course in Calverton, MD.

(U//FOUO) OTHER SUPPORT:

- (U//FOUO) Terrorist Explosive Device Analytical Center (TEDAC)/Joint Improvised Explosive Devices Defeat Organization (JIEDDO) requested a technical opinion on



b2
b7E

~~SECRET~~

SECRET // NOFORN // ORCON // 20320621

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (OTD) (FBI)
Sent: Friday, April 27, 2007 9:49 AM
To: [redacted] (OTD) (FBI)
Subject: FW: CIPAV Anthrax threat to cruiseliner.

b6
b7C

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

[redacted] here is the info about the Miami case (Parrot Head) 279B-MM-107759

(S) In short, someone was threatening to release a pathogen on a Royal Caribbean Cruise Line ship unless they pay a specified amount of money [redacted]

b2
b7E

b1

J...

[redacted]
Information Technology Specialist
Operational Technology Division
Office - [redacted]
Mobile - [redacted]
Pager - [redacted]

b6
b7C
b2

-----Original Message-----

From: [redacted] (OTD) (FBI)
Sent: Wednesday, May 31, 2006 9:23 AM
To: [redacted] (OTD) (FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OTD) (FBI)
Subject: FW: CIPAV Anthrax threat to cruiseliner.

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

b6
b7C

[redacted]
Please coordinate with [redacted] on this... we want to maximize our chances on this CIPAV. The warrants aren't signed yet, but please prepare the message accordingly. DO NOT DEPLOY or give to the case agent until we have an approved warrant. (Pardon if I state the obvious).

[redacted]

DATE: 02-12-2009
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 02-12-2034

b6
b7C

-----Original Message-----

From: [redacted] (MM) (FBI)
Sent: Tuesday, May 30, 2006 3:34 PM
To: [redacted] (OTD) (FBI)
Cc: [redacted] (MM) (FBI)
Subject: CIPAV

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

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S)

Here is the affidavit and warrant. Could we send anthra [redacted] a message saying [redacted]

b1

b2
b7E

~~SECRET~~

(S) [Redacted]

[Redacted] let me know. I am looking at going to get the warrant signed on May 31 or June 1.

b6
b7C

b1

(S) [Redacted]

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SECRET~~

~~TOP SECRET~~

[redacted] (OTD) (CI)
[redacted] (OTD) (CI)
[redacted] (CI) (FBI)
Subject: RE: EC Directing end to CIPAV operations

b6
b7C

~~SENSITIVE BUT UNCLASSIFIED
NON-RECORD~~

[redacted]

Thanks for the EC. [redacted]
[redacted] If not, could you get and provide that info to me as soon as feasible.

b2
b7A

Thanks,

SSA [redacted]
Operational Technology Division
Digital Evidence Section
Cryptologic and Electronic Analysis Unit
Software Development Group
[redacted] (desk)
[redacted] (cell)
[redacted] (fax-unclass)

b6
b7C
b2

-----Original Message-----

From: [redacted] (CI) (FBI)
Sent: Friday, February 23, 2007 2:55 PM
To: [redacted] (CG) (FBI); [redacted] (CG) (FBI); [redacted] (CI) (FBI); [redacted] (CI) (FBI);
[redacted] (CyD) (FBI); [redacted] (OTD) (FBI); [redacted] (CyD) (FBI); [redacted] (JK)
(FBI); [redacted] (CI) (FBI); [redacted] (CI) (FBI); [redacted] (JK) (FBI);
(CyD) (FBI); [redacted] (CI) (FBI); [redacted] (CyD) (FBI); [redacted] (CyD) (FBI);
[redacted] (OTD) (FBI); [redacted] (CyD) (FBI); [redacted] (CI) (FBI); [redacted] (CI) (FBI);
[redacted] (CI) (FBI)

b6
b7C

Subject: EC Directing end to CIPAV operations

~~SENSITIVE BUT UNCLASSIFIED
NON-RECORD~~

b1

b7A

This is an update on [redacted] [redacted] This EC has not yet been approved.

<< File: EC ending web bug operations >>

(S)

SA [redacted]
[redacted] Desk
[redacted] Nextel
[redacted] Direct connect
[redacted] Text Messages

DATE: 02-09-2009
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 02-09-2034

b6
b7C
b2

~~SENSITIVE BUT UNCLASSIFIED~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SENSITIVE BUT UNCLASSIFIED
SECRET~~

[redacted] (OTD) (FBI)

Subject: CIPAV
Start Date: Thursday, March 08, 2007
Due Date: Thursday, March 08, 2007

Status: Completed
Percent Complete: 100%
Date Completed: Monday, March 26, 2007

b6
b7C

Total Work: 0 hours
Actual Work: 0 hours

Owner: [redacted] (OTD) (FBI)

[redacted] Spoke with [redacted]. He advised that they have a case in which [redacted] would like to depoly a CIPAV to geophysically locate the subjects. Will forward EC setting lead for CEAU's assistance. In addition, he is currently working on the SW. He is using the CI SW as a ponie.

b2
b7E

From: [redacted] (OTD) (FBI)
Sent: Tuesday, March 06, 2007 11:39 AM
To: [redacted] (TP) (FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OTD) (FBI)
Subject: CIPAV

b6
b7C

Follow Up Flag: Follow up
Due By: Thursday, March 08, 2007 1:30 PM
Flag Status: Flagged

UNCLASSIFIED
NON-RECORD

[redacted]
Good to hear from you ! I appreciate the TELCAL and your interest in the CIPAV.

I am forwarding your request to [redacted] Program Manager of the Software Development Group. They are the team that does the CIPAV. His telephone number is [redacted]

b6
b7C
b2

Hope you are doing well!

[redacted] Can you please call [redacted] - he has some questions on the CIPAV--his telephone number is [redacted]

SSA [redacted]
Secure Technologies Exploitation
Cryptologic and Electronic Analysis Unit
Operational Technology Division
Engineering Research Facility

b6
b7C
b2

[redacted] voice
[redacted] STU III
[redacted] fax (non-secure)
[redacted] fax (secure)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-30-2008 BY 60322UC/LP/STP/gjg

UNCLASSIFIED

[redacted] (OTD) (FBI)

From: [redacted] (OTD)(FBI)
Sent: Friday, March 23, 2007 2:48 PM
To: [redacted] (CI) (FBI)
Cc: [redacted] (OTD) (FBI)
Subject: Removal of data from CEAU IPAV Regarding Case [redacted]

b2

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
b7C

Removal of data from CEAU IPAV Regarding Case [redacted]

b2

[redacted] our records indicate that we are no longer actively collecting data for your case.

Please download and save all data regarding your case from the CEAU IPAV server by June 23 2007. Once we have received confirmation that you have downloaded the data it will be deleted from CEAU computers and servers. This allows us to free up additional server capacity to support other matters.

If you need more time to download the information we would be happy to accommodate you. Please contact me regarding the disposition of the data and the computers.

v/r
[redacted]

SENSITIVE BUT UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-16-2008 BY 60322UC/LP/STP/gjg

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (OTD)(FBI)
Sent: Friday, March 23, 2007 10:09 AM
To: [redacted] (TP) (FBI)
Cc: [redacted] (OTD) (FBI)
Subject: RE: [redacted] - Computer Tracer

b6
b7C

b2

~~SENSITIVE BUT UNCLASSIFIED
RECORD~~ [redacted]

[redacted] just to confirm.

I'm sure you notice the activity last night. Their was no new data given.

I will have [redacted] set up a log in for you to download the IP logs from the last few days.

I am not sure what else we can do to help.

If you have any questions please feel free to contact me.

b6
b7C
b2

v/r

[redacted]

[redacted]

Information Technology Specialist
Operational Technology Division
Office
Mobile
Pager [redacted]

-----Original Message-----

From: [redacted] (TP) (FBI)
Sent: Thursday, March 22, 2007 3:07 PM
To: [redacted] (OTD)(FBI)
Subject: RE: [redacted] Computer Tracer

b2

~~SENSITIVE BUT UNCLASSIFIED
RECORD~~ [redacted]

b6
b7C

[redacted]

No pages, so I'm assuming no activity. Could we get the lps that have hit it so far?

Thanks,

[redacted]

Tampa Cyber

DATE: 02-24-2009
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 02-24-2034 b2

-----Original Message-----

From: [redacted] (OTD)(FBI)
Sent: Wednesday, March 21, 2007 1:28 PM
To: [redacted] (TP) (FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OTD) (FBI)
Subject: [redacted] - Computer Tracer

~~SENSITIVE BUT UNCLASSIFIED
RECORD~~ [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

[redacted] I just wanted to document the steps we have taken in the last few days.

Friday 16 March - Tampa field office contacted CEAU requesting assistance on locating a computer being used

[redacted]

(S)
b1

Monday 19 March

[redacted]

(S)

b1

Please feel free to amend or modify if needed.

v/r

[redacted]

b6
b7C
b2

[redacted]

Information Technology Specialist
Operational Technology Division

Office
Mobile
Pager

[redacted]

-----Original Message-----

From: [redacted] (TP) (FBI)
Sent: Monday, March 19, 2007 8:47 AM
To: [redacted] (OTD)(FBI)
Subject: Wire Receipt for CIPAV

~~SENSITIVE BUT UNCLASSIFIED~~

~~SECRET~~

NON-RECORD

[Redacted]

As per our telcal, here's the wire receipt for the CIPAV. Thanks again for your assistance!

b6
b7c

[Redacted]

Tampa Cyber

<< File: Transfer Receipt.doc >>

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (OTD) (FBI)
Sent: Friday, March 16, 2007 10:04 AM
To: [redacted] (OGC) (FBI)
Subject: FW: CIPAV Request

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
b7C
b2

[redacted]

Can you please review the attached affidavit and let me know what the contemplated court ordered authorizations are present. TP wants to submit this for signature this afternoon. That would put us on the clock for providing a solution no later than Sunday, March 25th. Let me know your findings as soon as possible so that I can respond to the FO.

Thanks,

SSA [redacted]
Operational Technology Division
Digital Evidence Section
Cryptologic and Electronic Analysis Unit
Software Development Group
[redacted] (desk)
[redacted] (cell)
[redacted] (fax-unclass)

-----Original Message-----

From: [redacted] (TP) (FBI)
Sent: Thursday, March 15, 2007 4:02 PM
To: [redacted] (OTD) (FBI)
Cc: [redacted] (TP) (FBI); [redacted] (CyD) (FBI)
Subject: FW: CIPAV Request

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
b7C

[redacted]

Here's a draft of our search warrant affidavit to obtain the CIPAV. It's moving through our legal dept and AUSA's office. Let me know if you all have any technical changes.

Thanks,

[redacted]



cipav.wpd (89 KB)

-----Original Message-----

From: [redacted] (TP) (FBI)
Sent: Thursday, March 08, 2007 3:22 PM
To: [redacted] (OTD) (FBI)
Cc: [redacted] (TP) (FBI); [redacted] (TP) (FBI); [redacted] (TP) (FBI); [redacted] (TP)(FBI)
Subject: CIPAV Request

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[Redacted]

As per our telcal, here's the request for the CIPAV for Tampa's Group II UCO. I'll send you a draft of the search warrant affidavit tomorrow. Please advise if you need any additional info.

b6
b7C

Thanks,

[Redacted]
Tampa Cyber



cipav.request.wpd
(28 KB)

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY

Date: 03/08/2007

To: Operational Technology

Attn: Cryptologic & Electronic
Analysis Unit

Cyber

Attn: SSA [redacted]
CyD/CIS/C3IU-1, Room [redacted]

b6
b7C

From: Tampa

Squad 8

Contact: SA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]:den

Case ID #: [redacted] (Pending)

b2
b7A

Title: [redacted]

Synopsis: Request the deployment of a Computer & IP Address Verifier (CIPAV).

Details:

BACKGROUND

[redacted]

b7A

[redacted]

To: Operational Technology From: Tampa
Re: [redacted] 03/08/2007

[redacted]

[redacted]

b2
b7A
b6
b7C

[redacted]

Tampa is currently drafting the search warrant necessary to obtain the requested CIPAV, which Tampa hopes to deploy on or around 03/15/2007.

To: Operational Technology From: Tampa
Re: [REDACTED] 03/08/2007

b2

LEAD(s):

Set Lead 1: (Action)

OPERATIONAL TECHNOLOGY

AT QUANTICO, VIRGINIA

The Cryptologic & Electronic Analysis Unit is requested to facilitate the deployment of a CIPAV to support captioned Group II UCO.

Set Lead 2: (Info)

CYBER

AT WASHINGTON, D.C.

For information, read and clear.

◆◆

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (OTD)(FBI)
Sent: Thursday, March 08, 2007 4:35 PM
To: [redacted] (OTD) (FBI); [redacted] (ITD) (FBI)
Subject: RE: CIPAV Request

b6
b7C

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

Seems that since the UCE is in direct communication with the target, we may be able to [redacted]
It would be helpful to know the e-mail provider for the target and UCE.

b1
(S)

J...

[redacted]
Information Technology Specialist
Operational Technology Division
Office [redacted]
Mobile [redacted]
Pager [redacted]

b6
b7C
b2

-----Original Message-----

From: [redacted] (OTD) (FBI)
Sent: Thursday, March 08, 2007 4:24 PM
To: [redacted] (ITD) (FBI)
Cc: [redacted] (OTD)(FBI)
Subject: FW: CIPAV Request

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

Gentlemen,

Here is the EC regarding the Tampa case. Let me know your thoughts.

b6
b7C
b2

SSA [redacted]
Operational Technology Division
Digital Evidence Section
Cryptologic and Electronic Analysis Unit
Software Development Group
[redacted] (desk)
[redacted] (cell)
[redacted] (fax-unclass)

DATE: 02-24-2009
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 02-24-2034

-----Original Message-----

From: [redacted] (TP) (FBI)
Sent: Thursday, March 08, 2007 3:22 PM
To: [redacted] (OTD) (FBI)
Cc: [redacted] (TP) (FBI); [redacted] (TP) (FBI); [redacted] (TP) (FBI); [redacted] (TP)(FBI)
Subject: CIPAV Request

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

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

~~SECRET~~

[Redacted]

As per our telcal, here's the request for the CIPAV for Tampa's Group II UCO. I'll send you a draft of the search warrant affidavit tomorrow. Please advise if you need any additional info.

b6
b7C

Thanks,

[Redacted]
Tampa Cyber

<< File: cipav.request.wpd >>

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (OTD)(FBI)
Sent: Friday, March 02, 2007 10:54 AM
To: [redacted] (OTD) (FBI)
Subject: FW: RMS Request 00000000115736 aged of at least 60 days.

UNCLASSIFIED
NON-RECORD

[redacted] can you please clear this from RMS?

Thanks
J..

[redacted]
Information Technology Specialist
Operational Technology Division
Office - [redacted]
Mobile - [redacted]
Pager - [redacted]

b2
b7E
b6
b7C

-----Original Message-----

From: Request Managment System [mailto:[redacted]]
Sent: Friday, March 02, 2007 10:39 AM
To: [redacted]
Subject: RMS Request 00000000115736 aged of at least 60 days.

RMS Request 00000000115736 aged of at least 60 days.

Division (Required) : OTD
Program (Required) : Computer Exploitation
Unit (Required) : CEAU
Item (Required) : Remote Computer Search/Surveillance
Classification :

Requested Support : Per previous telephone conversations between SA [redacted] (STL) and [redacted]
[redacted] St Louis Division is requesting that CEAU install CIPAV devices in [redacted]

[redacted]
112 : 1014;3730;
2000104 : [redacted]
536870924 : [redacted]

UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-23-2008 BY 60322UC/LP/STP/gjg

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (OTD)(FBI)
Sent: Friday, March 02, 2007 10:54 AM
To: [redacted] (OTD) (FBI)
Subject: FW: RMS Request 000000000116159 aged of at least 60 days.

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

b6
b7C

[redacted] can you please clear this from RMS?

Thanks
J..

[redacted]
Information Technology Specialist
Operational Technology Division
Office - [redacted]
Mobile - [redacted]
Pager - [redacted]

-----Original Message-----
From: Request Managment System [mailto:[redacted]]
Sent: Friday, March 02, 2007 10:39 AM
To: [redacted]
Subject: RMS Request 000000000116159 aged of at least 60 days.

b6
b7C

RMS Request 000000000116159 aged of at least 60 days.

Division (Required) : OTD

[Large redacted area]

(S)

b1

~~UNCLASSIFIED~~

DATE: 02-09-2009
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 02-09-2034

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (CI) (FBI) b6
Sent: Friday, March 02, 2007 8:40 AM b7C
To: [redacted] (OS)(FBI); [redacted] (OS) (FBI);
[redacted] (CI) (FBI); [redacted] (CI) (FBI); [redacted] (CI)(FBI);
[redacted] (MW) (FBI); [redacted] (CvD) (FBI);
[redacted] (CvD) (FBI); [redacted] (CI)(FBI); [redacted] (CI) (FBI);
[redacted] (OTD) (FBI); [redacted] (CI) (FBI); [redacted] (OTD)
(FBI)
Subject: FW: [redacted]

b2
b7E

UNCLASSIFIED
NON-RECORD

An additional document for the conference all is posted below (at the bottom).

SA [redacted]
[redacted] Desk
[redacted] Nextel
[redacted] Direct connect
[redacted]

b6
b7C
b2

-----Original Message-----
From: [redacted] (IP) (FBI)
Sent: Friday, March 02, 2007 8:39 AM
To: [redacted] (CI) (FBI)
Subject: FW: [redacted]

b2
b7E

UNCLASSIFIED
NON-RECORD

Here it is.

b6
b7C

-----Original Message-----
From: [redacted] (IP) (FBI)
Sent: Thursday, March 01, 2007 2:22 PM
To: [redacted] (IP) (FBI)
Cc: [redacted] (CI) (FBI)
Subject: [redacted]

b2
b7E

UNCLASSIFIED
NON-RECORD

[redacted]: The lead is [redacted]. It's in your lead box now. Attached is [redacted] 302. I'm routing the original 302 to you, so you can package it up with your final product for CI.

[redacted] Our investigation takes us to Evansville RA. I've reassigned the lead.



060dd01.302 (12 KB)

UNCLASSIFIED

[redacted] (OTD) (FBI)

From: [redacted] (CI) (FBI) b6
Sent: Friday, March 02, 2007 8:29 AM b7C
To: [redacted] (OS)(FBI); [redacted] (OS) (FBI); [redacted] (CI) (FBI); [redacted] (CI)(FBI); [redacted] (CI)(FBI); [redacted] (CI)(FBI); [redacted] (MW) (FBI); [redacted] (CyD) (FBI); [redacted] (CyD) (FBI); [redacted] (CI)(FBI); [redacted] (CI) (FBI); [redacted] (OTD) (FBI); [redacted] (CI) (FBI); [redacted] (OTD) (FBI)
Subject: RE: Web Bug Analysis Conference Call
Importance: High

UNCLASSIFIED
NON-RECORD



daytonbeac report.doc (190 KB)...



[redacted] Analysis (14 KB)



038mpe01.ec.wpd (27 KB)

Dear Conference Call Participants,

Here are some documents for your review before we begin the conference call. Conference call information is posted below.

SA [redacted]
[redacted] Desk
[redacted] Nextel
[redacted] Direct connect
[redacted]

b6
b7C
b2

-----Original Message-----

From: [redacted] (IR)(FBI)
Sent: Thursday, March 01, 2007 6:04 PM
To: [redacted] (CI) (FBI); [redacted] (OS)(FBI); [redacted] (OS) (FBI); [redacted] (CI) (FBI); [redacted] (CI) (FBI); [redacted] (CI)(FBI); [redacted] (MW) (FBI); [redacted] (CyD) (FBI); [redacted] (CyD) (FBI); [redacted] (CI)(FBI); HO. Div13. SLOC [redacted] (CI) (FBI); [redacted] (OTD) (FBI); [redacted] (CI) (FBI); [redacted] (OTD) (FBI)
Subject: RE: Web Bug Analysis Conference Call
Importance: Hig

UNCLASSIFIED
NON-RECORD

b6
b7C

SA [redacted]

Your call was scheduled as requested. To access the conference system, dial [redacted] when prompted, enter your pin code [redacted]. Your parties may begin dialing in as early as 9:45 AM (EST) on 3/2/07.

If you have any questions, please call SIOC at [redacted] or e-mail SIOC at HQ_DIV13_SIOC.

b6
b7C
b2

EAS [redacted]
SIOC [redacted]
[redacted]

-----Original Message-----

b6
b7C

From: [redacted] (CI) (FBI)
Sent: Tuesday, March 01, 2007 5:48 PM
To: [redacted] (OS) (FBI); [redacted] (OS) (FBI); [redacted] (CI) (FBI); [redacted] (CI)
[redacted] (FBI); [redacted] (CI) (FBI); [redacted] (MW) (FBI); [redacted] (CyD) (FBI); [redacted]
[redacted] (CyD) (FBI); [redacted] (CI) (FBI); HQ Div13 SIOC; [redacted] (CI) (FBI); [redacted]
[redacted] (OTD) (FBI); [redacted] (CI) (FBI); [redacted] (OTD) (FBI)
Subject: Web Bug Analysis Conference Call
Importance: High

UNCLASSIFIED
NON-RECORD

Dear SIOC,

Cincinnati requests a conference call for 12 participants tomorrow (3/2/2007) at 10:00 a.m. EST. The Point of Contact is SA [redacted] (see below). The purpose of the conference call is to discuss with STAU analysis of web bug data. Please respond to all with the conference number and PIN.

Best wishes,

b6
b7C
b2

SA [redacted]
[redacted] Desk
[redacted] Nextel
[redacted] Direct connect
[redacted]

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (CI) (FBI)
Sent: Monday, February 26, 2007 4:13 PM
To: [redacted] (OTD) (FBI)
Subject: RE: EC Directing end to CIPAV operations

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Dear [redacted]

b6
b7C
b2

I'm working on that issue.

Thanks,

SA [redacted]

Desk
Nextel
Direct connect

[redacted]

-----Original Message-----

From: [redacted] (OTD) (FBI)
Sent: Monday, February 26, 2007 10:21 AM
To: [redacted] (CI) (FBI)
Subject: RE: EC Directing end to CIPAV operations

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

Thanks for the EC. By the way, were you able to gather the info from the bank concerning which accounts were actually hit by the subjects? If not, could you get and provide that info to me as soon as feasible.

b6
b7C
b2

Thanks,

SSA [redacted]

Operational Technology Division
Digital Evidence Section
Cryptologic and Electronic Analysis Unit
Software Development Group

[redacted]
(desk).
(cell)
(fax-unclass)

DATE: 02-09-2009
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 02-09-2034

-----Original Message-----

From: [redacted] (CI) (FBI)
Sent: Friday, February 23, 2007 2:55 PM
To: [redacted] (CG) (FBI); [redacted] (CG) (FBI); [redacted] (CI) (FBI); [redacted] (CI) (FBI);
[redacted] (CyD) (FBI); [redacted] (OTD) (FBI); [redacted] (CyD) (FBI); [redacted] (JK) (FBI);
[redacted] (FBI); [redacted] (CI) (FBI); [redacted] (CI) (FBI); [redacted] (JK) (FBI);
[redacted] (CyD) (FBI); [redacted] (CI) (FBI); [redacted] (CyD) (FBI); [redacted] (CyD) (FBI);
[redacted] (CI) (FBI); [redacted] (OTD) (FBI); [redacted] (CyD) (FBI); [redacted] (CI) (FBI); [redacted] (CI) (FBI)

Subject: EC Directing end to CIPAV operations

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

~~SECRET~~

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

This is an update on [redacted]
not yet been approved.

[redacted]

This EC has

(S)

b1

b7A

<< File: EC ending web bug operations >>

SA [redacted]

[redacted]

Desk
Nextel
Direct connect

[redacted]

b6
b7C
b2

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

~~SECRET~~

SECRET

DATE: 10-02-2009
CLASSIFIED BY 60322 UC LP/STP
REASON: 1.4 (c)
DECLASSIFY ON: 10-02-2034

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 02/23/2007

To: Cyber

Attn: C3IU-2

OTD

SSA [redacted]

Attn: DES/CEAU

UC [redacted]

SSA [redacted]

Chicago

Attn: [redacted] / NRA1

SA [redacted]

SA [redacted]

b2
b7E
b6
b7C

From: Cincinnati

Squad 13

Contact: SA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]:jk

Case ID #: [redacted] (Pending)

Title: CIPAV OPERATIONS;
[redacted]

b7A
b2

Synopsis: CIPAV operations have ended.

Reference: [redacted]

Details: Cincinnati has employed a Computer and Internet Protocol Address Identifier ("CIPAV") to gather evidence concerning

[redacted]

b7A

(S)

[redacted]

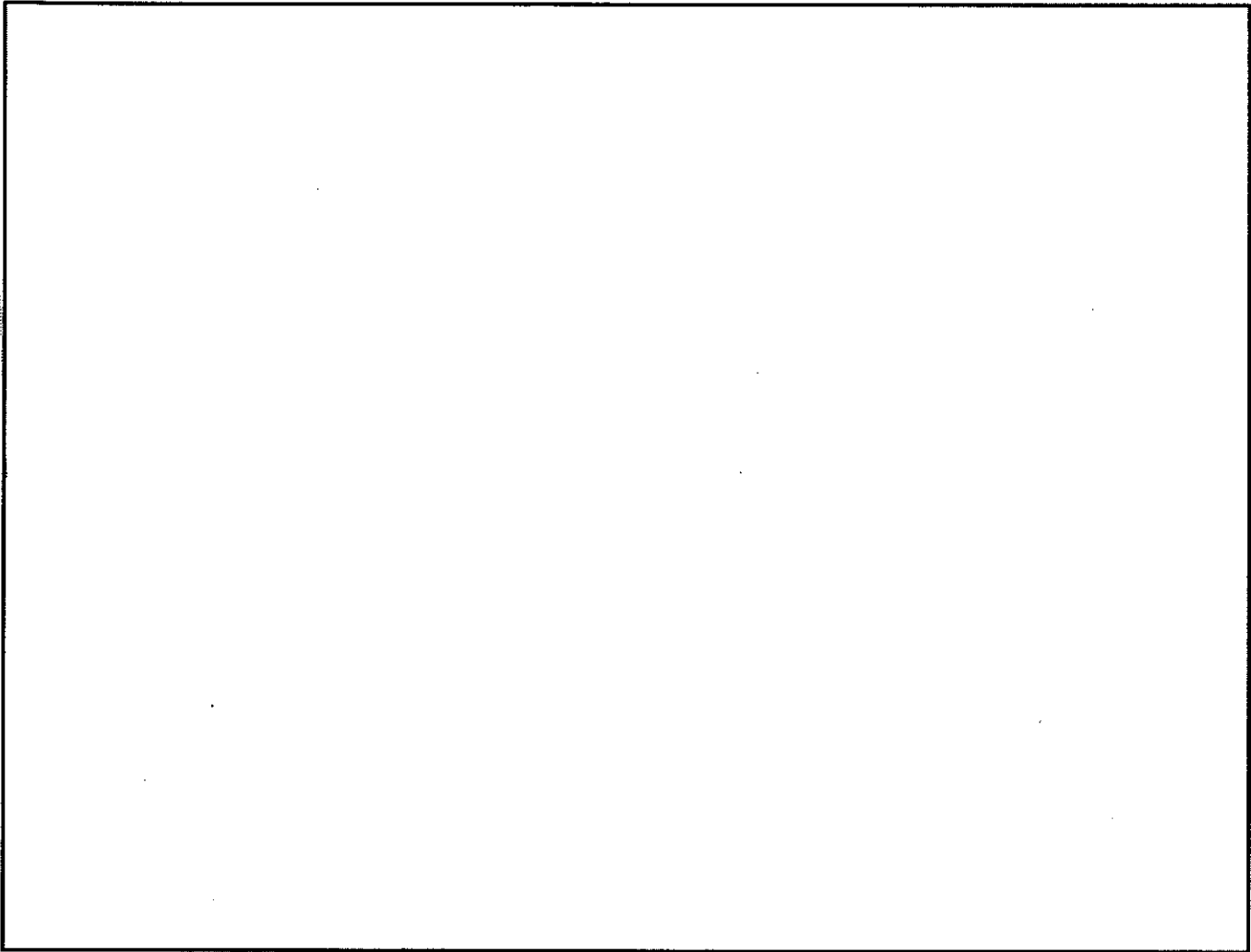
b1

~~SECRET~~

To: Cyber From: Cincinnati
Re: [REDACTED] 02/23/2007

b2
b7A

(S)



b1

~~SECRET~~

SECRET

To: Cyber From: Cincinnati
Re: [REDACTED] 02/23/2007

b2

LEAD(s):

Set Lead 1: (Info)

CYBER

AT C3IU-2, DC

Read and clear.

Set Lead 2: (Action)

OPERATIONAL TECHNOLOGY

AT CEAU, VA

End CIPAV operations in support of this case and send evidence to Cincinnati.

Set Lead 3: (Action)

CHICAGO

b1

(S) AT NRA1 [REDACTED]

Discontinue support of undercover accounts associated with this case and send bill for services to Cincinnati.

◆◆

SECRET

~~SECRET~~

[Redacted] (OTD) (FBI)

b6
b7C

From: [Redacted] (CI)(FBI)
Sent: Tuesday, February 20, 2007 3:44 PM
To: [Redacted] (CI) (FBI); [Redacted] (CI) (FBI); [Redacted] (CI) (FBI);
[Redacted] (CI) (FBI); [Redacted] (CyD) (FBI); [Redacted] (OTD) (FBI);
[Redacted] (CyD) (FBI); [Redacted] (JK) (FBI); [Redacted]
(JK) (FBI); [Redacted] (CyD) (FBI); [Redacted] (CyD)(FBI);
[Redacted] (CyD) (FBI); [Redacted] (OTD) (FBI); [Redacted]
(CyD) (FBI); [Redacted] (CI) (FBI); [Redacted] (CI)(FBI)

Subject: RE: Today's CIPAV report

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

CART in FL is working on it.

-----Original Message-----

From: [Redacted] (CI) (FBI)
Sent: Tuesday, February 20, 2007 3:33 PM
To: [Redacted] (CI)(FBI); [Redacted] (CI) (FBI); [Redacted] (CI) (FBI); [Redacted] (CI) (FBI); [Redacted]
[Redacted] (CyD) (FBI); [Redacted] (OTD) (FBI); [Redacted] (CyD) (FBI); [Redacted] (JK) (FBI);
[Redacted] (JK) (FBI); [Redacted] (CyD) (FBI); [Redacted] (CyD)(FBI);
[Redacted] (CyD) (FBI); [Redacted] (OTD) (FBI); [Redacted] (CyD) (FBI); [Redacted] (CI) (FBI); [Redacted]
[Redacted] (CI)(FBI)

Subject: RE: Today's CIPAV report

b6
b7C

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

[Redacted]

b2
b7E
b7D

SA [Redacted]

-----Original Message-----
From: [Redacted]
Sent: Tuesday, February 20, 2007 3:06 PM
To: [Redacted]

Subject: RE: Today's CIPAV report

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

I had the same question about [Redacted]

DATE: 02-09-2009
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 02-09-2034

b2
b7D
b7E

-----Original Message-----
From: [Redacted] (CI) (FBI)
Sent: Tuesday, February 20, 2007 3:06 PM
To: [Redacted] (CI) (FBI); [Redacted] (CI) (FBI); [Redacted] (CI) (FBI); [Redacted] (CyD) (FBI); [Redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

~~SECRET~~

[redacted] (OTD) (FBI); [redacted] (CvD) (FBI); [redacted] (JK) (FBI); [redacted] (CI)
[redacted] (FBI); [redacted] (JK) (FBI); [redacted] (CvD) (FBI); [redacted] (CvD) (FBI); [redacted] (CvD) (FBI);
[redacted] (CvD) (FBI); [redacted] (OTD) (FBI); [redacted] (CvD) (FBI); [redacted]
[redacted] (CI) (FBI); [redacted] (CI) (FBI)

Subject: RE: Today's CIPAV rerport

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

b6
b7C

A link chart would help me (as I am a little slow), but I have a question about [redacted]

b2
b7D
b7E

[redacted]

SA [redacted]

b6
b7C

-----Original Message-----

From: [redacted] (CI) (FBI)
Sent: Tuesday, February 20, 2007 2:44 PM
To: [redacted] (CI) (FBI); [redacted] (CI) (FBI); [redacted] (CvD) (FBI); [redacted] (OTD) (FBI); [redacted] (CvD) (FBI); [redacted] (JK) (FBI); [redacted] (CI) (FBI); [redacted] (CI) (FBI); [redacted] (JK) (FBI); [redacted] (CvD) (FBI); [redacted] (CvD) (FBI); [redacted] (CvD) (FBI); [redacted] (OTD) (FBI); [redacted] (CvD) (FBI); [redacted] (CI) (FBI); [redacted] (CI) (FBI); [redacted] (CI) (FBI); [redacted] (CI) (FBI)
Subject: FW: Today's CIPAV rerport

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

SA [redacted]

Desk
Nextel
Direct connect
[redacted]

b6
b7C
b2

-----Original Message-----

From: [redacted] (OS) (FBI)
Sent: Tuesday, February 20, 2007 2:21 PM
To: [redacted] (CI) (FBI); [redacted] (CI) (FBI); [redacted] (CI) (FBI)
Subject: Today's CIPAV rerport

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

Hi Guys,

I hope everything is going well with your investigation. WE've been looking at the CIPAV stuff today and I have the following report to add from recent activity. We're still looking at stuff and expect a second report maybe tomorrow morning, but we're trying to feed you info as fast as possible.

b2
b7E

[redacted]

We're thinking a conference call maybe tomorrow might be a good idea?

b1

[redacted]

(S)

~~SECRET~~

~~SECRET~~

[Redacted]

b1

(S)

Here's the report for today:

[Redacted]

Ps. I'm heading out right now, but feel free to try me on my cell if you need anything or have any questions

[Redacted]

b6
b7C
b2

+++++

[Large Redacted Area]

(S)

b1

~~SECRET~~

~~SECRET~~

[Redacted]

(S)

[Large Redacted Area]

(S)

b1

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SECRET~~

~~SECRET~~

[Redacted] (OTD) (FBI)

b6
b7C

From: [Redacted] (CI) (FBI)
 Sent: Thursday, February 15, 2007 5:06 PM
 To: [Redacted] (CI) (FBI); [Redacted] (CI) (FBI); [Redacted] (CyD) (FBI);
 [Redacted] (OTD) (FBI); [Redacted] (CyD) (FBI); [Redacted]
 (JK) (FBI); [Redacted] (CI) (FBI); [Redacted] (CI) (FBI); [Redacted]
 (JK) (FBI); [Redacted] (CyD) (FBI); [Redacted] (CyD) (FBI); [Redacted]
 [Redacted] (OTD) (FBI); [Redacted] (CyD) (FBI); [Redacted] (CI) (FBI);
 [Redacted] (CI) (FBI); [Redacted] (CI) (FBI)
 Subject: [Redacted] - CIPAV may have deployed

b2
b1
b2
b7E
b7A

~~SENSITIVE BUT UNCLASSIFIED~~
~~RECORD~~ [Redacted]

(S)

[Redacted]

SA [Redacted]
 [Redacted] Desk
 [Redacted] Nextel
 [Redacted] Direct connect
 [Redacted]

b6
b7C
b2

~~SENSITIVE BUT UNCLASSIFIED~~

DATE: 02-24-2009
 CLASSIFIED BY 60322UC/LP/STP/gjg
 REASON: 1.4 (C)
 DECLASSIFY ON: 02-24-2034

ALL INFORMATION CONTAINED
 HEREIN IS UNCLASSIFIED EXCEPT
 WHERE SHOWN OTHERWISE

~~SECRET~~

[redacted] (OTD) (FBI)

b6
b7C

From: [redacted] (CI) (FBI)
 Sent: Wednesday, February 14, 2007 8:56 AM
 To: [redacted] (CI) (FBI); [redacted] (CI) (FBI); [redacted] (CyD) (FBI);
 [redacted] (OTD) (FBI); [redacted] (CyD) (FBI); [redacted] (JK) (FBI);
 [redacted] (CI) (FBI); [redacted] (CI) (FBI); [redacted] (JK) (FBI);
 [redacted] (CyD) (FBI); [redacted] (CyD) (FBI); [redacted] (OTD) (FBI);
 [redacted] (CyD) (FBI); [redacted] (CI) (FBI); [redacted] (CI) (FBI);
 Subject: [redacted] CIPAV update

b7A
b2

~~SENSITIVE BUT UNCLASSIFIED~~
~~RECORD~~ [redacted]

[redacted]

The investigating Agent checked the log files for the CIPAV being operated pursuant to a federal search warrant obtained on 02/12/2007. The previous update discussed log entries [redacted] As of 8:03 a.m. this morning (02/14/2007) we saw new [redacted] entries. The new entries occurred between [redacted]

b1
b2
b7E

(S) [redacted]

[redacted]

SA [redacted]
 Desk
 Nextel
 Direct connect
 [redacted]

b6
b7C
b2

~~SENSITIVE BUT UNCLASSIFIED~~

DATE: 02-09-2009
 CLASSIFIED BY 60322UC/LP/STP/gjg
 REASON: 1.4 (C)
 DECLASSIFY ON: 02-09-2034

ALL INFORMATION CONTAINED
 HEREIN IS UNCLASSIFIED EXCEPT
 WHERE SHOWN OTHERWISE

[Redacted] (OTD) (FBI)

From: [Redacted] (CI) (FBI)
Sent: Tuesday, February 13, 2007 2:55 PM
To: [Redacted] (CI) (FBI); [Redacted] (CI) (FBI); [Redacted] (CvD) (FBI);
[Redacted] (OTD) (FBI); [Redacted] (CvD) (FBI); [Redacted] (JK) (FBI); [Redacted] (CI) (FBI); [Redacted] (CI) (FBI); [Redacted] (JK) (FBI); [Redacted] (CvD) (FBI); [Redacted] (CvD) (FBI); [Redacted] (OTD) (FBI); [Redacted] (CvD) (FBI); [Redacted] (CI) (FBI); [Redacted] (CI) (FBI)

~~SENSITIVE BUT UNCLASSIFIED~~
~~RECORD~~ [Redacted]

b2
b7E
b7A

This is the [Redacted] Daily Update for February 13, 2007:

On Friday, 02/09/2007, our CIPAV search warrant expired and monitoring was shut down. It was the opinion of our AUSA that a seamless renewal of the CIPAV was not possible because search warrant execution periods can not be extended. On Monday, 02/12/2007, we learned that [Redacted]
[Redacted] After learning this, I drafted a new affidavit. On the evening of 02/12/2007, I made return on the five previous search warrants, marking them unexecuted. I then obtained five new search warrants and provided faxed copies to CEAU/ERF. At 7:16 p.m. the CIPAV again became functional.

(S) Starting at 12:23 p.m. EDT on 02/13/2007, we again began to observe activity [Redacted] This time [Redacted]
(S) [Redacted] b1
[Redacted] b2
[Redacted] b7E
[Redacted] b7A
[Redacted] Analysis of the logs indicates the Unsub(s) are using [Redacted] (S)

We are still looking at the logs to determine what we now know. At 2:46 p.m., I spoke with UC [Redacted] about interpretation of the logs. She indicated that she would conduct liaison with STAS to obtain interpretation of the logs.

b2
b7E
b6
b7C
b7A

Expect another update tomorrow.

Sincerely,

SA [Redacted]
[Redacted] Desk
[Redacted] Nextel
[Redacted] Direct connect
[Redacted]

DATE: 02-24-2009
CLASSIFIED BY 60322UC/LP/STP/gjg b6
REASON: 1.4 (C) b7C
DECLASSIFY ON: 02-24-2034 b2

~~SENSITIVE BUT UNCLASSIFIED~~

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (OTD)(FBI)
Sent: Friday, February 09, 2007 9:40 AM
To: [redacted] (OTD) (FBI)
Cc: [redacted] (OTD)(CON); [redacted] (OTD)(CON)
Subject: RE: Shut down CIPAV

~~SENSITIVE BUT UNCLASSIFIED~~
~~RECORD~~ [redacted]

b2

b6
b7C
b2
b7E

Per your directions, as of 0935 on 9 Feb 2007 the case was closed [redacted]

J...

[redacted]
Information Technology Specialist
Operational Technology Division
Office [redacted]
Mobile [redacted]
Pager [redacted]

-----Original Message-----

From: [redacted] (OTD) (FBI)
Sent: Friday, February 09, 2007 :34 AM
To: [redacted] (OTD)(FBI)
Subject: FW: Shut down CIPAV
Importance: High

~~SENSITIVE BUT UNCLASSIFIED~~
~~RECORD~~ [redacted]

b2

[redacted]

b6
b7C
b2

Read below and execute ASAP!

Thanks,

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

[redacted] (desk)
[redacted] (cell)
[redacted] (fax-unclass)

-----Original Message-----

From: [redacted] (CI) (FBI)
Sent: Friday, February 09, 2007 :07 AM
To: [redacted] (OTD) (FBI); [redacted] (CyD) (FBI); [redacted] (CI) (FBI); [redacted] (CI)(FBI); [redacted] (CyD) (FBI)
Subject: Shut down CIPAV
Importance: High

~~SENSITIVE BUT UNCLASSIFIED~~
~~RECORD~~ [redacted]

~~SECRET~~

DATE: 02-09-2009
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 02-09-2034

b2

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

b6
b7C

Dear SSA [redacted]

(S)

b1

[redacted]

[redacted]

This record e-mail will be followed by an EC.

(S)

Sincerely,

SA [redacted]

[redacted]

Desk
Nextel
Direct connect

b6
b7C
b2

[redacted]

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (CI) (FBI)
Sent: Wednesday, January 31, 2007 3:55 PM
To: [redacted] (OTD) (FBI)
Subject: RE: [redacted]

**SENSITIVE BUT UNCLASSIFIED
RECORD** [redacted]

b2
b7E

Please notify me at the numbers listed below:

b6
b7C
b2

SA [redacted]
[redacted] Desk
[redacted] Nextel
[redacted] Direct connect
[redacted]

-----Original Message-----

From: [redacted] (OTD) (FBI)
Sent: Wednesday, January 31, 2007 3:52 PM
To: [redacted] (CI) (FBI)
Cc: [redacted] (CI) (FBI)
Subject: RE: [redacted]

b6
b7C
b2
b7E

**SENSITIVE BUT UNCLASSIFIED
RECORD** [redacted]

b2

[redacted]
We are ready to go. [redacted]
[redacted]
[redacted]

Thanks,
Kd

-----Original Message-----

From: [redacted] (CI) (FBI)
Sent: Wednesday, January 31, 2007 12:05 PM
To: [redacted] (CI) (FBI); [redacted] (IP) (FBI); [redacted] (CG) (FBI); [redacted] (CyD) (FBI); [redacted] (CyD) (FBI); [redacted] (CI) (FBI); [redacted] (OTD) (FBI)
Subject: [redacted]

b6
b7C

**SENSITIVE BUT UNCLASSIFIED
RECORD** [redacted]

b2

b6
b7C
b2
b7E

Dear UC [redacted] et al,

As of noon on 01/31/2007, [redacted]
[redacted] We await word from ERF that the CIPAVs have been triggered.

Best wishes,

SA [redacted]
[redacted] Desk

[Redacted] Nextel
Direct connect
[Redacted]

b6
b7C
b2

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (OTD)(FBI)
Sent: Friday, January 12, 2007 3:10 PM
To: [redacted] (OTD) (FBI)
Subject: [redacted]

b6
b7C

b2
b7E

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] I have received the following RMS request. It looks similar to [redacted] but don't know if it is or not.

Here is the RMS info.

b2
b7E

[redacted]

Case is 315Q

Requested Support is:

[redacted]

b1

(S)

Contact [redacted]

b6
b7C

SENSITIVE BUT UNCLASSIFIED

DATE: 09-26-2008
CLASSIFIED BY 0322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 09-26-2033

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

[redacted] (OTD) (FBI)

b6
b7C

From: [redacted] (OTD) (FBI)
Sent: Friday, January 12, 2007 12:36 PM
To: [redacted] (SI) (FBI)
Cc: [redacted] (CTD) (FBI)
Subject: FW: [redacted]

UNCLASSIFIED
NON-RECORD

b6
b7C

[redacted]

Review the below listed opinion. If possible, execute on as many of the suggestions as you can. If you think of any other steps you can take, excluding ones we have already discussed, implement them so that [redacted] [redacted]

b2
b7E

Thanks,

SSA [redacted]
Operational Technology Division
Digital Evidence Section
Cryptologic and Electronic Analysis Unit
Software Development Group
[redacted] (desk)
[redacted] (cell)
[redacted] (fax-unclass)

b6
b7C
b2

-----Original Message-----

From: [redacted] (OGC) (FBI)
Sent: Thursday, January 11, 2007 5:19 PM
To: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OGC) (FBI)
Subject: RE: [redacted]

b6
b7C
b2

UNCLASSIFIED
NON-RECORD

Cc to [redacted]

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

[redacted]

**Associate General Counsel - Unit Chief
Science & Technology Law Unit
Engineering Research Facility
Bldg 27958A, Room A-207
Quantico, VA 22135
Tel. [redacted]
Fax. [redacted]**

-----Original Message-----

From: [redacted] (OGC) (FBI)

Sent: Thursday, January 11, 2007 5:17 PM

To: [redacted] (OGC) (FBI)

Cc: [redacted] (OTD) (FBI)

Subject: [redacted]

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted]

As discussed, I concur that the CEAU proposal [redacted]

[redacted]

b2
b7E
b5

[redacted]

[redacted]

Ultimately, these facts not only need to be document, but we will need to know who witnessed each of them as a precaution to proving that there was not a domestic tracking without a court order [redacted]

[redacted]

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

~~SECRET~~

[redacted] (OTD) (FBI)

b6
b7c

From: [redacted] (OTD) (FBI)
Sent: Tuesday, January 09, 2007 12:51 PM
To: [redacted] (CyD) (FBI)
Subject: RE: Technical Question regarding the use of IPAV

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

[redacted]

b1

Sorry for the dealyed response. To answer your question [redacted]

(S)

-----Original Message-----

From: [redacted] (CyD) (FBI)
Sent: Friday, January 05, 2007 8:58 AM
To: [redacted] (OTD) (FBI)
Cc: [redacted] (CyD) (FBI)
Subject: Technical Question regarding the use of IPAV

b6
b7c
b2

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

[redacted]

I have a question regarding possible countermeasures that could be used against the IPAV. [redacted]

(S)

b2
b7E

(S)

b1

Thanks,

Supervisory Special Agent [redacted]
CATU - Cyber Division (HQ)

(W)
(C)
(F)
(E)

"I protect that which is most important" - Seraph

~~UNCLASSIFIED~~

~~UNCLASSIFIED~~

DATE: 02-24-2009
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 02-24-2034

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (OTD) (FBI)
Sent: Friday, January 05, 2007 7:58 AM
To: [redacted] (HO) (FBI)
Subject: RE: INFORMATION TO CEAU RE CIPAV REQUEST

b6
b7C

~~SECRET~~
~~RECORD~~

[redacted]

{S}

b1

[redacted]

Not a problem. Glad we could help. Happy New Year!!

-----Original Message-----

From: [redacted] (HO) (FBI)
Sent: Thursday, January 04, 2007 5:36 PM
To: [redacted] (OTD) (FBI)
Subject: RE: INFORMATION TO CEAU RE CIPAV REQUEST

b6
b7C

~~SECRET~~
~~RECORD~~

[redacted]

{S}

b1

Hi [redacted] Hope you had a good holidays. I just got back today and I want to apologize for the rush to get the cipav request handled last week. I asked and was told the request would not be made until this week. Apparently [redacted] personnel and AUSA decided otherwise. Again, I apologize for the mix up. On the bright side, [redacted]

[redacted] Thanks for all your help.

b2
b7E
b7A

-----Original Message-----

From: [redacted] (OTD) (FBI)
Sent: Thursday, December 21, 2006 4:17 PM
To: [redacted] (HO) (FBI); [redacted] (OTD)(FBI)
Cc: [redacted] (HO) (FBI); [redacted] (HO) (OGA); [redacted] (HO) (OGA); [redacted] (HO) (FBI)
Subject: RE: INFORMATION TO CEAU RE CIPAV REQUEST

~~SECRET~~
~~RECORD~~

[redacted]

{S}

b1
b6
b7C

[redacted]

I know that some of our requests are already in the process of being completed. However, I just wanted to document the telephone conversation that my engineers and I had with [redacted] in this email. Thus, per our telephone call, the attached word document contains the requested information that we discussed.

<< File: houstonquestions.doc >>

Thanks for the quick response,

DATE: 09-26-2008
CLASSIFIED BY 0322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 09-26-2033

Kd

-----Original Message-----

From: [redacted] (HO) (FBI)
Sent: Thursday, December 21, 2006 2:43 PM
To: [redacted] (OTD) (FBI); [redacted] (OTD)(FBI)
Cc: [redacted] (HO) (FBI); [redacted] (HO) (OGA); [redacted] (HO) (OGA); [redacted] (HO) (FBI)
Subject: INFORMATION TO CEAU RE CIPAV REQUEST
Importance: High

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

~~SECRET~~

(S) RECORD [redacted]

b1
b7A
b2
b7E
b6
b7C

(S) << File: E-mail.wpd >>
Attached is the E-mail which we intend to [redacted]

(S) [redacted]

Please call if you have any further questions.

SA [redacted]
Houston Squad CT-5
(O) [redacted]
(C) [redacted]

b6
b7C
b2

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign Counterintelligence Investigations
DECLASSIFY ON: 20311221
SECRET~~

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign Counterintelligence Investigations
DECLASSIFY ON: 20311221
SECRET~~

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign Counterintelligence Investigations
DECLASSIFY ON: 20311221
SECRET~~

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign Counterintelligence Investigations
DECLASSIFY ON: 20311221
SECRET~~

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (CI) (FBI)
Sent: Thursday, January 04, 2007 2:56 PM
To: [redacted] (OTD) (FBI)
Subject: Web Bug Affidavit

SENSITIVE BUT UNCLASSIFIED
RECORD [redacted]

b2

b6
b7C
b2

Dear SSA [redacted]

I've enclosed a copy of our proposed CIPAV affidavit for use in the captioned matter. Please review and make any changes you feel necessary. When making changes, use the revision feature of WordPerfect so that changes can be automatically incorporated into the final document.

Best wishes,

SA [redacted]
[redacted] Desk
[redacted] Nextel
[redacted] Direct connect

[redacted]



Web Bug
ffidavit.wpd (57 KB)

SENSITIVE BUT UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-24-2008 BY 60322UC/LP/STP/gjg

[redacted] (OTD) (FBI)

From: [redacted] (OTD) (FBI)
Sent: Thursday, December 21, 2006 6:09 PM
To: [redacted] (HO) (FBI)
Subject: FW: PR/TT Example

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

Attached is a pony to used in constructing your order for the CIPAV. If you have any questions, please contact

[redacted]

Thanks,

Kd

-----Original Message-----

From: [redacted] (OGC) (FBI)
Sent: Wednesday, December 20, 2006 9:51 AM
To: [redacted] (OTD) (FBI)
Subject: FW: PR/TT Example

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
b7C
b2



oen_pony.PDF (149 KB)

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

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

~~SECRET~~

[redacted] (OTD) (FBI)

b6
b7C

From: [redacted] (OTD) (FBI)
Sent: Thursday, December 21, 2006 10:48 AM
To: [redacted] (HO) (FBI)
Subject: RE: 2ND DRAFT EC REQUESTING CEAU ASSISTANCE

~~SECRET//ORCON,NOFORN~~
~~RECORD~~ [redacted]

{S}

Can you call me ASAP? I need some additional info regarding [redacted]

b2
b7E

-----Original Message-----

From: [redacted] (HO) (FBI)
Sent: Thursday, December 21, 2006 10:13 AM
To: [redacted] (OTD) (FBI)
Subject: FW: 2ND DRAFT EC REQUESTING CEAU ASSISTANCE
Importance: High

b6
b7C

~~SECRET//ORCON,NOFORN~~
~~RECORD~~ [redacted]

{S}

b1

Just wanted to make sure you were aware of this. Any thing you need me to do?

-----Original Message-----

From: [redacted] (HO) (FBI)
Sent: Tuesday, December 19, 2006 2:45 PM
To: [redacted] (HO) (FBI)
Cc: [redacted] (HO) (OGA); [redacted] (HO) (OGA); [redacted] (HO) (FBI)
Subject: FW: 2ND DRAFT EC REQUESTING CEAU ASSISTANCE
Importance: High

~~SECRET//ORCON,NOFORN~~
~~RECORD~~ [redacted]

{S}

FYI, it looks like this is being supported by CEAU, and they should be reaching out to you, at some point.

We [redacted] are putting together an affidavit for the AUSA to get a court order. We're hoping to get some input from CEAU's AGC [redacted] before we send to the AUSA.

We won't set a date to take to the court until everyone's ready, as the 10 day period kicks in as soon as it's signed.

Does [redacted] get involved in this, or are you our POC for all things CIPAV related?

b6
b7C

Thanks.

-----Original Message-----

From: [redacted] (HO) (FBI)
Sent: Thursday, December 14, 2006 3:32 PM
To: [redacted] (OTD) (FBI)
Cc: [redacted] (HO) (OGA); [redacted] (HO) (OGA); [redacted] (HO) (FBI)

DATE: 02-12-2009
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 02-12-2034

~~SECRET~~

~~SECRET~~

Subject: 2ND DRAFT EC REQUESTING CEAU ASSISTANCE
Importance: High

~~SECRET//ORCON.NOFORN~~
RECORD

[Redacted]

{S}

b1

<< File: 348wdb01.wpd >>

[Redacted]

Per our discussion today, please see the attached EC and let me know if it looks sufficient for utilization of CIPAV in support of our case. If not, please suggest any changes, corrections, etc., and they will be made.

Many thanks.

b6
b7C
b2

SA [Redacted]
Houston Squad CT-5
(O) [Redacted]
(C) [Redacted]

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign Counterintelligence Investigations
DECLASSIFY ON: 20311214
SECRET//ORCON.NOFORN~~

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign Counterintelligence Investigations
DECLASSIFY ON: 20311219
SECRET//ORCON.NOFORN~~

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign Counterintelligence Investigations
DECLASSIFY ON: 20311219
SECRET//ORCON.NOFORN~~

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign Counterintelligence Investigations
DECLASSIFY ON: 20311219
SECRET//ORCON.NOFORN~~

~~SECRET~~

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (OTD) (FBI)
Sent: Thursday, December 14, 2006 5:01 PM
To: [redacted] (OGC) (FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OTD) (FBI)
Subject: RE: Search Return and Collection

b6
b7C

Follow Up Flag: Follow up
Due By: Tuesday, December 19, 2006 9:00 AM
Flag Status: Completed

**SECRET//ORCON,NOFORN
RECORD** [redacted]

(S)

[redacted]

Concerning the Houston matter, execute using simplest tool possible pending proper legal authority.

b1

[redacted]

b6
b7C

-----Original Message-----

From: [redacted] (OGC) (FBI)
Sent: Thursday, December 14, 2006 2:13 PM
To: [redacted] (OTD) (FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OTD) (FBI)
Subject: RE: Search Return and Collection

**SECRET//ORCON,NOFORN
RECORD** [redacted]

(S)

[redacted]

The list below looks good.

b2
b7E
b7A

FYI, I spoke with the AUSA in Houston today re CEAU support [redacted].
[redacted] He understands the legal requirements and he understands that at most he will get only circumstantial evidence [redacted].
He wants to do it. Case Agent will be calling [redacted] with details.

[redacted] as this is a criminal case, [redacted] and given that the AUSA only needs [redacted]

[redacted]

b5

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

b6
b7C
b2

Ph [redacted]
Cell [redacted]
Ph (Secure) [redacted]
Fax [redacted]

DATE: 09-26-2008
CLASSIFIED BY 0322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 09-26-2033

~~SECRET~~

-----Original Message-----

From: [redacted] (OTD) (FBI)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

Sent: Thursday, December 14, 2006 12:58 PM
To: [redacted] (OGC) (FBI)
Subject: RE: Search Return and Collection

b6
b7C

~~SECRET//ORCON,NOFORN~~
~~RECORD~~ [redacted]

(S)

Gentlemen,

To continue with the theme that a split of this mission has caused difficulties, it should be noted that last evening, CEAU had additional success in testing our planned solution. However, this morning, AGC [redacted] reviewed the current order is not adequate [redacted] SPU identifies the [redacted] (so identified in the draft EC that was not shared with CEAU until 12/12/2006). This information has been communicated to [redacted] NSLB for correction in the new order. [redacted] Further, if SPU had been successful in their attempts [redacted] situation as well. The old saying "Fools rush in..." comes to mind.

b2
b7E
b7A
b6
b7C

As promised, the following is a list of [redacted]

[redacted]

(S)

[Large redacted area]

b1
b2
b7E
b7A

(S)



b1

-----Original Message-----

From: [redacted] (OTD) (FBI)
Sent: Wednesday, December 13, 2006 7:08 PM
To: [redacted] (OTD)(FBI); DICLEMENTE, ANTHON P. (OTD) (FBI)
Cc: [redacted] (OTD) (FBI)
Subject: RE: Search Return and Collection

SECRET//ORCON,NOFORN
RECORD [redacted]

(S)

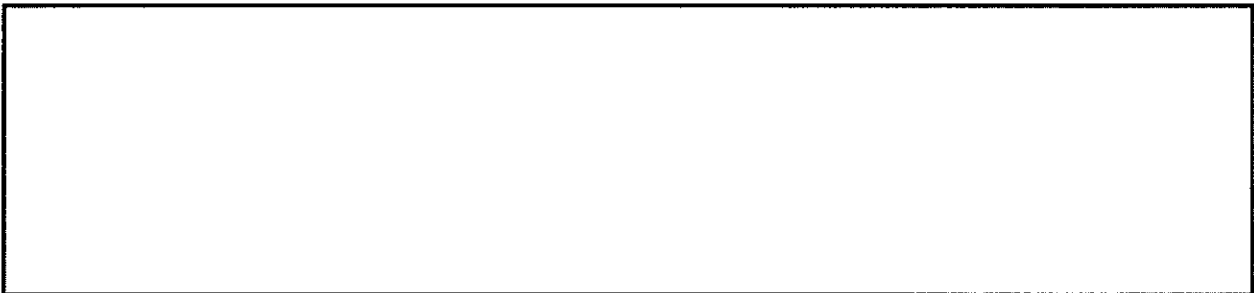
The timeline is attached. There have been multiple problems with getting this matter successfully deployed, not the least of which has been difficulty with coordinating efforts between the two entities involved, SPU and CEAU. Specifically, this lack of coordination manifested itself in the following:

1. CEAU was unaware of the amount of information that SPU had concerning [redacted]
[redacted]
[redacted] This was critical and lead to unnecessary delays.

2. [redacted]
[redacted]

3. [redacted]
[redacted]
[redacted] This was critical and resulted in delays and lack of direction concerning CEAU's role in this matter.

Finally, this was one of many cases that CEAU/SDG was working on at the time, with successful deployments. In fact, CEAU has so many currently pending operations that I have borrowed an SSA from DITU to work an overseas matter. A full accounting will be forthcoming shortly.



~~SECRET~~

b6
b7C

b2
b7E
b7A
b6
b7C

~~SECRET~~

<< File: Pittsburgh case.doc >>

-----Original Message-----

From: [redacted] (OTD)(FBI)
Sent: Wednesday, December 13, 2006 5:08 PM
To: DICLEMENTE, ANTHON P. (OTD) (FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OTD) (FBI)
Subject: RE: Search Return and Collection

b6
b7C

(S) ~~SECRET//ORCON.NOFORN~~
~~RECORD~~ [redacted]

b1

Tony,

Did you get the timeline yet?

[redacted]

-----Original Message-----

From: DICLEMENTE, ANTHON P. (OTD) (FBI)
Sent: Wednesday, December 13, 2006 3:30 PM
To: [redacted] (OTD)(FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OTD) (FBI)
Subject: FW: Search Return and Collection
Importance: High

b6
b7C

~~SECRET//ORCON,NOFORN~~
~~RECORD~~ [redacted]

b1

(S)

[redacted] - FYI re the return for [redacted]

Anthony P. DiClemente
Chief, Digital Evidence Section
Operational Technology Division

[redacted]

b2

-----Original Message-----

From: [redacted] (OGC) (FBI)
Sent: Monday, December 11, 2006 3:59 PM
To: [redacted] (OTD) (FBI); [redacted] (CyD) (FBI)
Cc: DICLEMENTE, ANTHON P. (OTD) (FBI); [redacted] (CyD) (FBI); [redacted] (CyD) (FBI); [redacted] (OGC)(FBI); [redacted] (CTD) (FBI); [redacted] (CTD) (FBI); [redacted] (PG) (FBI); [redacted] (PG) (FBI); [redacted] SSA F. (OGC)(FBI)
Subject: FW: Search Return and Collection
Importance: High

b7A
b2
b7E
b6
b7C

~~SECRET//ORCON.NOFORN~~
~~RECORD~~ [redacted]

b1

(S)

[redacted]

SPU forwarded a draft EC to [redacted] in November for his review [redacted]

[redacted] Per conversation with [redacted]

this morning, he has drafted the portion of the return related to [redacted] not need further information from us. As [redacted] is aware, the actual search and surveillance has not yet been effected...we anticipated execution of the search/surveillance authority to occur

~~SECRET~~

~~SECRET~~

tomorrow...SPU will provide additional input [redacted]
support of this effort. I'll defer to [redacted] and the operational side to provide more details on what's
going on there....

[redacted]
Assistant General Counsel
Science and Technology Law Unit
Special Technologies and Applications Office
[redacted]

b2
b7E
b7A
b6
b7C

-----Original Message-----
From: [redacted] (CyD) (FBI)
Sent: Monday, December 11, 2006 3:34 PM
To: [redacted] (OGC) (FBI)
Subject: FW: Search Return and Collection
Importance: High

SECRET//ORCON.NOFORN
RECORD [redacted]

b1

(S)

FYI

-----Original Message-----
From: [redacted] (CTD) (FBI)
Sent: Monday, December 11, 2006 12:37 PM
To: [redacted] (OTD) (FBI); [redacted] (CyD) (FBI)
Cc: DICLEMENTE, ANTHON P. (OTD) (FBI); [redacted] (CyD) (FBI); [redacted] (CyD) (FBI);
[redacted] (OGC)(FBI); [redacted] (CTD) (FBI); [redacted] (CTD) (FBI);
[redacted] (PG) (FBI); [redacted] (PG) (FBI); [redacted] (OGC)(FBI)
Subject: Search Return and Collection
Importance: High

b6
b7C

SECRET//ORCON.NOFORN
RECORD [redacted]

b1

(S)

b2
b7E
b7A
b6
b7C

All,

Referencing telephone call with OGC Atty [redacted] 12/11/06:
CTD needs the Search Return for the conducted survey as soon as possible, today if possible.
Unbelievably even more important, to state the obvious, we, the FBI, need to collect intel [redacted]

[redacted]

SPU- Does PG have what they need to submit the Search Return? CTD needs that Search Return
as soon as possible, if not today.
CEAU- CTD briefed the FISA Review Board that 12/18/06 was the projected collection date. Legally,
we need collection even sooner, if possible, for presentation to the FISC. Upon
collection, please provide PG with the specifics so that they can submit the Search Return.
OGC- Legally, are we on point here?
PG- Any operational highlights?

b6
b7C


Not intending to add to the administrative requirements, please copy myself and [redacted] on
all communications, e-mail and telephone calls, to ensure proper coordination of efforts. CTD is
required to coordinate the efforts of FBIHQ/CTD, FBI PG, CEAU/OTD, OST/SPU, OGC/NSLB, and
OIPR, and answer to the FISC.

Thanks

~~SECRET~~

~~SECRET~~



SSA 
FBIHQ/CTD/LX1
ITOS 1/CONUS 1
Rm 4W158
Desk
Pgr
Internal Secure



b2
b6
b7C

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFY ON: 20311211
SECRET//ORCON,NOFORN

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFY ON: 20311211
SECRET//ORCON,NOFORN

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFY ON: 20311211
SECRET//ORCON,NOFORN

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFY ON: 20311211
SECRET//ORCON,NOFORN

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFY ON: 20311211
SECRET//ORCON,NOFORN

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFY ON: 20311211
SECRET//ORCON,NOFORN

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFY ON: 20311211
SECRET//ORCON,NOFORN

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFY ON: 20311211
SECRET//ORCON,NOFORN

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFY ON: 20311211
SECRET//ORCON,NOFORN

~~SECRET~~

~~SECRET//ORCON//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY

Date: 12/14/2006

To: Operational Technology

Attn: Cryptologic & Electronic
Analysis Unit

UC [redacted]
SSA [redacted]

b6
b7C

From: Houston

CT-1

Contact: SA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted] wdb

Case ID #: [redacted] (Pending)

Title: [redacted] (S)

Full Investigation Initiated: 01/11/2005 (USPER).

Reference: [redacted] (S)

(U) [redacted]

[redacted] (S)

b1
b7A
b2
b7E

~~(S) Derived From: G-3
Declassify On: 12/14/2031~~

[redacted] (S)

(S)

~~SECRET//ORCON//NOFORN~~

DATE: 12-23-2008
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 12-23-2033

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

To: Operational Technology From: Houston

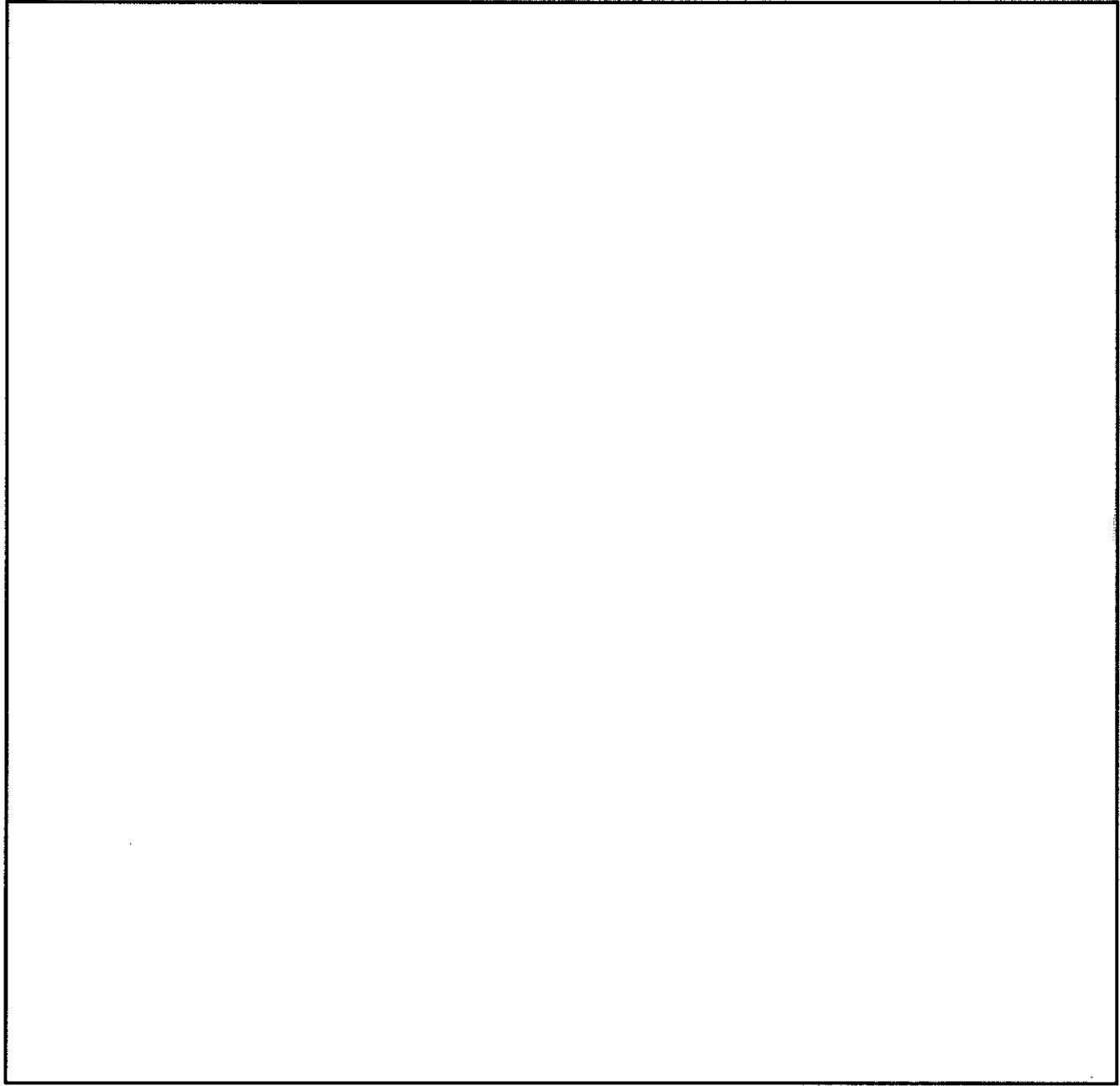
Re: (S) [redacted] 12/14/2006

b1

(S)

Details:

BACKGROUND



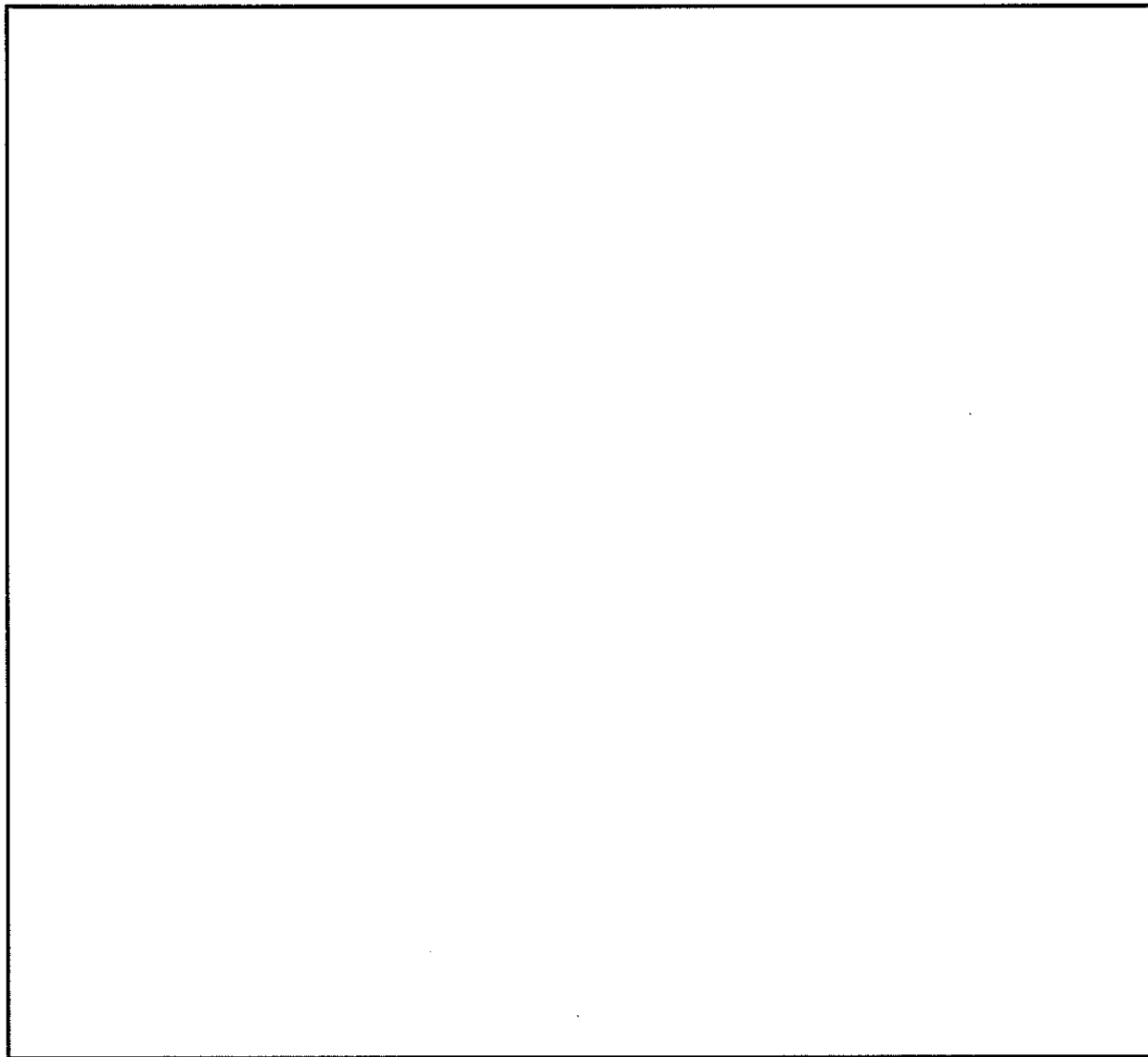
(S)

b1

To: Operational Technology From: Houston
Re: (S) [redacted] 12/14/2006

b1

(S)



(S)

b1



(S)

b1

To: Operational Technology From: Houston
Re: (S) [redacted] 12/14/2006
(S)

b1

(S) (U) Houston Division has developed a Confidential
Witness (CW) who is willing to assist with this investigation by

[redacted]

(S)

[redacted]

b1

SECRET//ORCON/NOFORN

To: Operational Technology From: Houston
Re: (S) [redacted] 12/14/2006
(S)

b1

LEAD(s):

Set Lead 1: (Action)

OPERATIONAL TECHNOLOGY

AT CRYPTOLOGIC & ELECTRONIC ANALYSIS UNIT

[redacted]

b1

(S)

◆◆

SECRET//ORCON/NOFORN

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (OTD) (FBI) b6
Sent: Thursday, December 14, 2006 11:05 AM b7C
To: [redacted] (OTD) (FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OTD)(FBI); [redacted] (ITD)
(FBI); [redacted] (OTD) (FBI)
Subject: [redacted]

~~SENSITIVE BUT UNCLASSIFIED~~
RECORD [redacted]

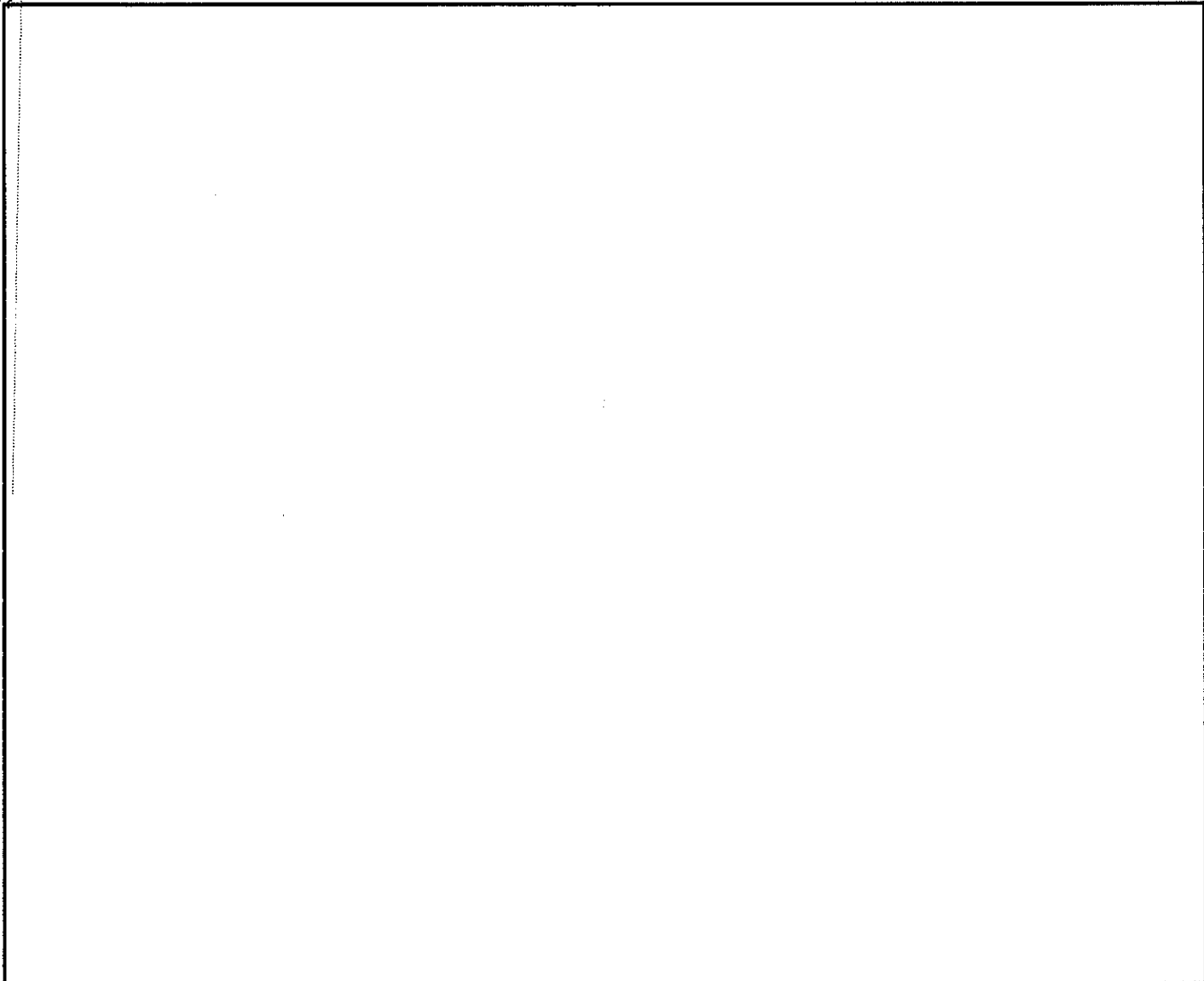
b2
b7E



Per your request, below denotes [redacted]

Active Deployments

(S)



b1

~~SECRET~~

~~SECRET~~

SSA [redacted]
Software Development Group (SDG)
Cryptologic Electronic Analysis Unit (CEAU)
Digital Evidence Section (DES)
Operational Technology Division (OTD)

b6
b7C
b2

[redacted] (desk)
[redacted] (cell)

~~SENSITIVE BUT UNCLASSIFIED~~

~~SECRET~~

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (OTD) (FBI)
Posted At: Wednesday, December 06, 2006 10:33 AM
Conversation: (S) [redacted] Concerning Conversation w/ [redacted] on 12/6/2006
Posted To: (S) [redacted] Phone Conversations
Subject: [redacted] Concerning Conversation w/ [redacted] on 12/6/2006
Categories: (S) Document Phone Conversation

b6
b7C

Telephonically contacted [redacted] and advised him that the request for CIPAV technology for use in the subject investigation was problematic due to the following concerns:

(S)

b1

[Large redacted area]

5. Requested that HO forward an EC providing a synopsis of the case, what they are trying to accomplish with the use of CEAU's technology, and a lead requesting assistance with the case.

DATE: 02-12-2009
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 02-12-2034

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (HO) (FBI) b6
Sent: Friday, December 01, 2006 4:58 PM b7C
To: [redacted] (HO) (OGA); [redacted] (HO) (OGA); [redacted] (OTD) (FBI)
Cc: [redacted] (HO) (FBI); [redacted] (HO) (FBI); [redacted]
Subject: [redacted] (HO) (FBI)
CIPAV REQUEST

SECRET//ORCON,NOFORN
RECORD [redacted]

b1

{S}

[redacted] with CEAU at ERF, phone [redacted] advised that he would like an explanation of what it is you want to accomplish with the CIPAV request. He would also like to review the proposed affidavit/court order for the CIPAV. Upon receipt of this info, he can prepare the CIPAV which can take several days. Please contact him as soon as possible to provide info requested. Thanks.

[redacted]
Squad SO-1
Houston Division

b2

[redacted] w
c

b6
b7C

-----Original Message-----

From: [redacted] (HO) (OGA)
Sent: Monday, November 27, 2006 11:01 AM
To: [redacted] (HO) (FBI)
Subject: RE: FISA

SECRET//ORCON,NOFORN
RECORD [redacted]

b1

{S}

Thanks for sending this to me

-----Original Message-----

From: [redacted] (HO) (FBI)
Sent: Monday, November 27, 2006 9:36 AM
To: [redacted] (HO) (OGA)
Subject: FW: FISA

SECRET//ORCON,NOFORN
RECORD [redacted]

b1

{S}

FYI

-----Original Message-----

From: [redacted] (HO) (FBI)
Sent: Friday, November 17, 2006 2:53 PM
To: [redacted] (HO) (FBI); [redacted] (HO) (OGA)
Cc: [redacted] (HO) (FBI); [redacted] (HO) (FBI)
Subject: RE: FISA

DATE: 02-12-2009
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 02-12-2034

SECRET//ORCON,NOFORN
RECORD [redacted]

b1

{S}

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

~~SECRET~~

[redacted]

I completed the RMS requests. All ERF needs now is a copy of the FISA order. So in addition to myself, [redacted] and [redacted] include [redacted] (CEAU), who is assigned the CIPAV request, and [redacted] (DITU), who is assigned the email intercepts, in the email with the FISA order attached. Also briefly describe in the email what you will be wanting from both CEAU and DITU. List your contact info in the email and this will start the ball rolling. Thanks.

-----Original Message-----

From: [redacted] (HO) (FBI)
Sent: Friday, November 17, 2006 2:08 PM
To: [redacted] (HO) (OGA)
Cc: [redacted] (HO) (FBI); [redacted] (HO) (FBI)
Subject: RE: FISA

b6
b7C

~~SECRET//ORCON,NOFORN~~
~~RECORD~~ [redacted]

b1

{S}

When you get the email with attachments, forward to me, [redacted] and [redacted]. Both [redacted] and I will be out next week so [redacted] will be available to get this started if you don't get it today. As soon as we get the order, we will forward to ERF and request via RMS their assistance with both the email and CIPAV requests. Thanks.

-----Original Message-----

From: [redacted] (HO) (OGA)
Sent: Friday, November 17, 2006 11:52 AM
To: [redacted] (HO) (FBI)
Cc: [redacted] (HO) (FBI); [redacted] (HO) (FBI); [redacted] (HO) (OGA)
Subject: FISA

b6
b7C

~~SECRET//ORCON,NOFORN~~
~~RECORD~~ [redacted]

b1

{S}

Hi [redacted]
Just a follow up to my telephone message. It looks like the FISA will be going to court today (I have not heard anything yet). So just giving you a heads up. [redacted]

I have also talked to [redacted] today about this case.
When I hear something, ill let you know.
Thanks

b2
b7E

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

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

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

~~SECRET~~

~~SECRET~~

[redacted] (OTD) (FBI)

Subject: CIPAV for [redacted]

b2
b7E

Status: Not Started
Percent Complete: 0%

b6
b7C

Total Work: 0 hours
Actual Work: 0 hours

Owner: [redacted] (OTD) (FBI)

Spoke with [redacted] Monday on Friday, December 1, 2006 @ 10:08am

b1

[redacted]

[redacted]

(S)

From: [redacted] (CTD) (FBI)
Sent: Friday, December 01, 2006 9:22 AM
To: [redacted] (OTD) (FBI)
Subject: CIPAV for [redacted]

b6
b7C

b2
b7E

SECRET
RECORD 315N

[redacted]

b2
b7E

This is something that will probably eventually be deployed to all

[redacted]

[redacted]

b1

[redacted]

(S)

Thanks,

(S)

SSA [redacted]
CTD-CXS, EOPS
[redacted] desk
[redacted] cell
[redacted] pager

b2
b6
b7C

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign Counterintelligence Investigations
DECLASSIFY ON: 20311201
SECRET

DATE: 02-10-2009
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 02-10-2034

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (OTD) (FBI) b6
Sent: Tuesday, November 28, 2006 6:34 PM b7C
To: [redacted] (OTD) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] (OTD) (FBI)
Subject: RE: CIPAV court orders - Re 315Q-SL-191661 (Case Agent [redacted])

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

Silly question here, but this message says that these were signed on 22 November. [redacted]

-----Original Message-----

From: [redacted] (OGC) (FBI) b6
Sent: Tuesday, November 28, 2006 4:21 PM b7C
To: [redacted] (OTD) (FBI); [redacted] (OTD) (FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OGC) (FBI); [redacted] (OTD) (FBI)
Subject: CIPAV court orders - Re 315Q-SL-1916611 (Case Agent [redacted])

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

[redacted]

(S)

b1

The remaining four orders are authorize Pen Register Trap and Trace collections. 18 USC 3123. [redacted]

b2
b7E

All orders were signed on 22 November 2006 by a US Magistrate Judge (un-readable). Pursuant to [redacted] and following discussions and agreement with the supported AUSA, all eight orders expire at midnight on 21 December 2006.

Please ensure, absent a signed renewal order in hand, that CEAU's exploits are removed from [redacted] this expiration date/time.

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

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b2
b6
b7C

Ph - [redacted]
Cell [redacted]
Ph (Secure) - [redacted] DATE: 02-10-2009
Fax [redacted] CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 02-10-2034

~~SECRET~~

-----Original Message-----

From: [redacted] (SL)(FBI)
Sent: Friday, November 17, 2006 6:54 PM
To: [redacted] (OGC) (FBI)
Subject: CIPAV court orders

b6
b7C

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

[redacted] asked me to send these to you for your review (he does not have access to FBINET). These concern [redacted] You probably already have his number, but if [redacted] not, you can reach him at [redacted] or can reach me at [redacted] Thanks.

b6
b7C
b1
b2
b7E

<< [redacted] >> (S)

~~**SENSITIVE BUT UNCLASSIFIED**~~

~~**SENSITIVE BUT UNCLASSIFIED**~~

~~**SENSITIVE BUT UNCLASSIFIED**~~

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (OTD) (FBI)
Sent: Tuesday, November 28, 2006 5:14 PM
To: [redacted] (OTD)(FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OGC) (FBI); [redacted] (OTD) (FBI)
Subject: FW: CIPAV court orders - Re 315Q-SL-191661 (Case Agent [redacted])
Importance: High
Follow Up Flag: Follow up
Flag Status: Flagged

b6
b7C

~~SENSITIVE BUT UNCLASSIFIED
NON-RECORD~~

[redacted]
[redacted]

b1
(S)

It will be the case agent responsibility to get the renewal authorization to us well in advance to give the largest window of opportunity possible.

[redacted] will address this with the case agent and send a reminder.

[redacted] is the POC and he will coordinate with the field.

If you have questions please give me a call.

b6
b7C
b2

[redacted]
Unit Chief, Cryptologic & Electronic Analysis Unit (CEAU)
Digital Evidence Section
Operational Technology Division

[redacted]

-----Original Message-----

From: [redacted] (OGC) (FBI)
Sent: Tuesday, November 28, 2006 4:54 PM
To: [redacted] (OTD)(FBI); [redacted] (OTD) (FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OTD) (FBI)
Subject: RE: CIPAV court orders - Re 315Q-SL-191661 (Case Agent [redacted])
Importance: High

b6
b7C

~~SENSITIVE BUT UNCLASSIFIED
NON-RECORD~~

DATE: 02-10-2009
FBI INFO.
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 02-10-2034

b1

[redacted]

[redacted]

~~SECRET~~
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

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

b2
b6
b7C

-----Original Message-----

From: [redacted] (OTD)(FBI)
Sent: Tuesday, November 28, 2006 4:41 PM
To: [redacted] (OGC) (FBI); [redacted] (OTD) (FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OTD) (FBI)
Subject: RE: CIPAV court orders - Re 315Q-SL-191661 (Case Agent [redacted])

b1
b2
b7E
b6
b7C

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

Thanks [redacted]

[Large redacted block]

(S)

[redacted]
Information Technology Specialist
Operational Technology Division
Office - [redacted]
Mobile - [redacted]
Pager - [redacted]

-----Original Message-----

From: [redacted] (OGC) (FBI)
Sent: Tuesday, November 28, 2006 4:21 PM
To: [redacted] (OTD) (FBI); [redacted] (OTD)(FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OGC) (FBI); [redacted] (OTD) (FBI)
Subject: CIPAV court orders - Re 315Q-SL-191661 (Case Agent [redacted])

b6
b7C

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

[Large redacted block]

(S)

[Redacted block]

(S)

b1

~~SECRET~~

[redacted] (OTD) (FBI)

b6
b7C

From: [redacted] (OGC) (FBI)
Sent: Tuesday, November 21, 2006 3:00 PM
To: [redacted] (SL)(FBI)
Subject: RE: CIPAV court orders

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

One comment that has come in from my unit re the draft orders that should be forwarded to AUSA [redacted] is that he should also cite to the All Writs Act, 28 U.S.C. § 1651(a), given that neither Rule 41 nor 3117 provides for the ongoing execution of a SW--surveillance.

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

b2
b6
b7C

-----Original Message-----

From: [redacted] (SL)(FBI)
Sent: Friday, November 17, 2006 6:54 PM
To: [redacted] (OGC) (FBI)
Subject: CIPAV court orders

b6
b7C
b2
b7E
b1

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

(S) [redacted] asked me to send these to you for your review (he does not have access to FBINET). These concern [redacted] you probably already have his number, but if not, you can reach him at [redacted] or can reach me at [redacted] Thanks.

(S) [redacted]

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

DATE: 10-15-2008
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 10-15-2033

~~SECRET~~

~~SECRET~~

From: [redacted] (SL)(FBI)
Sent: Tuesday, October 03, 2006 4:29 PM
To: [redacted] (OTD) (FBI)
Cc: [redacted] (SL) (FBI); [redacted] (SL) (FBI)
Subject: FW: St Louis CIPAV issue - with attachments

b6
b7C

Follow Up Flag: Follow up
Due By: Wednesday, October 04, 2006 9:00 AM
Flag Status: Flagged

SECRET
RECORD 315q-sl-191661

[redacted] asked me to get in touch with you on the CIPAVs we are wanting to deploy. Just in case you don't have them, here is the affidavit and the search warrant language we were planning to use for our CIPAVS. I see you already have my explanation of the case (in the email string below). Our AUSA has looked at the affidavit warrant language and is ready to go on our end to get the search warrant and PR/TT orders. I know [redacted] and [redacted] discussed the classification issue on the devices, and that seems to be the only outstanding hurdle to getting this done. The summary of the case outlined in the email string below should help you evaluate the case with respect to that restriction. Can you take a look at that summary and let us know what you think about whether this restriction applies?

[Large redacted block]

b2
b7E
b6
b7E
b5

[redacted] Anyway, please let me know if there are any other items you need/things you need us to do/changes you need us to make to either 1) get this process started, or 2) reach the conclusion that we are wasting our time and this technique is not going to be possible on our case. Thanks in advance for your help.

[redacted]
SL JTTF

[redacted] (cell)

[redacted]

(S)

b1

-----Original Message----- (

lang ue [redacted] (SL) (FBI)
owr ue Wednesday, September 27, 2006 11:26 AM
tn ue [redacted] (SL)(FBI)
.pdo(r ue FW: St Louis CIPAV issue - with attachments

b6
b7C

~~SECRET~~

~~SECRET~~

~~SECRET~~

RECORD 315q-sl-191661

-----Original Message-----

lang ue [redacted] (OTD) (FBI)
owr le Tuesday, September 26, 2006 11:22 AM
tn le [redacted] (SL) (FBI)
5(le [redacted] (OTD) (FBI); [redacted] (OTD) (FBI)
.pdo(r le RE: St Louis CIPAV issue - with attachments

SECRET
RECORD 315q-sl-191661

[redacted]

Let me take a minute to introduce myself. I am [redacted] the new program manager for the Software Development Group (SDG). SDG handles all software deployments in CT, CI, and Criminal investigations for CEAU. Please contact me for all future inquiries regarding your case. My contact info is as follows:

b6
b7C
b2

SSA [redacted]
Supervisory Special Agent
Operational Technology Division
Digital Evidence Section
Cryptologic Electronic Analysis Unit
[redacted] (office)
[redacted] (cellular)

-----Original Message-----

lang ue [redacted] (SL) (FBI)
owr le Tuesday, September 26, 2006 9:27 AM
tn le [redacted] (OTD) (FBI); [redacted] (SL)(FBI)
5(le [redacted] (OTD) (FBI); [redacted] (OTD) (FBI)
.pdo(r le RE: St Louis CIPAV issue - with attachments

b6
b7C

SECRET
RECORD 315q-sl-191661

[redacted] thanks yet again for the good insight and info. I'm not sure point 2 is a show stopper: you're right - this case was originally pretty much straight criminal. [redacted]

[redacted]

We'll get to work on this end and keep you guys in the loop as we go. Would you prefer we deal with someone else in your unit for the day-to-day aspect of this case?

b2
b7E
b6
b7C

Talk to you soon

[redacted]

[redacted]

St Louis

[redacted] desk
[redacted] cell

-----Original Message-----

lang ue [redacted] (OTD) (FBI)

~~SECRET~~

~~SECRET~~

owr le Monday, September 25, 2006 4:44 PM
tn le [redacted] (SL) (FBI); [redacted] (SL) (FBI)
5(le [redacted] (OTD) (FBI); [redacted] (OTD) (FBI)
.pdofr uRE: St Louis CIPAV issue - with attachments

b6
b7C

SECRET
RECORD 315q-sl-191661

Thanks for reminding me. With several cases from the same FO, it is difficult to keep them straight.

There were several issues with this particular case, some easily overcome, and one that may be a show stopper. They are as follows:

1. Legal Process. We discussed this at length because the nature of the investigation is without precedent.

[redacted]

b2
b7E
b5

[redacted]

2. Case Classification.

[redacted]

b2
b7E
b5

Those are the issues thus far. I have included the Unit Chief and the Program Manager for these ops on this message as well.

[redacted]

-----Original Message-----
lang ue [redacted] (SL) (FBI)
owr le Friday, September 22, 2006 10:14 AM
tn le [redacted] (OTD) (FBI)
.pdofr le St Louis CIPAV issue - with attachments

b6
b7C
b2
b7E

SECRET
RECORD 315q-sl-191661

[redacted]

I resent you the email [redacted] wrote on the deal - you have to forgive him, we're still trying to teach him the beauty of brevity.

[redacted]

~~SECRET~~

~~SECRET~~

[Redacted]

St Louis

[Redacted] desk
[Redacted] cell

-----Original Message-----

lang ue [Redacted] (SL)(FBI)
owr ue Friday, September 22, 2006 9:12 AM
tn ue [Redacted] (SL) (FBI)
.pdo(r ue FW: St Louis CIPAV issue - with attachments

b6
b7C
b2

SECRET
RECORD 315q-si-191661

-----Original Message-----

lang ue [Redacted] (SL)(FBI)
owr ue Thursday, September 14, 2006 10:21 AM
tn ue [Redacted] (SL)(FBI); [Redacted] (OTD) (FBI)
S(ue [Redacted] (OTD) (FBI); [Redacted] (SL) (FBI); [Redacted] (SL) (FBI) [Redacted]
A. (SL) (FBI)
.pdo(r ue RE: St Louis CIPAV issue - with attachments

SECRET
RECORD 315q-si-191661

[Redacted]

b1

(S)

SECRET
RECORD 315q-si-191661

[Redacted]

(U) Ref our telcall on Tuesday, as you requested, I have attached the draft affidavit/warrant language we are planning to use (if we can clear all the hurdles) for installation of the CIPAVs here in St Louis. If we get the green light on this first effort, we will likely also be doing another affidavit

[Redacted]

[Redacted]

b2
b7E
b6
b7C
b1

(S)

(U/FOUO) [Redacted]

[Redacted]

~~SECRET~~

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (OGC) (FBI) b6
Sent: Monday, November 20, 2006 6:21 PM b7C
To: [redacted] (SL)(FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OTD) (FBI); [redacted] (OTD) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)

Subject: RE: [redacted] b1
(S)

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

[redacted]
A few points. The order for [redacted] is for a 30 day period while the PRT&T is for 60 days. The language of the order [redacted] in my opinion over-rides the language, in this case of the PenTrap. So, you have limited your collection to 30 days. I suggest that you ask AUSA [redacted] to amend the [redacted] order to extend it to 60 days (sec. 3117 doesn't provide time limits), absent some reason that I'm not aware of. Seems inconsistent to ask for 30 days [redacted] but then ask for 60 days to capture PenTrap information - the [redacted] b6
b7C
b2
b7E

Another point is that the [redacted] order provides for [redacted] the CEAU software) for 30 days [redacted] It does not make clear when the exploit must be removed consistent with the order, that is, within the 30 days or after the 30th day of collection of data. I see this as a source of trouble should the court sign this order. [redacted] If this is your intent then I have no problems with the wording of the order on this point but clarification would be helpful.

While I see AUSA [redacted] point that [redacted] as defined by the statute, as a matter of practice I haven't seen this before. I want to run it by my Unit Chief and see if he has any comments to add. All that said, CEAU hasn't used their tools in this manner before so we are setting a new course.

[redacted]
Assistant General Counsel
Science and Technology Law Unit
Office of the General Counsel
Federal Bureau of Investigation
Ph - [redacted]
Cell [redacted]
Ph (Secure) - [redacted]
Fax - [redacted]

b6
b7C
b2
b7E

-----Original Message-----

From: [redacted] (SL)(FBI)
Sent: Friday, November 17, 2006 6:54 PM
To: [redacted] (OGC) (FBI)
Subject: CIPAV court orders

DATE: 02-10-2009
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 02-10-2034

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

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S) [redacted] asked me to send these to you for your review (he does not have access to FBINET). These concern [redacted] You probably already have his number, but if not, you can reach him at [redacted] or can reach me at [redacted] Thanks.

~~SECRET~~

~~SECRET~~

(S)

b1

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SECRET~~

From: [redacted] (OTD) (FBI)
Sent: Thursday, September 14, 2006 3:13 PM
To: [redacted] (OGC) (FBI)
Cc: [redacted] (OTD) (FBI); [redacted] (OTD) (FBI)
Subject: RE: CIPAV boiler plate/FISA boiler plate
SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
b7C

[redacted]

[redacted]

[redacted]

b2
b7E
b6
b7C

Finally, keep in mind, if I'm not mistaken, that these are two different cases. The one that shows on the original message in this chain is a likely FISA (IT) matter, while the one that I was asking about with the stolen laptops is a separate case.

[redacted]

-----Original Message-----
Origin: [redacted] (OGC) (FBI)
Date: Thursday, September 14, 2006 1:43 PM
From: [redacted] (OTD) (FBI)
Subject: FW: CIPAV boiler plate/FISA boiler plate

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

[redacted]

b2
b7E
b5

You'll have to decide this.

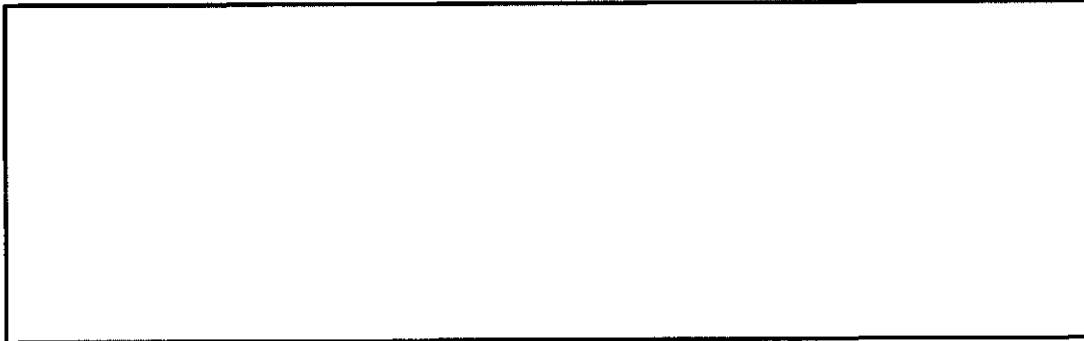
NSLB should be involved early on to resolve concerns about whether this is properly being worked as a FISA matter.

[redacted]
Assistant General Counsel
Science and Technology Law Unit
Office of the General Counsel
Federal Bureau of Investigation
Ph - [redacted]
Cell - [redacted]
Ph (Secure) - [redacted]
Fax - [redacted]

b6
b7C
b2

-----Original Message-----
-Originator [redacted] (OGC) (FBI)
Date and Time Sent Tuesday, September 05, 2006 1:01 PM
Sender [redacted] (CyD) (FBI)
Recipient(s) askIINM gn RE: CIPAV boiler plate/FISA boiler plate

SENSITIVE BUT UNCLASSIFIED
NON-RECORD



b2
b7E

Finally, tell SL they must work with the substantive desk at FBIHQ and they must work with NSLB when drafting the order. NSLB actually drafts the order.

b6
b7C
b2

[redacted]
Assistant General Counsel
Science and Technology Law Unit
Office of the General Counsel
Federal Bureau of Investigation
Ph - [redacted]
Cell - [redacted]
Ph (Secure) - [redacted]
Fax [redacted]

-----Original Message-----
-Originator [redacted] (CyD) (FBI)
Date and Time Sent Tuesday, September 05, 2006 11:35 AM
Sender [redacted] (OGC) (FBI)
Recipient(s) askIINM gFW: CIPAV boiler plate/FISA boiler plate

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

As we discussed.

b6
b7C

-----Original Message-----
-Ori gn [redacted] (OTD) (FBI)
al M gn Wednesday, August 30, 2006 2:36 PM
er gn [redacted] (OTD) (FBI); [redacted] (CyD) (FBI)
askIINM gFW: CIPAV boiler plate/FISA boiler plate

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Please provide [redacted] with the help he requests.

[redacted]

b6
b7C

-----Original Message-----
-Ori gn [redacted] (SL) (FBI)
al M gn Wednesday, August 30, 2006 10:35 AM
er gn [redacted] (OTD) (FBI)
GN gn [redacted] (SL)(FBI)
askIINM gCIPAV boiler plate/FISA boiler plate

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] I hate to admit this to you, but your presentation was very helpful last week. We talked about the CIPAV affidavit language your group has - I'd like to get some of that.

[redacted]

[redacted]

b2
b7E

Any help is good help.

Thanks again

[redacted]

[redacted]

St. Louis

[redacted] desk
[redacted] cell

b6
b7C
b2

SENSITIVE BUT UNCLASSIFIED

[redacted] (OTD) (FBI)

b6
b7C

From: [redacted] (OTD) (FBI)
Sent: Monday, November 20, 2006 5:24 PM
To: [redacted] (HO) (OGA)
Subject: FW: CIPAV for [redacted]

b2

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

I forgot to mention in my previous email to you that your order does not contain the language required for OTD's technology. Your order must authorize "remote access search and surveillance (RASS)" prior to us deploying our technology. If you desire the use of our techniques, you will have to have your order amended. Please contact the below listed person so that he can provide you with the necessary language.

b6
b7C

[redacted]
[redacted]

Thanks,
Kd

-----Original Message-----

From: [redacted] (OTD) (FBI)
Sent: Monday, November 20, 2006 4:25 PM
To: [redacted] (HO) (OGA)
Subject: CIPAV for [redacted]

b2
b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

[redacted] forwarded me your email regarding your case and your request for OTD's CIPAV technology. This is the first I am hearing of your case. Could you please provide me with a synopsis of your case and what your objectives are. Please provide the aforementioned information via a lead EC. The requested information will allow me to determine what technology is best suited for your case and whether we can assist with this matter.

If you have any questions regarding this request, feel free to contact me at the below listed telephone number(s).

Thanks,

SSA [redacted]
Software Development Group (SDG)
Cryptologic Electronic Analysis Unit (CEAU)
Digital Evidence Section (DES)
Operational Technology Division (OTD)

b6
b7C
b2

[redacted] (desk)
[redacted] (cell)

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

~~SECRET~~

From: [redacted] (OTD)(FBI)
Sent: Tuesday, November 07, 2006 8:17 AM
To: [redacted] (OTD) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] (ITD) (FBI)
Subject: RE: St Louis CIPAV
~~SENSITIVE BUT UNCLASSIFIED~~
~~RECORD~~ [redacted]

b6
b7C

b1
b7A
b2

(S)

(S) One other concern is that the Affidavit calls out specifically that we will use CIPAV. I believe the best tool for this is a [redacted] is that an issue?

b1
b2

Personally I don't like using our tool names in the affidavit.

J...

[redacted]
Information Technology Specialist
Operational Technology Division
Office - [redacted]
Mobile - [redacted]
Pager - [redacted]

b6
b7C
b2

-----Original Message-----

From: [redacted] (OTD)(FBI)
Sent: Tuesday, November 07, 2006 7:57 AM
To: [redacted] (OTD) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] (OTD) (FBI)
Subject: RE: St Louis CIPAV

~~SENSITIVE BUT UNCLASSIFIED~~
~~RECORD~~ [redacted]

(S)

We have received the computers here at OTD.

Are we cleared to have [redacted] people open the boxes and for us to do the install?

I do not know the status of the warrant.

J...

b6
b7C
b2

[redacted]
Information Technology Specialist
Operational Technology Division
Office - [redacted]
Mobile - [redacted]
Pager - [redacted]

-----Original Message-----

From: [redacted] (OTD) (FBI)
Sent: Monday, November 06, 2006 6:29 PM DATE: 02-10-2009
To: [redacted] (OTD)(FBI) CLASSIFIED BY 60322UC/LP/STP/gjg
Cc: [redacted] (ITD) (FBI) REASON: 1.4 (C)
Subject: FW: St Louis CIPAV DECLASSIFY ON: 02-10-2034

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SENSITIVE BUT UNCLASSIFIED~~
~~RECORD~~ [redacted]

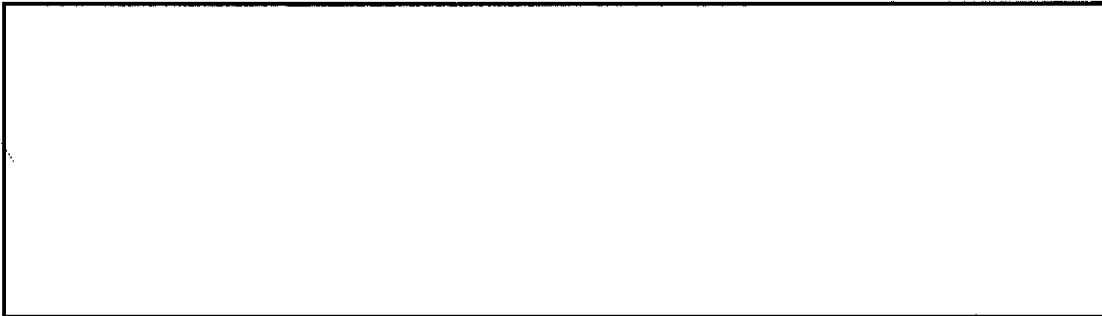
b2

-----Original Message-----
From: [redacted] (SL)(FBI)
Sent: Monday, October 30, 2006 5:30 PM
To: [redacted] (OTD) (FBI)
Subject: FW: St Louis CIPAV

b6
b7C

~~SENSITIVE BUT UNCLASSIFIED~~
~~RECORD~~ [redacted]

{S}



Also, based on [redacted] concurrence on the legal side, do you want us to go ahead and send the computers?

Thanks

[redacted]

b6
b7C

b1

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Monday, October 30, 2006 3:55 PM
To: [redacted] (SL)(FBI)
Cc: [redacted] (SL) (FBI); [redacted] (OTD) (FBI); [redacted] (OTD) (FBI); [redacted] E. (OGC) (FBI)
Subject: RE: St Louis CIPAV

b2

~~SENSITIVE BUT UNCLASSIFIED~~
~~RECORD~~ [redacted]

{S}



Absent the minor recommended additions in yellow in the above attachment, I concur with your drafts. Good job.

[redacted]

Assistant General Counsel
Science and Technology Law Unit
Office of the General Counsel
Federal Bureau of Investigation

Ph [redacted]
Cell [redacted]
Ph (Secure) - [redacted]
Fax [redacted]

b2
b6
b7C

-----Original Message-----
From: [redacted] (SL)(FBI)
Sent: Sunday, October 29, 2006 5:52 PM
To: [redacted] (OGC) (FBI)
Cc: [redacted] (SL) (FBI)
Subject: St Louis CIPAV

SENSITIVE BUT UNCLASSIFIED
RECORD [redacted]

[redacted]

As we discussed, here is a draft of the search warrant affidavit and warrant language for the use of the CIPAV. I have also included a draft of the language I am thinking to use of the PRT&T. Can you take a look and see what you think? Thanks again for all your help with this.

[redacted]

SL JTTF

(S) [redacted]

b1

~~**SENSITIVE BUT UNCLASSIFIED**~~
~~**SENSITIVE BUT UNCLASSIFIED**~~
~~**SENSITIVE BUT UNCLASSIFIED**~~
~~**SENSITIVE BUT UNCLASSIFIED**~~
~~**SENSITIVE BUT UNCLASSIFIED**~~
~~**SENSITIVE BUT UNCLASSIFIED**~~

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (OGC) (FBI)
 Sent: Tuesday, October 31, 2006 2:59 PM
 To: [redacted] (CyD) (FBI); [redacted] (OTD) (FBI); [redacted] (OTD) (FBI)
 Cc: [redacted] (CI) (FBI); [redacted] (CyD) (FBI); [redacted] (CyD) (FBI); [redacted] (CI) (FBI); [redacted] (NO) (FBI); [redacted] (AT) (FBI); [redacted] (CI) (FBI); [redacted] (CI) (FBI); [redacted] P (CyD) (FBI); [redacted] (PG) (FBI); [redacted] (CyD) (FBI); [redacted] (CI) (FBI); [redacted] (OGC) (FBI)
 Subject: RE: Web Bug for [redacted]

b6
b7C

b2

UNCLASSIFIED
NON-RECORD

[redacted]

b2
b7E
b7A
b6
b7C

I've reviewed the materials and EC that you provided. Depending on what you want the CIPAV to do for your investigation, [redacted] certainly at least a search warrant. We can discuss this when you and [redacted] agree on what capabilities you need from the CIPAV.

[redacted]

[redacted] If it is, then we will need to react and adjust your operations accordingly by getting required authorizations. [redacted] it is my opinion that at least a CIPAV set to provide Pen Register/Trap and Trace information (SW and PRT&T order) can be sought from your federal district court.

[redacted]

get involved. We can sort this out when you have better information.

Hope this helps,

[redacted]

Assistant General Counsel
 Science and Technology Law Unit
 Office of the General Counsel
 Federal Bureau of Investigation
 Ph - [redacted]
 Cell - [redacted]
 Ph (Secure) - [redacted]
 Fax - [redacted]

b6
b7C
b2

DATE: 02-10-2009
 CLASSIFIED BY 60322UC/LP/STP/gjg
 REASON: 1.4 (C)
 DECLASSIFY ON: 02-10-2034

b6
b7C

-----Original Message-----

From: [redacted] (CyD) (FBI)
 Sent: Tuesday, October 31, 2006 10:54 AM
 To: [redacted] (OGC) (FBI); [redacted] (OTD) (FBI)
 Cc: [redacted] (CI) (FBI); [redacted] (CyD) (FBI); [redacted] (CyD) (FBI); [redacted] (CI) (FBI); [redacted] (NO) (FBI); [redacted] (AT) (FBI); [redacted] (CI) (FBI); [redacted] (CI) (FBI); [redacted] (CyD) (FBI); [redacted] (PG) (FBI); [redacted] (CyD) (FBI); [redacted] (CI) (FBI)
 Subject: Web Bug for [redacted]

UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

[redacted] ~~SECRET~~

[Redacted]

b2
b7E
b7A
b6
b7C

Per our conversation [Redacted] the best background serial for the case is [Redacted]

We are considering utilizing a CIPAV/IPAV in conjunction with [Redacted] We are currently drafting an affidavit/application for the CIPAV/IPAV in order to employ the tool upon the approval for [Redacted]

(S) [Redacted]

b1
b2
b7A
b7E

(S) [Redacted]

We should get a draft application to you soon.

SSA [Redacted]
Cyber Action Team Unit
Computer Intrusion Section
Cyber Division
Room 5931
935 Pennsylvania Avenue
Washington, D.C. 20535

b6
b7C
b2

DESK- [Redacted]
FAX- [Redacted]
CELL- [Redacted]
PAGER [Redacted]
EMAIL- [Redacted]

The information transmitted is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination, or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact the sender and delete the material from any computer.

~~UNCLASSIFIED~~

~~UNCLASSIFIED~~

~~SECRET~~

[redacted] (OTD) (FBI)

b6
b7C

From: [redacted] (SL)(FBI)
Sent: Monday, October 30, 2006 6:30 PM
To: [redacted] (OTD) (FBI)
Subject: FW: St Louis CIPAV

b2

~~SENSITIVE BUT UNCLASSIFIED~~
~~RECORD~~ [redacted]

(S)

[Large redacted block]

b1

Any other configuration info that ya'll need?

Also, based on [redacted] concurrence on the legal side, do you want us to go ahead and send the computers?

Thanks

b6
b7C

[redacted]

-----Original Message-----

From: [redacted] (OGC) (FBI)
Sent: Monday, October 30, 2006 3:55 PM
To: [redacted] (SL)(FBI)
Cc: [redacted] (SL) (FBI); [redacted] (OTD) (FBI); [redacted] (OTD) (FBI); [redacted] (OGC) (FBI)
Subject: RE: St Louis CIPAV

b2

~~SENSITIVE BUT UNCLASSIFIED~~
~~RECORD~~ [redacted]

b1

[redacted]

(S)

[redacted]

Absent the minor recommended additions in yellow in the above attachment, I concur with your drafts. Good job.

[redacted]
Assistant General Counsel
Science and Technology Law Unit
Office of the General Counsel
Federal Bureau of Investigation
Ph - [redacted]
Cell - [redacted]
Ph (Secure) - [redacted]
Fax [redacted]

DATE: 10-15-2008
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 10-15-2033

b2
b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

-----Original Message-----

From: [redacted] (SL)(FBI)
Sent: Sunday, October 29, 2006 5:52 PM

~~SECRET~~

~~SECRET~~

To: [redacted] (OGC) (FBI)
Cc: [redacted] (SL) (FBI)
Subject: St Louis CIPAV

b6
b7C

b2

~~SENSITIVE BUT UNCLASSIFIED~~
~~RECORD~~ [redacted]

[redacted]

As we discussed, here is a draft of the search warrant affidavit and warrant language for the use of the CIPAV. I have also included a draft of the language I am thinking to use of the PRT&T. Can you take a look and see what you think? Thanks again for all your help with this.

b6
b7C

[redacted]

SL JTTF

(S)

[redacted]

b1

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SECRET~~

~~SECRET~~

[redacted] (OTD) (FBI)

From: [redacted] (OGC) (FBI)
Sent: Tuesday, October 10, 2006 1:40 PM
To: [redacted] (OTD) (FBI)
Subject: FW: St Louis CIPAV issue - with attachments

b6
b7C

SECRET
RECORD 315q-sl-191661

If you can attend, it might save you some time in the long run.

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

b2
b6
b7C

!!!!*#\$%\$&'()*+.,%+!!!!

From: o o
Sent: e to mtF t tF t
To: t t to t
Subject: t t :bt c t:bb utrt: te e uSb

SECRET
RECORD 315q-sl-191661

[redacted]
I'm doing a teleconference with [redacted] at 2:30 today. FYI.

b2
b6
b7C

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

DATE: 02-12-2009
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 02-12-2034

!!!!*#\$%\$&'()*+.,%+!!!!

From: c t j t to t c t t
Sent: u Sub e to umt t t t T
To: j c to t to t c
Subject: t t :bt c t:bb utrt: te e uSb

SECRET
RECORD 315q-sl-191661

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

They would like this to fire for the duration of [redacted] warrant authorization.

b2
b7E

~~SECRET~~

~~SECRET~~

!!!!#\$%\$&'()*+.,%+!!!!

From: jc totto t ctt
Sent: uSube to umt t t tT
To: ctj tto t c
Subject: t t :btc t:bb utrt: te e uS b

SECRET
RECORD 315g-si-191661

[Redacted]

No need for a PRT&T is you are only using [Redacted]

[Redacted]

Assistant General Counsel
Science and Technology Law Unit
Office of the General Counsel
Federal Bureau of Investigation

b2
b6
b7C

Ph [Redacted]
Cel [Redacted]
Ph (Secure) [Redacted]
Fax [Redacted]

!!!!#\$%\$&'()*+.,%+!!!!

From: ctj tto t ctt
Sent: uSube to umt t t tT
To: tc cTto t c
Cc: jcC toCt to t ct oCtoCt to ct t tjtto t c
Subject: t t :btc t:bb utrt: te e uS b

SECRET
RECORD 315g-si-191661

[Redacted]

I just spoke with SL regarding this matter and they are elated that we have decided to support the case. They are really in the market for a tool that would provide them with PT&T functionality. I explained to them that [Redacted] [Redacted]. However, following the conversation with SL, I thought to myself that [Redacted] would better serve the case. It would provide the functionality of the CIPAV [Redacted] [Redacted] as well as provide other useful info that could help further the case. Of course, the latter would depend on SL getting the proper authorization. Your thoughts?

b2
b7E
b6
b7C

[Redacted]

I told SL to contact you for your assistance in drafting the language for the hybrid SW/PT&T order. I [Redacted] is amenable to deploying [Redacted] would you make sure that the proper language is conveyed to SL to support the deployment.

They are planning on forwarding the boxes to us for the install. We will coordinate with Flaps & Seals to assist with this matter.

Thanks,
Kd

!!!!#\$%\$&'()*+.,%+!!!!

From: tc cTto t ctt
Sent: uSube to umt t tF FtT
To: ctj tto t c
Cc: c TC tC oCt to t c
Subject: t t :btc t:bb utrt: te e uS b

~~SECRET~~

~~SECRET~~

SECRET
RECORD 315q-sl-191661

Opinion from [redacted] As long as we are using only a CIPAV, I am willing to say this is strictly unclass. b6
Should the need arise for additional tools, we will certainly enter the classified realm. Please pass this to SL b7C

[redacted]

!!!!*#%\$&'()*+,,%+!!!!
From: jcC to Ct to t ctt
Sent: uSub e to umt t tF tT
To: tc cTto t c
Cc: c TC tC oCt to t c
Subject: t t :bt c t:bb utrt: te e uS b

SECRET
RECORD 315q-sl-191661

[redacted]

(S)

b1

What the case agent and AUSA have put together is a search warrant that allows loading the computers with the exploit and subsequent seizure of this same PPT&T data [redacted] with a caveat that they will return to the court with another application if this collection operation is to extend [redacted] All of this is based upon probable cause.

b2
b7E

I think it is awkward and will require more work for the CA and AUSA but it may work IF the court sees it for what it really is. As a continuing search, it may fail, but as a search and subsequent PRT&T, it will work. I recommend specifically notifying the court in the warrant and affidavit that this is a two step request, a search (to get into the computer even though at the time it is FBI property) and subsequent PRT&T. The search is good for [redacted] and the PRT&T can be good for up to [redacted].

Ultimately, if the court signs the order, I think it is sufficient but issues are being generated unnecessarily. This doesn't address the security classification issues raised below.

[redacted]
Assistant General Counsel
Science and Technology Law Unit
Office of the General Counsel
Federal Bureau of Investigation
Ph - [redacted]
Cell [redacted]
Ph (Secure) - [redacted]
Fax [redacted]

b2
b6
b7C

!!!!*#%\$&'()*+,,%+!!!!
From: tc cTto t ctt
Sent: uSub e to umt t tFF tT
To: jcC to Ct to t c
Cc: c TC tC oCt to t c
Subject: t t :bt c t:bb utrt: te e uS b

SECRET
RECORD 315q-sl-191661

[redacted] ~~SECRET~~

~~SECRET~~

[redacted] (OTD) (FBI)

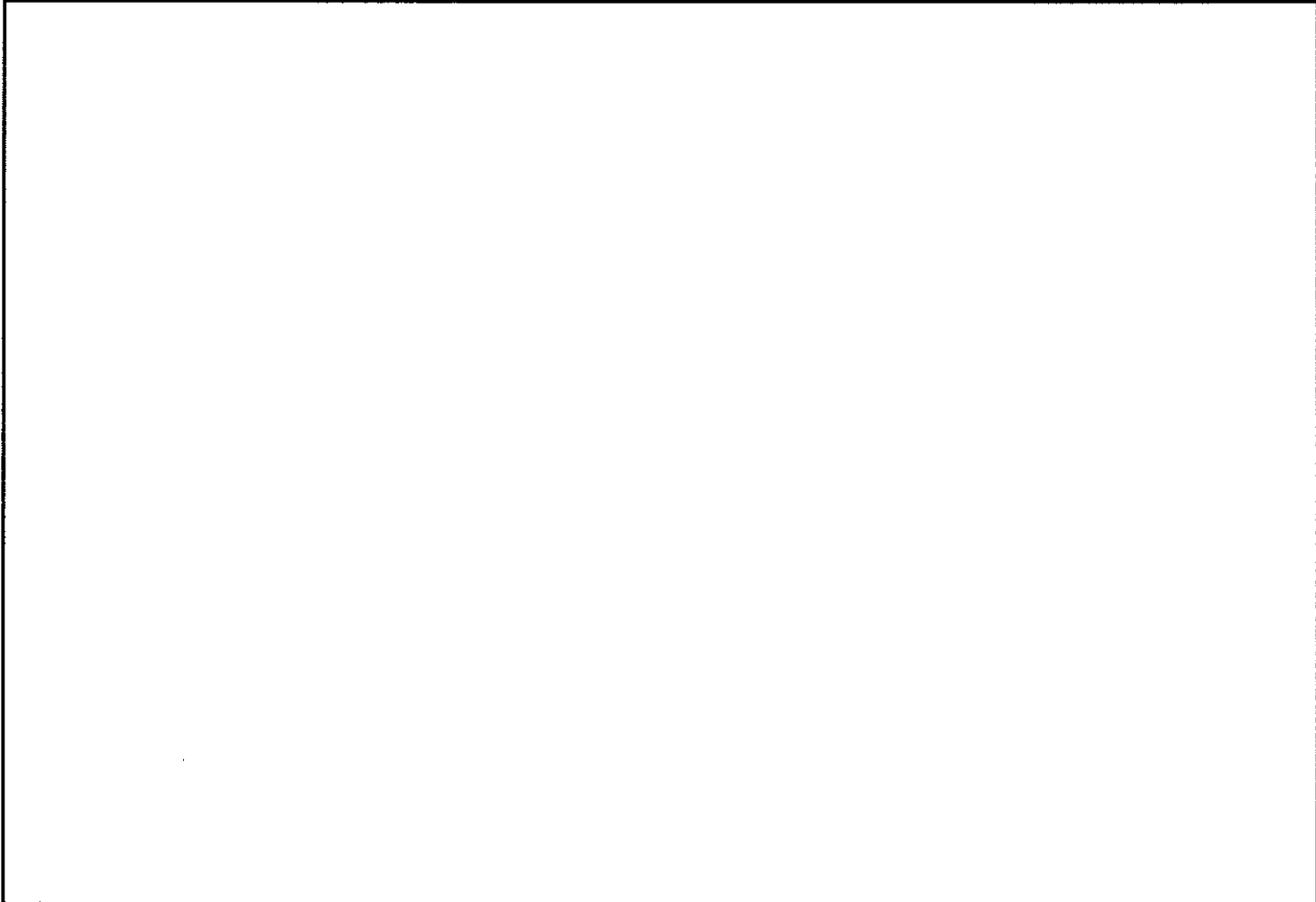
b6
b7C

To: [redacted] (OTD) (FBI)
Cc: [redacted] (OTD) (FBI)
Subject: [redacted]

b2

(S)

[redacted]



b1

SSA [redacted]
Software Development Group (SDG)
Cryptologic Electronic Analysis Unit (CEAU)
Digital Evidence Section (DES)
Operational Technology Division (OTD)

b2
b6
b7C

[redacted] (desk)
[redacted] (cell)

DATE: 09-25-2008
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 09-25-2033

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

~~SECRET~~

United States District Court

Southern DISTRICT OF Florida

In the Matter of the Search of

[Redacted]

(S)

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

b1

CASE NUMBER:

I, Herbert E. Hogberg III being duly sworn depose and say:

I am a Special Agent and have reason to believe
Official Title

that I on the person of or I on the property or premises known as

b1

[Redacted]

(S)

in the Southern District of Florida

[Redacted]

b1

(S)

concerning a violation of Title 18 United States code, Section(s) 2332a

The facts to support a finding of Probable Cause are as follows:

see attached affidavit

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-24-2009 BY 60322UC/LP/STP/gjg

Continued on the attached sheet and made a part hereof: Yes No

Sworn to before me and subscribed in my presence,

Signature of Affiant

Date

at _____
City and State

Name & Title of Judicial Officer

~~SECRET~~

Signature of Judicial Officer

United States District Court

Southern DISTRICT OF Florida

In the Matter of the Search of

[Redacted]

(S)

SEARCH WARRANT

b1

CASE NUMBER:

TO: _____ and any Authorized Officer of the United States
Affidavit(s) having been made before me by Herbert E. Hogberg III who has reason to
Affiant

b1

believe that _____ on the person of or ! _____ on the premises known as

(S)

[Redacted]

b1

in the _____ Southern _____ District of _____ Florida _____ there is now
concealed a certain property, namely

[Redacted]

(S)

I am satisfied that the affidavit(s) and any recorded testimony establish probable cause to believe that the person or property so described is now concealed on the person or premises above-described and establish grounds for the issuance of this warrant.

YOU ARE HEREBY COMMANDED to search on or before _____
Date

(not to exceed 10 days) the person or place named above for the person or property specified, serving this warrant and making the search (in the daytime - 6:00 A.M. to 10:00 P.M.) (at any time in the day or night as I find reasonable cause has been established) and if the person or property be found there to seize same, leaving a copy of this warrant and receipt for the person or property taken, and prepare a written inventory of the person or property

seized and promptly return this warrant to _____

as required by law. ALL FBI INFORMATION CONTAINED

U.S. Magistrate Judge

HEREIN IS UNCLASSIFIED

DATE 02-24-2009 BY 60322UC/LP/STP/gjg

Date and Time Issued _____

at

City and State _____

Name and Title of Judicial Officer _____

Signature of Judicial Officer _____