

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-18-2008 BY 60322UC/LP/STP/gjg

b6
b7C

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

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Good Afternoon,

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

b6
b7C

Thanks,

[redacted]

[redacted]

Management Assistant
Operational Technology Division (OTD)
Cryptologic and Electronic Analysis Unit (CEAU)

b2
b6
b7C

[redacted] (Chantilly)
[redacted] (Quantico)
[redacted] (Cell)

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

Importance: High

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Good Afternoon,

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

Thanks,

b2
b6
b7c

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

[redacted] (Chantilly)
[redacted] (Quantico)
[redacted] (Cell)

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

[Redacted] (OTD) (CON)

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

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Good Afternoon,

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

v/r
[Redacted]

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

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

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Good Afternoon,

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

Thanks,

[Redacted]

[Redacted]
Management Assistant
Operational Technology Division (OTD)
Cryptologic and Electronic Analysis Unit (CEAU)

[Redacted] (Chantilly)
[Redacted] (Quantico)
[Redacted] (Cell)



b6
b7C

[Redacted] (OTD) (CON)

From: [Redacted] (OGC) (FBI)
Sent: Monday, July 23, 2007 12:22 PM
To: [Redacted] (OGC) (FBI)
Subject: RE: CIPAV/Magic Lantern news blurb - FYI

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Just law enforcement sensitive.

[Redacted]

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

b2
b6
b7C

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

From: [Redacted] (OGC) (FBI)
Sent: Monday, July 23, 2007 12:22 PM
To: [Redacted] (OGC) (FBI)
Subject: RE: CIPAV/Magic Lantern news blurb - FYI

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-22-2010 BY 67203 UCLP/STP

b6
b7C

I'm assuming it was not a classified technique?

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

From: [Redacted] (OGC) (FBI)
Sent: Monday, July 23, 2007 12:13 PM
To: [Redacted] (OGC) (FBI)
Subject: RE: CIPAV/Magic Lantern news blurb - FYI

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Saw it. Thanks. People are not happy around here about it. I haven't been able to learn if the agent made the mistake of not filing under seal or whether the court removed the seal after the kid plead guilty and was sentenced.

[Redacted]

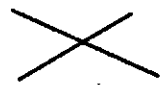
Assistant General Counsel
Science and Technology Law Unit
Phone: [Redacted]
Cell phone [Redacted]
Secure phone [Redacted]
Fax [Redacted]

b2
b6
b7C

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

From: [Redacted] (OGC) (FBI)
Sent: Monday, July 23, 2007 12:11 PM
To: [Redacted] (OGC) (FBI)
Cc: [Redacted] (OGC) (FBI); [Redacted] (OGC) (FBI)
Subject: FW: CIPAV/Magic Lantern news blurb - FYI

SENSITIVE BUT UNCLASSIFIED



~~NON-RECORD~~

[redacted]
JUST FYI.

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Monday, July 23, 2007 11:38 AM
To: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI)
Subject: FW: CIPAV/Magic Lantern news blurb - FYI

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

b6
b7C

I assume you folks know of this—but just in case.

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Wednesday, July 18, 2007 12:18 PM
To: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: CIPAV/Magic Lantern news blurb - FYI

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

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

Wired.com

2:00 AM

By Kevin Poulsen

July 18, 2007

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

The court filing offers the first public glimpse into the bureau's long-suspected spyware capability, in which the FBI adopts techniques more common to online criminals. The software was sent to the owner of an anonymous MySpace profile linked to bomb threats against Timberline High School near Seattle. The code led the FBI to 15-year-old Josh Glazebrook, a student at the school, who on

~~NON-RECORD~~

Monday pleaded guilty to making bomb threats, identity theft and felony harassment. In an affidavit seeking a search warrant to use the software, filed last month in U.S. District Court in the Western District of Washington, FBI agent Norman Sanders describes the software as a "computer and internet protocol address verifier," or CIPAV.

FBI Spyware In A Nutshell

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

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

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

Under a ruling this month by the 9th U.S. Circuit Court of Appeals, such surveillance -- which does not capture the content of the communications -- can be conducted without a wiretap warrant, because internet users have no "reasonable expectation of privacy" in the data when using the internet.

According to the affidavit, the CIPAV sends all the data it collects to a central FBI server located somewhere in eastern Virginia. The server's precise location wasn't specified, but previous FBI internet surveillance technology -- notably its Carnivore packet-sniffing hardware -- was developed and run out of the bureau's technology laboratory at the FBI Academy in Quantico, Virginia.

The FBI's national office referred an inquiry about the CIPAV to a spokeswoman for the FBI Laboratory in Quantico, who declined to comment on the technology. The FBI has been known to use PC-spying technology since at least 1999, when a court ruled the bureau could break into reputed mobster Nicodemo Scarfo's office to plant a covert keystroke logger on his computer. But it wasn't until 2001 that the FBI's plans to use hacker-style computer-intrusion techniques emerged in a report by MSNBC.com. The report described an FBI program called "Magic Lantern" that uses deceptive e-mail attachments and operating-system vulnerabilities to infiltrate a target system. The FBI later confirmed the program, and called it a "workbench project" that had not been deployed.

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

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

The FBI's 2008 budget request hints at the bureau's efforts in the hacking arena,

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

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

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

On June 7, the hoaxer started issuing threats through other online mediums. In his most brazen move, he set up a MySpace profile called Timberlinebombinfo and sent friend requests to 33 classmates. The whole time he was daring law enforcement officials to trace him. "The e-mail was sent over a newly made Gmail account, from overseas in a foreign country," he wrote in one message. "Seeing as you're too stupid to trace the e-mail back lets (sic) get serious," he taunted in another. "Maybe you should hire Bill Gates to tell you that it is coming from Italy. HAHAHA. Oh wait. I already told you that it's coming from Italy." As promised, attempts to trace the hoaxer dead-ended at a hacked server in Grumello del Monte, Italy.

The FBI's Seattle Division contacted the FBI legal attaché in Rome, who provided an official request to the Italian national police for assistance. But on June 12, perhaps fed up with the mocking, the FBI applied for and obtained a

~~XXXXXXXXXX~~
search warrant authorizing the bureau to send the CIPAV to the Timberlinebombinfo MySpace profile. Court documents reveal the search warrant was "executed" June 13 at 5:49 p.m. Though the CIPAV provided a wealth of information, Glazebrook's IP address would have been enough to guide the FBI to the teen's front door. John Sinclair, Glazebrook's attorney, says his client never intended to blow anything up -- "it was a prank from the get-go" -- but admits he hacked into computers in Italy to launder his activities, and that he launched the denial-of-service attack against the school district's network.

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

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

[Redacted]
Assistant General Counsel
OGC, Privacy & Civil Liberties Unit
Phone [Redacted]
Fax: [Redacted]

b2
b6
b7c

**THE FOREGOING MAY BE A PRIVILEGED
FBI OGC COMMUNICATION AND SHOULD NOT BE DISSEMINATED WITHOUT
OGC APPROVAL**

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~
~~XXXXXXXXXX~~

~~SECRET~~

[Redacted]

(OTD) (CON)

b6
b7C

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

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

b6
b7C

(S) [Redacted] the pony we sent stated

[Redacted]

b1
b2
b7E

I am concerned that the the current wording greatly constrains what we can deliver.

[Redacted]

b2
b7E

[Redacted]

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

b2
b6
b7C

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

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: Re: [Redacted]

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

(S) [Redacted]

b1
b2
b7E
b6
b7C

Assistant General Counsel
Science and Technology Law Unit

DATE: 10-20-2008
CLASSIFIED BY 60322UC/LP/STP/gjg
REASON: 1.4 (C)
DECLASSIFY ON: 10-20-2033

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

~~SECRET~~

Office of the General Counsel
Federal Bureau of Investigation

Ph - [REDACTED]

Cell

Ph (Secure) [REDACTED]

Fax [REDACTED]

b2

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SECRET~~

[Redacted] (OTD) (CON)

From: [Redacted]
Sent: Monday, July 02, 2007 10:52 AM
To: [Redacted] (SE) (FBI)
Cc: [Redacted] (SE) (FBI); [Redacted] (SE) (FBI); [Redacted] (CG) (FBI); [Redacted] (OTD) (FBI)
Subject: RE: [Redacted] Question

b2
b6
b7C
b7E

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[Redacted]

[Redacted]

b5

[Redacted]

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

b2
b6
b7C

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

From: [Redacted]
Sent: [Redacted]
To: [Redacted]
Cc: [Redacted]
Subject: [Redacted]

b2
b6
b7C
b7E

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Thanks [Redacted] Hoping to hear a decision soon. The [Redacted] and we think this would be a great strategy in identifying the [Redacted] Thanks for all your help. [Redacted]

SA [Redacted]
FBI Seattle

[Redacted] (Fax) [Redacted]
[Redacted] (Nextel) DC: [Redacted]
[Redacted]

b2
b6
b7C
b7E

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

From: [Redacted] (OGC) (FBI)
Sent: Monday, June 25, 2007 7:55 AM
To: [Redacted] (SE) (FBI)
Subject: [Redacted] Question

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[Redacted]

[Redacted]

[Redacted]

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

b2
b6
b7C
b7E

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

[Redacted] (OTD) (CON)

From: [Redacted] (SE) (FBI)
Sent: Monday, June 25, 2007 11:53 AM
To: [Redacted] (OGC) (FBI)
Cc: [Redacted] (SE) (FBI); [Redacted] (SE) (FBI); [Redacted] (CG) (FBI)
Subject: RE: [Redacted] Question

b2
b6
b7C
b7E

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Thanks [Redacted] Hoping to hear a decision soon. The [Redacted] and we think this would be a great strategy in identifying the [Redacted] Thanks for all your help. [Redacted]

SA [Redacted]
FBI Seattle

b2
b6
b7C
b7E

[Redacted] Fax) Nextel) DC: [Redacted]
[Redacted]

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

From: [Redacted] (OGC) (FBI)
Sent: Monday, June 25, 2007 7:55 AM
To: [Redacted] (SE) (FBI)
Subject: [Redacted] Question

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[Redacted]

[Large Redacted Block]

b2
b6
b7C
b7E

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

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

[Redacted] OTD) (CON)

From: [Redacted] (OGC) (FBI)
Sent: Monday, June 25, 2007 10:55 AM
To: [Redacted] (SE) (FBI)
Subject: [Redacted] Question

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b2
b6
b7C
b7E

[Redacted]

[Redacted]

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

SENSITIVE BUT UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-26-2008 BY 0322UC/LP/STP/gjg

[redacted] (OTD) (CON)

From: [redacted] (OGC) (FBI)
Sent: Wednesday, June 20, 2007 4:24 PM
To: [redacted] (OGC) (FBI)
Subject: Question

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

Since we won't overlap this week (I'm on leave on Friday), I wanted to get your thoughts on a question I received from SA [redacted] of Seattle. Here are the facts:

[redacted]

b2
b6
b7C
b7E

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

SENSITIVE BUT UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-26-2008 BY 0322UC/LP/STP/gjg

[REDACTED] (OTD) (CON)

b6
b7C

From: [REDACTED] (SE) (FBI)
Sent: Tuesday, June 12, 2007 8:20 PM
To: [REDACTED] (OGC) (FBI)
Subject: RE: CIPAV Affidavit - Seattle Division

UNCLASSIFIED
NON-RECORD

Thanks for your help.

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

From: [REDACTED] (OGC) (FBI)
Sent: Tuesday, June 12, 2007 8:06 AM
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

b6
b7C

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]

[REDACTED]

[REDACTED]

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

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

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

UNCLASSIFIED

NON-RECORD

[redacted] Attached is the revised affidavit. Copy was also sent to AUSA [redacted] to review [redacted]. I made the changes we discussed earlier. [redacted] described the intended deployment strategy, described the search warrant [redacted]. The formatting will be cleaned up by the AUSA's secretary. Hoping to sign and deploy on Tuesday. Thanks, [redacted]

<< File: Revised Affidavit for [redacted] >>

SA [redacted]
FBI Seama

[redacted]
(Fax) [redacted]
(Nextel) DC: [redacted]
[redacted]

b2
b7E
b6
b7C

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

[redacted] (OTD) (CON)

From: [redacted] (OGC) (FBI)
Sent: Tuesday, June 12, 2007 9:25 AM
To: [redacted] (OTD) (FBI)
Subject: FW: CIPAV Affidavit - Seattle Division

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted]

I need you to review for technical issues. I'm reviewing for the legal aspects.

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

b2
b6
b7C

b6
b7C

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

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

UNCLASSIFIED
NON-RECORD

[redacted] Attached is the revised affidavit. Copy was also sent to AUSA [redacted] to review [redacted] I made the changes we discussed earlier. [redacted] described the intended deployment strategy, decribed the search warrant and conversion to pen register. [redacted] The formatting will be cleaned up by the AUSA's secretary. Hoping to sign and deploy on Tuesday. Thanks, [redacted]

b2
b7E
b6
b7C



Revised Affidavit
for [redacted]

SA [redacted]
FBI Seattle

[redacted] (Fax)
[redacted] (Nextel) DC: [redacted]

UNCLASSIFIED

UNCLASSIFIED

~~SECRET~~

[redacted] (OTD) (CON)

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

b2
b6
b7C

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)

-----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

b1
b2
b7E
b6
b7C

UNCLASSIFIED
NON-RECORD

(S) [Large redacted area]

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

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

[Redacted]

(S)

b1

(S)

[Redacted]

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

b2
b6
b7C

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



[Redacted]

b2
b7E
b6
b7C

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

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

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

[Redacted]

b2
b7E
b6
b7C

SA [Redacted]
FBI Seattle

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

~~UNCLASSIFIED~~

~~UNCLASSIFIED~~

[Redacted]

(OTD) (CON)

From: MOTTA, THOMAS GREGORY (OTD) (FBI)
 Sent: Friday, June 08, 2007 9:17 AM
 To: [Redacted] (OGC) (FBI); [Redacted] (OGC) (FBI); [Redacted] (OGC) (FBI); [Redacted] (OGC) (FBI)
 Cc: (FBI) [Redacted] (OGC) (FBI); [Redacted] (OTD) (FBI); [Redacted] (OTD) (FBI); DICLEMENTE, ANTHONY P. (OTD) (FBI); [Redacted] (PG) (FBI); [Redacted] (CyD) (FBI); [Redacted] (OTD) (FBI); [Redacted] (OS) (FBI)
 Subject: FW: UR5214/SE/THREAT INVESTIGATION

b6
b7C

UNCLASSIFIED
NON-RECORD

I believe that CIPAVs are now deployed by DITU. I forward this to ensure that this is brought to their attention and the attention of the relevant elements of OGC who are now counsel to that unit.

Thos. Gregory Motta
Section Chief, Digital Evidence Section (DES)
Operational Technology Division (OTD)
Engineering Research Facility
Bldg 27958A, Room A-207
Quantico, VA 22135

Tel. [Redacted]
 Tel. [Redacted]
 Fax. [Redacted]

b2

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

From: [Redacted] (PG) (FBI)
 Sent: Friday, June 08, 2007 12:38 AM
 To: [Redacted] (CyD) (FBI); MOTTA, THOMAS GREGORY (OTD) (FBI)
 Subject: FW: UR5214/SE/THREAT INVESTIGATION

b6
b7C

UNCLASSIFIED
NON-RECORD

UNCLASSIFIED
NON-RECORD

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

SSA [Redacted]
 Watch Supervisor - SIOC
 [Redacted]

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

From: [Redacted] (SE) (FBI)
 Sent: Thursday, June 07, 2007 11:46 PM
 To: FBI_URGENT REPORTS
 Cc: SE All Supervisors

b6
b7C
b2

Subject: UNSUB TIMBERLINE HIGH SCHOOL - VICTIM, COMPUTER INTRUSION - THREAT; 288A-SE-93709

UNCLASSIFIED
NON-RECORD



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



158brf02.ec (11
KB)

b2
b6
b7c



A/ASAC Seattle Division
SSA - Squad 5
Gang/Criminal Enterprise Program;
Organized Crime Program;
Violent Crimes Program;
Desk: 
NEXTEL: 

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

FBI URGENT REPORT**Precedence:** IMMEDIATE**Date:** 06/07/2007

To: Director
 SIOC
 Cyber
 Operational Technology
 CIRG
 Rome

From: Seattle**Contact:** [REDACTED]**Approved By:** [REDACTED]

b2
 b6
 b7c

Drafted By: [REDACTED]

Subject/Title/Case ID #: UNSUB;
 TIMBERLINE HIGH SCHOOL - VICTIM,
 COMPUTER INTRUSION - THREAT;
 288A-SE-93709

Purpose/Synopsis: OTHER MATTER WARRANTING THE IMMEDIATE
 ATTENTION OF FBIHQ EXECUTIVES

INITIAL
URGENT REPORT

On 06/06/2007, the Seattle Field Office was contacted by the Lacey Police Department (LPD), Lacey, WA, regarding e-mail bomb threats and Distributed Denial of Service (DDOS) attacks received by Timberline High School, 6120 Mullen Road SE, Lacey, WA, 98503, in the North Thurston Public School District.

The e-mail threats commenced on 06/04/2007, and continue to the present. To date, there have been three e-mail threats that resulted in three separate deployments of K-9 Units from the Washington State Patrol and severe disruption in routine school operations. There has also been an increase in local media coverage of the incidents and growing parental concerns.

The e-mail content has repeatedly demeaned school faculty and teachers and taunts law enforcement. The UNSUB(S) also posted three of the e-mail threats in the "Comments" section of "The Olympian" news online website.

To: Director From: Seattle
Re: 06/07/2007, 288A-SE-93709

Investigation conducted by LPD identified three Internet Protocol (IP) addresses being utilized, [redacted], [redacted], which at this time are believed to be proxies. A request for assistance has been forwarded to the [redacted] by LEGAT Rome.

b7D
b2
b7E

LPD conducted several interviews on persons of interest, however, no subject have been identified. Logical investigative leads are being pursued.

FBI Seattle is developing a strategy to deploy a Computer and Internet Protocol Address Verifier (CIPAV) and drafting a search warrant affidavit. Seattle will also coordinate the investigation with LEGAT Rome and the Behavioral Analysis Unit.

FBI involvement in the investigation will not be revealed at this time to facilitate a scenario through which the CIPAV could be successfully deployed.

Graduation at Timberline High School is scheduled for 06/15/2007, and the last day of instruction is 06/21/2007.

◆◆C:\Documents and Settings\[redacted]\Local Settings\Temporary Internet Files\158brf02.ec

b6
b7C