

# CYBER DIVISION

FEDERAL BUREAU OF INVESTIGATION

## SITUATION ACTION BACKGROUND

TIMBERLINE SCHOOL DISTRICT; [REDACTED]

288A-SE-93709

29 October 2014

b6 -3  
b7C -3

(U//~~FOUO~~) SITUATION: On 28 October 2014 at 0810, SA [REDACTED] (Seattle Division) apprised the Operation Technology Division (OTD) and the Behavior Analysis Unit (BAU) of the recent events and news articles for operational awareness. [REDACTED]

b6 -1  
b7C -1  
b7E -5

(U//~~FOUO~~) During the course of SA [REDACTED] investigation and subsequent prosecution, [REDACTED] OGC handled the FOIA appropriately. [REDACTED] Undercover approval was authorized by the AUSA.

b6 -1  
b7C -1  
b7E -2

(U//~~FOUO~~) SA [REDACTED] reviewed the undercover chat logs. He verified that the undercover operation was in no way connected to anything associated with The Seattle Times, nor was a website of The Seattle Times spoofed. However, the undercover news article containing the CIPAV used the name of the Associated Press and was transmitted to the subject of the investigation.

b6 -1  
b7C -1

(U//~~FOUO~~) BACKGROUND: On 6 June 2007, the Seattle Division was contacted by the Lacey Police Department (LPD), Lacey, WA, and the Washington State Patrol (WSP) regarding numerous bomb threats and Distributed Denial of Service (DDOS) attacks received at the Timberline School District, Lacey, WA.

(U//~~FOUO~~) The threats began on 30 May 2007 and persisted through 4 June 2007. The threats necessitated the daily evacuation of Timberline High School. The LPD and the 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 6 June 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 OTD/CEAU with locating the subject.

(U//~~FOUO~~) On 11 June 2007, SSA [REDACTED] briefed ASAC [REDACTED] on the facts of the investigation and the need to engage in limited on-line undercover communication with the subject for the purpose of deploying a Computer & Internet Protocol Address Verifier (CIPAV). The Seattle Division did not anticipate more than three substantive contacts with the subject, nor was there any expectation of a face-to-face meeting. ASAC [REDACTED] authorized the limited on-line undercover activity.

b6 -1  
b7C -1

(U//~~FOUO~~) On 12 June 2007, the U.S. District Court for the Western District of Washington (Magistrate Judge James P. Donohoe) issued a search warrant [REDACTED]

b7E -5

# CYBER DIVISION

FEDERAL BUREAU OF INVESTIGATION

School in Lacey, Washington on June 4-7, 2007, threatening that 4 bombs had been planted at the school. The application was submitted to the court by the USAO for the W.D. Washington (AUSA Kathryn Warma) [REDACTED]

b7E -5

(U//~~FOUO~~) SA Norman Sanders' affidavit describes a CIPAV as a "specialized technique" that can help the government to identify a computer and/or the users of a computer. The application explains in some detail how the CIPAV would work and the type of information it would gather. Specifically, the affidavit states that "the CIPAV will be deployed through an electronic messaging program from an account controlled by the FBI" and makes clear that "essentially, if a warrant is approved, a communication will be sent to the computer being used to administer [www.myspace.com](http://www.myspace.com) (MySpace) user account 'Timberlinebombinfo.' The communication to be sent is designed to cause the above referenced computer to transmit data, in response, that will identify the computer and/or the user(s) of the computer ...." Affidavit ¶ 5. Relative to the Seattle Times piece, the affidavit does not describe the precise details of the communication(s) to be sent to the subject's computer.

(U//~~FOUO~~) [REDACTED]

b7E -2,5

(U//~~FOUO~~) The Behavior Analysis Unit (BAU) analyzed [REDACTED]

b6 -1  
b7C -1  
b7E -2

(U//~~FOUO~~) [REDACTED]

b7E -2,5

(U//~~FOUO~~) [REDACTED]

# CYBER DIVISION

FEDERAL BUREAU OF INVESTIGATION

(U//~~FOUO~~) Lacy Police Department executed an exigent circumstances request from Comcast and their SWAT Team arrested subject [redacted] at approximately 2am on 14 June 2007. The USAO declined prosecution as [redacted] was a minor and he was prosecuted at the State level.

b6 -3  
b7C -3

(U//~~FOUO~~) As there were no additional subjects in the investigation, the USAO unsealed the affidavit in 2007. Reporter Kevin Poulson, Wired Magazine, discovered and published the CIPAV article and affidavit in 2007 and no comments were provided by the FBI on the capabilities of the tool.

(U//~~FOUO~~) Upon arrest, [redacted] immediately confessed to sending multiple bomb threats to the Timberline School District. Bomb threats dated 14 June 2007 were found on the minor's computer. Two additional drafts of email bomb threats were located on his seized computer. [redacted] advised that he only used, but was not responsible for compromising, the two computers in Italy that were used to register newly created email accounts, send a series of bomb threats, and deploy DDOS attacks on the Timberline School District email server.

b6 -3  
b7C -3

(U//~~FOUO~~) On 16 July 2007, [redacted] pled guilty to three counts of Identity Theft (Class C Felony), two counts of Threat to Bomb or Injure Property (Class B Felony), and one count of Felony Harassment (Class B Felony) to the State of Washington District Court. [redacted] was sentenced on the same day to 90 days Juvenile Detention (unsuccessful at prosecuting as an adult), two years supervised release, two years mental health counseling, two years probation on all computers and electronic equipment (ipods, cell phones, X-boxes, computers, pagers, etc.), expelled from Timberline School District, and no contact prohibitions with school district and victims.

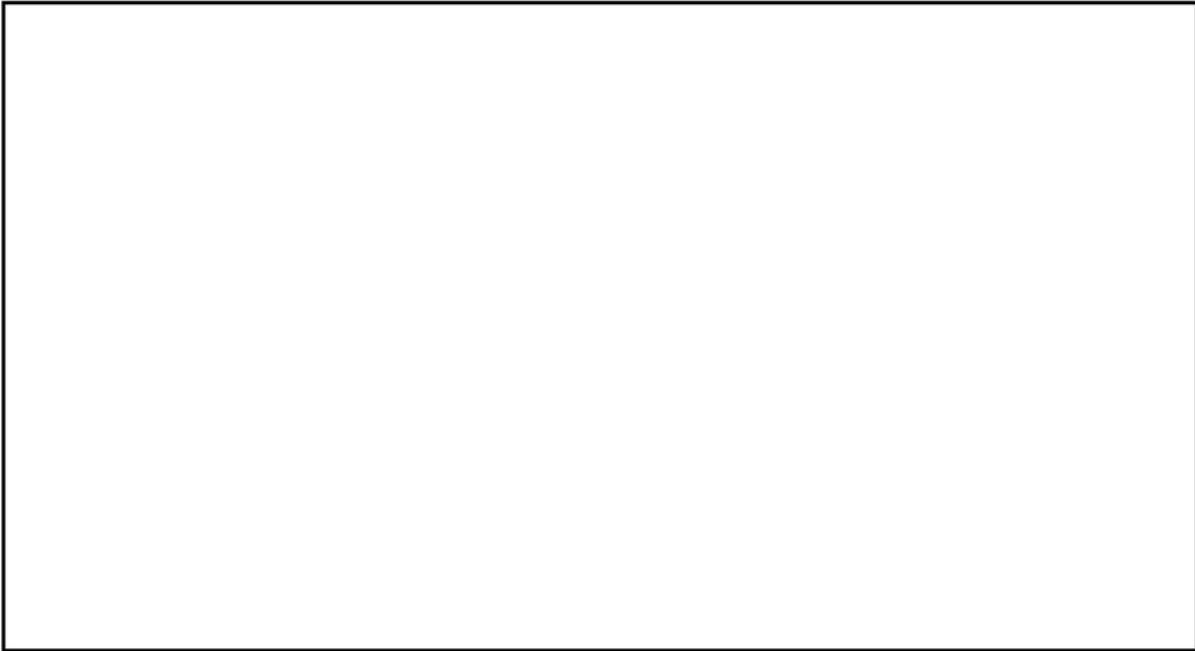
b6 -3  
b7C -3

## (U) DESCRIPTION OF CIPAV CAPABILITIES:

(U//~~FOUO~~) [redacted]

b7E -5

**CYBER DIVISION**  
FEDERAL BUREAU OF INVESTIGATION



b7E -5





**SITUATION ACTION BACKGROUND**  
**TIMBERLINE SCHOOL DISTRICT; [REDACTED]**  
**288A-SE-93709**  
**31 October 2014**

b6 -3  
b7C -3

**(U) BACKGROUND:**

(U//~~FOUO~~) On June 6, 2007, the Seattle Division was contacted by the Lacey Police Department (LPD), Lacey, WA, and the Washington State Patrol (WSP) regarding numerous bomb threats and Distributed Denial of Service (DDOS) attacks received at the Timberline School District, Lacey, WA.

(U//~~FOUO~~) The threats began on May 30, 2007 and persisted through June 7, 2007. The threats necessitated the daily evacuation of Timberline High School. The LPD and the 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 OTD/CEAU [REDACTED] [REDACTED] Further, FBI SE opened and assigned a computer intrusion investigation via EC to CyD, IOD, and OTD on June 7, 2007 [REDACTED] [REDACTED]

b7E -5

(U//~~FOUO~~) On June 11, 2007, based on the facts of the investigation the Seattle Division identified the need to engage in limited on-line undercover communication in order to identify and locate the subject through the use of a Computer & Internet Protocol Address Verifier (CIPAV). The Seattle Division did not anticipate more than three substantive contacts with the subject, nor was there any expectation of a face-to-face meeting. Seattle ASAC authorized the limited on-line undercover activity and OTD and OGC approved the use of the technique on June 12, 2007.

(U//~~FOUO~~) On June 12, 2007, the U.S. District Court for the Western District of Washington (Magistrate Judge James P. Donohoe) issued a search warrant [REDACTED] [REDACTED] School in Lacey, Washington on June 4-7, 2007, threatening that multiple explosive devices had been planted at the school. The application was submitted to the court by the USAO for the Western District of Washington, AUSA Kathryn Warma. [REDACTED] [REDACTED]

b7E -5

(U//~~FOUO~~) SA Norman Sanders' affidavit describes CIPAV as a "specialized technique" that can help the government identify a computer and/or the users of a computer. The application explains in some detail how the CIPAV would work and the type of information it would gather. Specifically, the affidavit states

# CYBER DIVISION

FEDERAL BUREAU OF INVESTIGATION

that "the CIPAV will be deployed through an electronic messaging program from an account controlled by the FBI" and makes clear that "essentially, if a warrant is approved, a communication will be sent to the computer being used to administer www.myspace.com (MySpace) user account 'Timberlinebombinfo.' The communication to be sent is designed to cause the above referenced computer to transmit data, in response, that will identify the computer and/or the user(s) of the computer ..." Affidavit ¶ 5. [REDACTED]

b7E -5

(U//FOUO) The Behavior Analysis Unit (BAU) analyzed [REDACTED]

b7E -2

(U//FOUO) [REDACTED]

b7E 2

(U//FOUO) [REDACTED]

b7E -2,5

(U//FOUO) Lacy Police Department executed an exigent circumstances request to Comcast and their SWAT Team arrested subject [REDACTED] at approximately 2:00am on 14 June 2007. The USAO declined prosecution as [REDACTED] was a minor and he was prosecuted at the State level.

b6 -3  
b7C -3

(U//FOUO) [REDACTED] immediately confessed to sending multiple bomb threats to the Timberline School District. Bomb threats dated June 14, 2007 were found on the minor's computer. Two additional drafts of email bomb threats were located on his seized computer. [REDACTED] advised that he only used, but was not responsible for compromising, the two computers in Italy that [REDACTED] used to register newly created email accounts, send a series of bomb threats, and deploy DDOS attacks on the Timberline School District email server.

b6 -3  
b7C -3

# CYBER DIVISION

FEDERAL BUREAU OF INVESTIGATION

(U//~~FOUO~~) On July 16, 2007, [REDACTED] pled guilty to three counts of Identity Theft (Class C Felony), two counts of Threat to Bomb or Injure Property (Class B Felony), and one count of Felony Harassment (Class B Felony) to the State of Washington District Court. [REDACTED] was sentenced on the same day to 90 days Juvenile Detention (unsuccessful at prosecuting as an adult), two years supervised release, two years mental health counseling, two years probation on all computers and electronic equipment (Ipods, cell phones, X-boxes, computers, pagers, etc.), expelled from Timberline School District, and no contact prohibitions with school district and victims.

b6 -3  
b7C -3

## (U) LEGAL ANALYSIS / UCO IMPERSONATING A MEMBER OF THE MEDIA:

### (U) Executive Summary:

(U//~~FOUO~~) Cyber Law Unit (CyLU) review of the relevant policies in effect at the time of the "Timberline" operation indicates the field office acted reasonably under the circumstances in approving the undercover activity. Although an argument can be made the reported impersonation of a fictitious member of the media constituted a "sensitive circumstance" that would have made the undercover activity subject to the FBI HQ review and approval required for a Group 1 undercover operation, the facts of the case do not clearly indicate that such a sensitive circumstance existed.

(U//~~FOUO~~) Even if a sensitive circumstance existed, the SAC could have provided emergency authorization of the Group 1 if he/she felt the facts justified such action and FBI HQ approval could not be obtained in time. Then-existing policy required formal notification to FBI HQ within 48 hours and additional review and notifications to DOJ. It appears FBIHQ was notified of most facts pertaining to the operation within 48 hours, but it is not clear if impersonation of a media member was part of the notification. It is also not clear if follow up with DOJ was ever conducted.

(U//~~FOUO~~) It's important to note that these FBIHQ approval requirements would only have been triggered if the activity constituted a sensitive circumstance. As detailed below, it would not have been unreasonable for Seattle to determine that no sensitive circumstances were present.

### (U) Policies:

(U//~~FOUO~~) The applicable policies at the time were the *Attorney General's Guidelines on FBI Undercover Operations (AGG-UCO May 2002)* and the *Field Guide for Undercover and Sensitive Operations (Field Guide, July 2003)* and the 2006 MIOG.

(U//~~FOUO~~) The key analysis is whether the undercover activity that took place 1) constituted an undercover operation, 2) whether that undercover operation constituted a "Group 1" that required FBI HQ approval (AD, as well as Undercover Review Committee, involving DOJ), 3) even if a sensitive circumstance were present, did the SAC grant emergency authorization to conduct the activity, and 4) was such authorization appropriate and done in accordance with policy?



(U) Was this a UCO?

(U//FOUO) The AGG-UCO (2003) defines "Undercover Operation" as: "an investigation involving a series of related undercover activities over a period of time by an undercover employee. For purposes of these Guidelines, a "series of related undercover activities" generally consists of more than three separate substantive contacts by an undercover employee with the individual(s) under investigation. However, undercover activity involving sensitive or fiscal circumstances constitutes an undercover operation regardless of the number of contacts involved."

(U//FOUO) [Redacted]

b5 -1

(U//FOUO) [Redacted]

- (j) A significant risk that a third party will enter into a professional or confidential relationship with a person participating in an undercover operation who is acting as an attorney, physician, clergyman, or member of the news media;

(U//FOUO) [Redacted]

b5 -1

(U//FOUO) However, a note in Section 3.2.C of the *Field Guide* [Redacted]

- C. Privileged Relationships  
*(7) A significant risk that a third party will enter into a professional or confidential relationship with a person participating in the UCO who is acting as an attorney, physician, clergyman, or member of the news media.*  
 \* \* \*

*NOTE: These sensitive circumstances are listed in order to identify any operational scenario in which privileged communications or defense trial strategy might be overheard; a relationship with a subject is established which the subject believes to be privileged; or a cooperating individual may be placed in*

# CYBER DIVISION

FEDERAL BUREAU OF INVESTIGATION

b7E -2

**(U) DESCRIPTION OF CIPAV CAPABILITIES:**

(U//FOUO)

||

||

||

||

||

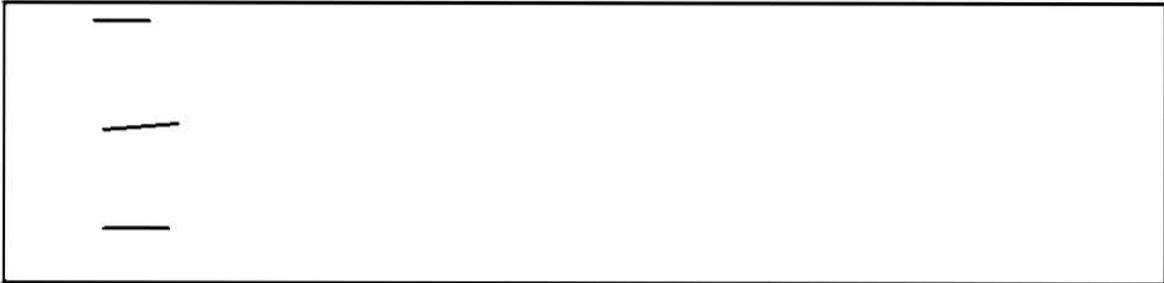
||

||

||

b7E -5

**CYBER DIVISION**  
FEDERAL BUREAU OF INVESTIGATION



b7E -5

[Redacted]

**From:** [Redacted]  
**Sent:** Thursday, June 07, 2007 11:09 PM  
**To:** [Redacted]  
**Cc:** [Redacted]  
**Subject:** Second IP Address

**UNCLASSIFIED**  
**NON-RECORD**

All,

At approximately 4:15 pm, Pacific Standard Time, an UNSUB uploaded three of the threatening emails, that were previously sent to Timberline High School, to the "Comments" section of "The Olympian" online website. We were informed that this was conducted from IP Address 192.135.29.30 which resolved to the following:

National Institute of Nuclear Physics  
Laboratori Nazionali di Legnaro  
Consortium GARR Italian Academic and Research Network  
I-00155 Roma, Italy

Abuse Contact information:

[Redacted]  
35020 Legnaro PD  
Italy  
Phone [Redacted]  
Fax [Redacted]



Timberline\_Urgent  
Report.wpd (...)



Timberline\_High\_Sc  
hool.ec.wpd ...

The above Urgent Report is being sent out tonight. We are working on [Redacted] as well as [Redacted] b7E -2  
[Redacted] We are also working on a search warrant affidavit for a CIPAV.

[Redacted]

Would you be the ones to help us on another school threat? If so, can you give me a fax number so we can send the [Redacted] b7E -2  
[Redacted]

Thanks [Redacted]

SSA [Redacted]  
Seattle Field Office  
Cyber Squad 11  
[Redacted]

[Redacted]

b6 -1  
b7C -1

**From:** [Redacted]  
**Sent:** Tuesday, June 12, 2007 8:24 PM  
**To:** [Redacted]  
**Cc:** [Redacted]  
**Subject:** RE: Timberline HS questionnaire

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

All,

The CIPAV court order was signed today. We are deploying it tonight and will let you know how it goes. Thanks again for all your help.

[Redacted]

b6 -1  
b7C -1

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

**From:** [Redacted]  
**Sent:** Tuesday, June 12, 2007 2:13 PM  
**To:** [Redacted]  
**Cc:** [Redacted]  
**Subject:** Timberline HS questionnaire

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

[Redacted]

Attached you'll find [Redacted] that you may want to consider using in your Timberline threats investigation. We have adjusted it to make it specific to your case. [Redacted]

[Redacted]

[Redacted]

b6 -1  
b7C -1  
b7E -2

Good luck -

[Redacted]

SSA [Redacted]  
Behavioral Analysis Unit 1  
CIRG/NCAVC

[Redacted]



b6 -1  
b7C -1

<< File: timberline questionnaire.wpd >>

**SENSITIVE BUT UNCLASSIFIED**

**SENSITIVE BUT UNCLASSIFIED**

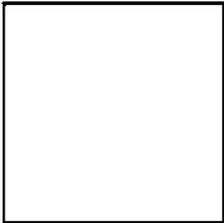
[Redacted]

b6 -1  
b7C -1

From: [Redacted]  
Sent: Tuesday, June 12, 2007 4:19 PM  
To: [Redacted]  
Subject: [Redacted]

SENSITIVE BUT UNCLASSIFIED  
NON-RECORD

b7E -2



SENSITIVE BUT UNCLASSIFIED

[Redacted]

b6 -1  
b7C -1

**From:** [Redacted]  
**Sent:** Tuesday, June 12, 2007 9:48 PM  
**To:** [Redacted]

**Cc:** [Redacted]

**Subject:** RE: Seattle Division School Bomb Threat

**Importance:** High

UNCLASSIFIED  
NON-RECORD

All,

Seattle obtained court authorization to deploy a Computer and Internet Protocol Address Verifier (CIPAV) which was deployed [Redacted]

[Redacted]

b6 -4  
b7C -4  
b7E -2,5

Timberline High School, Lacey, Washington, has been evacuated six times in the last week due to email threats emanating from [Redacted]

b7E -2,5

[Redacted]

[Redacted]

We do not have many investigative options left. Any help would be appreciated.

Thanks [Redacted]

b6 -1  
b7C -1

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

**From:** [Redacted]  
**Sent:** Wednesday, June 06, 2007 5:34 PM  
**To:** [Redacted]  
**Cc:** [Redacted]  
**Subject:** Seattle Division School Bomb Threat

**UNCLASSIFIED**  
**NON-RECORD**

<< File: lacey.rtf >>

b6 -1,5  
b7C -1,5

My name is Detective [redacted] of the Washington State Patrol. I am a member of the Northwest Cybercrime Task force located in Seattle Washington under the supervision of SSA [redacted] SSA [redacted] will be back in the Division on June 7. [redacted] advised me to provide you with this urgent information. An official opening of a case is in progress. Members of the Task Force have been in contact with a Detective [redacted] of Lacey Police Department located in Lacey, WA. He is currently working a case involving bomb threats to a high school. The unsub(s) have sent several threatening emails to school officials advising them of the presence of bombs throughout the school are set to go off at certain times. Although there have been no actual bombs found by law enforcement, school officials have evacuated the schools and expended numerous law enforcement resources. In addition, the unsub(s) have threatened to launch an DDOS attack on the school servers. The unsub(s) did perform the DDOS attack in which, according to IT personell, received over 8 million hits to their firewall in a short time frame. The following is a synopsis of the events from Detective [redacted]

The Lacey (WA) Police Department responded to Timberline High School, Wednesday May 30, Monday June 4, Tuesday June 5, and Wednesday June 6, 2007 for a bomb threat at the school. The threat on May 30th was received on a hand written note. The threats received June 4th-6Th have been received via electronic e-mail. The school has been searched extensively several times by Lacey Police Officers, School Staff, and Washington State Patrol's Bomb Detection K-9. Nothing has been found during any of these searches. In each of the e-mailed threats, the same student's name (or a variation on the spelling thereof) has been used in a "g-mail" web-based e-mail account (through Google). This student has been thoroughly interviewed and does not appear to be the suspect. He had a student in mind who may be responsible. That student has been interviewed, denied involvement. His home PC is currently being analyzed. The last e-mail was sent while that PC was in our custody. Of the now five E-mails that have been sent to school staff, we were able to serve Google with emergency disclosure requests and learned that the user created the e-mail account and was "logged-in" from an IP address associated to an ISP in Italy. (IP 80.76.80.103). The suspect, in the e-mails, provides details that would be known by a student familiar with current happenings in the school, leading us to believe he is likely a current student. Currently, several students have been interviewed who have been identified by staff as possibly having both the perceived "technical capability" as well as some reason to believe that they may be inclined to do such a thing. Nothing in the interviews has yielded a viable suspect.

I have attached several e-mails, to include header information. Any assistance that can be provided in identifying the source, or a means to contact and further identify the Italian ISP and / or proxy would be greatly appreciated.

[redacted]  
Detective,  
Lacey Police Department  
420 College St. SE.  
P.O. Box 3400  
Lacey, WA 98509-3400  
Office: [redacted]  
Nextel: [redacted]  
Dispatch: (360) 704-2740

b6 -5  
b7C -5

Detective [redacted] and SA [redacted]

[redacted]

b6 -1,5  
b7C -1,5  
b7E -2

SSA [redacted] will be calling the morning hours Pacific time to further discuss this urgent matter. I have included an attachment of the emails sent to the school officials.

Thank you for your assistance in this matter.

Detective [redacted]  
Northwest Cybercrime Task Force  
Seattle, Wa  
wk: [redacted]  
cell [redacted]

b6 -5  
b7C -5

**UNCLASSIFIED**

**UNCLASSIFIED**

[Redacted]

**From:** [Redacted]  
**Sent:** Thursday, June 14, 2007 4:02 PM  
**To:** [Redacted]  
**Subject:** Urgent Report

UNCLASSIFIED  
NON-RECORD

[Redacted]

b6 -1  
b7C -1

This was what we sent today.



Timberline\_Urgent\_Report\_Arres...

Thanks, [Redacted]

UNCLASSIFIED

### FBI URGENT REPORT

**Precedence:** IMMEDIATE

**Date:** 06/14/2007

**To:** Director  
SIOC  
Cyber  
CIRG  
Operational Technology  
International Operations  
Rome

**From:** Seattle

**Contact:** SSA [REDACTED]

b6 -1  
b7C -1

**Approved By:** SAC

**Drafted By:** [REDACTED]

**Subject/Title/Case ID #:** 288A-SE-93709

[REDACTED] (JUVENILE) - SUBJECT  
TIMBERLINE HIGH SCHOOL - VICTIM  
COMPUTER INTRUSION - THREAT

b6 -3  
b7C -3

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

UPDATE  
URGENT REPORT

On 06/14/2007, at approximately 2:00 am, Pacific Standard Time, the below listed juvenile was arrested by the Lacey Police Department, for seven Washington State counts of Threats to Bomb or injure Property, Felony Harassment (Threats to Kill), and Identity Theft.

**NAME:** [REDACTED]  
**DOB:** [REDACTED]  
**AGE:** [REDACTED]  
**SEX:** MALE  
**RACE:** WHITE  
**ADDRESS:** [REDACTED]  
**MISC:** 10TH GRADE STUDENT  
TIMBERLINE HIGH SCHOOL

b6 -3  
b7C -3

[REDACTED] was identified as the subject of the investigation after a successful deployment of a court authorized

To: Director From: Seattle  
Re: 06/14/2007

Computer and Internet Protocol Address Verifier (CIPAV). The CIPAV was deployed through an undercover electronic message session between Seattle undercover employees and [REDACTED]

b6 -3  
b7C -3

[REDACTED] immediately confessed to sending the threats and two additional drafts of email bomb threats were located on his seized computer. [REDACTED] advised that he only used, but was not responsible for compromising the two computers in Italy. Investigation in Seattle continues.

#### BACKGROUND

On 06/06/2007, the Seattle Field Office was contacted by the Lacey Police Department (LPD), Lacey, WA, regarding email bomb threats and Distribute 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 email threats commenced on 06/04/2007, and continue to the present. To date, there have been three email 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 email content has repeatedly demeaned school faculty and teachers and taunts law enforcement. The UNSUB(S) also posted three of the email threats in the "Comments" section of "The Olympian" news online website.

Investigation conducted by LPD identified three Internet Protocol (IP) addresses being utilized, two in Italy and one in the Czech Republic, which at this time are believed to be proxies. A request for assistance has been forwarded to the Italian National Police by LEGAT Rome.

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.

To: Director From: Seattle  
Re: 06/14/2007

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

(URGENT REPORT 06/07/2007)

◆◆

FILED  
LODGED

ENTERED  
RECEIVED

JUN 12 2007

AFFIDAVIT

MS07 088 JPS

AT SEATTLE  
CLERK U.S. DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

STATE OF WASHINGTON  
COUNTY OF KING

ss:

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

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

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

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

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

Warrant FBSSU.

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 being used to administer  
6 www.myspace.com,<sup>1</sup> ("MySpace") user account "Timberlinebombinfo".

7 The communication to be sent is designed to cause the above referenced  
8 computer to transmit data, in response, that will identify the computer and/or the  
9 user(s) of the computer.<sup>2</sup> In this manner, the FBI may be able to identify the computer  
10 and/or user of the computer that are involved in committing criminal violations of  
11 United States Code specifically, Title 18, United States Code, Sections 875(c)  
12 (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 a). the use of a Computer & Internet Protocol Address<sup>3</sup> ("IP address")

16  
17 <sup>1</sup> MySpace is a international free service that uses the Internet for online communication through  
18 an interactive social network of photos, videos, weblogs, user profiles, blogs, e-mail, instant  
19 messaging, web forums, and groups, as well as other media formats. MySpace users are capable of  
20 customizing their user webpage and profile. Users are also capable of searching or browsing other  
21 MySpace webpages and adding other users as "friends". If the person identified approves your  
22 "friend" request, he or she will be added to your list of friends. Users are capable of sending MySpace  
23 messages and posting comments on other user's MySpace webpages.

24 <sup>2</sup> In submitting this request, the Government respectfully does not concede that a reasonable  
25 expectation of privacy exists in the internet protocol address assigned by a network service provider or  
26 other provider to a specific user and used to address and route electronic communications to and from  
27 that user. Nor does the government concede that a reasonable expectation of privacy is abridged by the  
28 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.

<sup>3</sup> Conceptually, IP addresses are similar to telephone numbers, in that they are used to identify  
computers that exchange information over the Internet. An IP address is a unique numeric address  
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  
and receiving the information. Section 216 of the USA Patriot Act (P.L. 107-56) amended 18 U.S.C.  
§§3121 *et seq* to specifically authorize the recovery of "addressing" and "routing" information of

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 messages<sup>4</sup> containing the activating computer's IP address and/or MAC  
8 address,<sup>5</sup> other environment variables, and certain registry-type information<sup>6</sup> 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 d). that, pursuant to 18 U.S.C. §3103a(b)(3), to satisfy the notification  
14

15 \_\_\_\_\_  
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 <sup>4</sup> 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 <sup>5</sup> 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 <sup>6</sup> As used here, "registry-type information" refers to information stored on the internal hard  
27 drive 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 requirement of Federal Rule of Criminal Procedure 41(f)(3), the FBI may delay  
2 providing a copy of the search warrant and the receipt for any property taken until no  
3 more than thirty (30) days after such time as the name and location of the owner or user  
4 of the activating computer is positively identified or a latter date as the court may, for  
5 good cause shown, authorize. Provision of a copy of the search warrant and receipt  
6 may, in addition to any other methods allowed by law, be effectuated by electronic  
7 delivery of true and accurate electronic copies (e.g. Adobe PDF file) of the fully  
8 executed documents.

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

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

1 | messages, and/or other variables, and/or registry information, over the Internet<sup>7</sup> 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) of 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.

25 |       9. Every time a computer accesses the Internet and connects to a web site,

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

1 that computer broadcasts its IP address along with other environment variables.  
2 Environment variables, such as what language the user is communicating in, allows the  
3 web site to communicate back and display information in a format that the computer  
4 accessing the web site can understand. These environment variables, including but not  
5 limited to, the IP address and the language used by the computer, may assist in locating  
6 the computer, as well as provide information that may help identify the user of the  
7 computer.

8 10. The hard drives of some computers contain registry-type information. A  
9 registry contains, among other things, information about what operating system  
10 software and version is installed, the product serial number of that software, and the  
11 name of the registered user of the computer. Sometimes when a computer accesses the  
12 Internet and connects to a software vendor's web site for the purpose of obtaining a  
13 software upgrade, the web site retrieves the computer's registry information stored on  
14 its internal hard drive. The registry information assists the software vendor in  
15 determining if that computer is running, among other information, a legitimate copy of  
16 their software because the registry information contains the software's product  
17 registration number. Registry information, such as the serial number of the operating  
18 system software and the computer's registered owner, may assist in locating the  
19 computer and identifying its user(s).

## 20 21 THE INVESTIGATION

22 11. On May 30, 2007, a handwritten note was discovered on the premises of  
23 the Timberline High School in Lacey, Washington. Subsequently, school  
24 administrators ordered an evacuation of the students based on the handwritten bomb  
25 threat note.

26 a). On June 4, 2007, Timberline High School received a bomb threat  
27 e-mail from sender: "dougbriggs123@gmail.com". The Unknown Subject(s)  
28 (UNSUB) stated in the e-mail "I will be blowing up your school Monday, June 4,

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

8 b). On June 5, 2007, the UNSUB(s) sent an e-mail from  
9 "dougbriggs@gmail.com" stating the following:

10 <<Read This ASAP>>

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

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

22 The UNSUB(s) goes on to state:

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

29 c). In another e-mail from sender "dougbriggs234@gmail.com"  
30 the UNSUB(s) states the following:

31 Hello Again. Seeing as how you're too stupid to trace the email  
32 back lets get serious." [The UNSUB(s) mentions 6 bombs set to

33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
1000

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

1 | detonate between 10:45-11:15 AM, and adds] Seriously, you are not  
2 | going to catch me. So just give up. Maybe you should hire Bill  
3 | Gates to tell you that it is coming from Italy. HAHAHA Oh wait I  
4 | already told you that. So stop pretending to be "tracing it" because I  
5 | have already told you it's coming from Italy. That is where trace  
6 | will stop so just stop trying. Oh and this email will be behind a  
7 | proxy behind the Italy server.

8 | d). School administrators ordered an evacuation of the school on June  
9 | 5, 2007.

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

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

15 | Well hello Timberline, today is June 6, 2007 and I'M just emailing  
16 | you today to say that school will blow up and that's final! There  
17 | are 2 bombs this time (Iran short on money to buy things at home  
18 | depot). They will go off at exactly 10:45:00 AM. One is on  
19 | located on a portable. And the other is somewhere else. Keep  
20 | trying to 'trace' this email. The only thing you will be able to  
21 | track is that it came from Italy. There is no other information that  
22 | leads it back to the United States in any way so get over it.  
23 | You should hire Bill Gates to track it for you. HAHAHAHA. He  
24 | will just tell you that it came from over seas, so if you have close  
25 | relations with the POPE you might get some information. But  
26 | other than that, have fun looking in Italy. :-)

27 | Also, stop advising teachers to no show this email to classmates.  
28 | Everyone would be ammused by this email and I might stop if you  
29 | do. Funny how I can trick you all into thinking that I included my  
30 | name to show that it isn't me, because who the hell would put their  
31 | 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  
33 | email account that has  
34 | already been deleted of all information by the time you read this  
35 | email. Get your ass on a plane to Italy if you want it to stop.

36 | g). School administrators ordered an evacuation of the school on  
37 | June 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:

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

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

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

12  
13 k). On June 7, 2007, Detective Jeremy Knight, Lacey Police  
14 Department (LPD), received information from the Thurston County Sheriff's Office,  
15 which had revealed a complaint from a person identified as AG. AG stated that she  
16 received an invitation through myspace.com from the MySpace profile of  
17 "Timberlinebombinfo" wanting her to post a URL link to  
18 <http://bombermails.hyperphp.com> on her myspace.com webpage. The UNSUB(s)  
19 advised her that failure to comply would result in her name being associated with future  
20 bomb threats. Similarly, Knight received a phone call from a parent alleging that her  
21 son received the same request from the UNSUB(s). According to Knight, 33 students  
22 received a request from the UNSUB(s) to post the link on their respective myspace.com  
23 webpages. Subsequent interviews performed by Knight yielded limited information.

24  
25 l). On June 7, 2007, VW and BP received MySpace private invitations  
26 from an individual utilizing the MySpace moniker "Timberlinebombinfo". VW  
27 accepted the invitation from "Timberlinebombinfo" and received an America Online  
28 Instant Message (AIM) from an individual utilizing AIM screen name

1 "Alexspi3ring\_09." Communication ceased with "Alexspi3ring\_09" after VW  
2 requested additional information related to the bomb threats. VW believed screen name  
3 "Alexspi3ring\_09" was associated to ALEX SPIERING, a student at Timberline High  
4 School. VW stated "Alexspi3ring\_09" and "Timberlinebombinfo" used to have the  
5 identical graphic on their MySpace webpage. "Timberlinebombinfo" recently changed  
6 his/her graphic from a picture of guns to a picture of a bomb.

7  
8 m). On June 7, 2007, Thurston County School District reported ALEX  
9 SPIERING resides at 6133 Winnwood Loop SE, Olympia, WA, 98513, telephone (360)  
10 455-0569, date of birth [REDACTED], 19[REDACTED].

11  
12 n). On June 8, 2007, Comcast Internet, Thorofare, New Jersey,  
13 reported that residential address 6133 Winnwood Loop SE, Olympia, WA, 98513  
14 received Comcast Internet services for the following subscriber:

15 Sara Spiering  
16 6133 Winnwood Loop SE, Lacey, WA 98513  
17 Telephone (360) 455-0569  
18 Dynamically Assigned Active Account  
19 Account Number: 8498380070269681

20  
21 o). On June 8, 2007, Thurston County School District received two  
22 additional bomb threat e-mails from "Timberline.Sucks@gmail.com." which resulted in  
23 the evacuation of the Timberline High School.

24  
25 12. On June 4, 2007, Google provided subscriber, registration, and IP Address  
26 log history for e-mail address "dougbriggs123@gmail.com" with the following results:

27 Status: Enabled (user deleted account)  
28 Services: Talk, Search History, Gmail

1 Name: Doug Briggs  
2 Secondary Email:  
3 Created on: 03-Jun-2007  
4 Lang: en  
5 IP: 80.76.80.103  
6 LOGS: All times are displayed in UTC/GMT  
7 dougbriggs123@gmail.com

8	Date/Time	IP
9	04-Jun-2007 05:47:29 am	81.27.207.243
10	04-Jun-2007 05:43:14 am	80.76.80.103
11	03-Jun-2007 06:19:44 am	80.76.80.103

12  
13 a). On June 6, 2007, a SmartWhoIs lookup of IP Address 80.76.80.103  
14 resolved to Sonic S.R.L, Via S.Rocco 1, 24064, Grumello Del Monte, Italy,  
15 Phone: +390354491296, E-mail: Staff@sonic.it. Your affiant connected to  
16 http://sonic.it, which displayed an Italian business webpage for Sonic SRL Internet  
17 Service Provider.

18  
19 b). On June 7, 2007, a request to MySpace for subscriber and IP  
20 Address logs for MySpace user "Timberlinebombinfo" provided the following results:

21	User ID:	199219316
22	First Name:	Doug
23	Last Name:	Briggs
24	Gender:	Male
25	Date of Birth:	12/10/1992
26	Age:	14
27	Country:	US
28	City:	Lacey

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

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

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

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

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

24           b).       the individual(s) using the aforementioned activated computer  
25 utilized compromised computers to conceal their true originating IP address and thereby  
26 intentionally inhibiting the individual(s)' identification. Compromised computers are  
27 generally infected with computer viruses, trojans, or other malevolent programs, which  
28 can allow a user the ability to control computer(s) on the Internet or particular services

1 of compromised computer(s) without authorization. It is common for individuals  
2 engaged in illegal activity to access and control compromised computer(s) to perform  
3 malicious acts in order to conceal their originating IP addresses.

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

11 15. The CIPAV will be deployed through an electronic messaging program  
12 from an account controlled by the FBI. The computers sending and receiving the  
13 CIPAV data will be machines controlled by the FBI. The electronic message deploying  
14 the CIPAV will only be directed to the administrator(s) of the "Timberlinebombinfo"  
15 account.

- 16 a). Electronic messaging accounts commonly require a unique user  
17 name and password.
- 18 b). Once the CIPAV is successfully deployed, it will conduct a one-  
19 time search of the activating computer and capture the information  
20 described in paragraph seven.
- 21 c). The captured information will be forwarded to a computer  
22 controlled by the FBI located within the Eastern District of  
23 Virginia.
- 24 d). After the one-time search, the CIPAV will function as a pen register  
25 device and record the routing and destination addressing information  
26 for electronic communications originating from the activating  
27 computer.
- 28

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

7 CONCLUSION

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

15 17. Because notice as required by Federal Rule of Criminal Procedure  
16 41(f)(3) would jeopardize the success of the investigation, and because the investigation  
17 has not identified an appropriate person to whom such notice can be given, I hereby  
18 request authorization to delay such notice until an appropriate person is identified.  
19 Further, assuming providing notice would still jeopardize the investigation after an  
20 appropriate person to receive notice is identified, I request permission to ask this Court  
21 to authorize an additional delay in notification. In any event, the United States  
22 government will notify this Court when it identifies an appropriate person to whom to  
23 give notice, so that this Court may determine whether notice shall be given at that time.

24 18. Because there are legitimate law enforcement interests that justify an  
25 unannounced use of the CIPAV and review of the messages generated by the activating  
26  
27  
28

1 computer in this case,<sup>9</sup> 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 certain  
5 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  
8 warrant during the daytime unless the judge for good cause expressly authorizes  
9 execution at another time..." In order to comply with Rule 41, the Government will  
10 only deploy CIPAV between the hours of 6:00 a.m. and 10:00 p.m. (PST) during an  
11 initial 10-day period. However, the Government seeks permission to read any messages  
12 generated by the activating computer as a result of a CIPAV at any time of day or night  
13 during the initial 10-day period. This is because the individuals using the activating  
14 computer may activate the CIPAV after 10:00 p.m. or before 6:00 a.m., and law  
15 enforcement would seek to read the information it receives as soon as it is aware of the  
16 CIPAV response given the emergent nature of this investigation. If the CIPAV is not  
17 activated within the initial 10-day period, the Government will seek further authorization  
18 from the Court to read any information sent to the computer controlled by the FBI as a  
19 result of that CIPAV after the 10<sup>th</sup> day from the date the Court authorizes the use of the  
20 first 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 computer to activate  
23 a CIPAV, I request that this Court authorize the FBI to continue using additional  
24 CIPAV's in conjunction with the target MySpace account (for up to 10 days after this  
25 warrant is authorized), until a CIPAV has been activated by the activating computer.

26  
27 <sup>9</sup> 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           a).   the use of multiple CIPAVs until one CIPAV is activated by the  
4 activating computer in conjunction with the target MySpace "Timberlinebombinfo"  
5 account, without prior announcement, within 10 days from the date this Court authorizes  
6 the use of the first CIPAV;

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

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

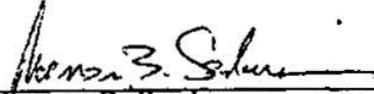
14          d).   that once the FBI has received an initial CIPAV response from the  
15 activating computer consisting of network level messages containing the activating  
16 computer's IP address, and/or MAC address, and/or other variables, and/or certain  
17 registry-type information, the FBI will thereafter only be collecting the types of  
18 addressing and routing information that can be collected pursuant to a pen register  
19 order; and

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

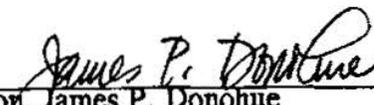
1 22. It is further requested that this Application and the related documents be  
2 filed under seal. The information to be obtained is relevant to an on-going investigation.  
3 Premature disclosure of this Application and related documents may jeopardize the  
4 success of the above-described investigation.

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

8  
9 **THIS APPLICATION DOES NOT SEEK AUTHORIZATION TO OBTAIN**  
10 **THE CONTENT OF ANY ELECTRONIC COMMUNICATIONS, AND THE**  
11 **WARRANT WILL SO SPECIFY.**

12   
13 Norman B. Sanders  
14 Special Agent  
15 Federal Bureau of Investigation

16 Sworn to and subscribed before  
17 me this 12<sup>th</sup> day of June, 2007

18   
19 Hon. James P. Donohue  
20 United States Magistrate Judge



# FBI FACSIMILE COVER SHEET

### PRECEDENCE

- Immediate
- Priority
- Routine

### CLASSIFICATION

- Top Secret
- Secret
- Confidential
- Sensitive
- Unclassified

Time Transmitted: [Redacted]  
 Sender's Initials: [Redacted]  
 Number of Pages: 12  
 (including cover sheet)

To: CIRG / NCAVC Date: 6/8/07  
Name of Office

b6 -1  
b7C -1

Facsimile Number: [Redacted]  
 Attn: SSA [Redacted]  
Name Room Telephone

From: Seattle  
Name of Office

Subject: Timberline High School  
Bomb Threats

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

Originator's Name: SSA [Redacted] Telephone: [Redacted]  
 Originator's Facsimile Number: [Redacted]

b6 -1  
b7C -1

Approved: \_\_\_\_\_  
 Brief Description of Communication Faxed: copies of email threats

### WARNING

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



07-3955



From:  
To:  
Cc:

Sent: Sun 6/3/2007 8:55 PM

b6 -4,6  
b7C -4,6



b6 -4  
b7C -4

Subject: Read Please  
Attachments:

I will be blowing up your school Monday, June 4, 2007. 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 starting at 9:15 AM. The bombs are in secret hiding places throughout the building I have specified.

Have fun.

-Your Mom

Oh and ps. The email server for your district will be offline starting at 8:45 am.



Black markings not FOIA redactions



From: [Redacted]  
Sent: Tuesday, June 05, 2007 7:33 AM  
To: [Redacted]  
Subject: Read this or die.

b6 -4,5,6  
b7C -4,5,6

Now that the school is scared from ~~the~~ ~~days~~ ~~fake~~ bomb threat it's now time to get serious. There are actually 5 bombs planted throughout the school. One in a gym locker room, the girls. It's in a locker hidden under a pile of clothes. The other four I will only say the general location. One in the Language Hall, One in the math hall, One underneath a portable taped with strong ducktape. This bomb will go off if any vibrations are felt. And the last one, is in a locker. It is enclosed in a soundproof package, and ~~is~~ undetectable. I have used a variety of chemicals to make the bombs. They are all different kinds.

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

Good luck.



b7E -7

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

PS - FREE PARIS HILTON!

Black markings not FOIA redactions

b6 -1  
b7C -1

[Redacted]

From: [Redacted]

Sent: Tuesday, June 05, 2007 5:04 PM

To: [Redacted]

Subject: FW: Bomb Threat Email. Should you open it? You better if you want to live nigga's!

b6 -4  
b7C -4

[Redacted] Here is the first one that came in and I will send the next one after this. Thanks, [Redacted]

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

From: [Redacted]

Sent: Tuesday, June 05, 2007 4:33 PM

To: [Redacted]

Cc: [Redacted]

b6 -6  
b7C -6

[Redacted]

b6 -4  
b7C -4

Subject: Bomb Threat Email. Should you open it? You better if you want to live nigga's!

— Hello Again. Seeing as how you're too stupid to trace the email back lets get serious. There are 6 bombs. One in a locker in the math hall, and the rest are scatted around the portables, commons, kitchen, etc. They will go off at any time between 10:45AM and 11:15AM

b7E -7

~~Seriously, you are not going to catch me. So just give up.~~ [Redacted]

Maybe you should hire Bill Gates to tell you that it is coming from Italy. HAHHAH Oh wait I already told you that. ~~because I have already told you it's coming from Italy.~~ That is where any trace will stop ~~so just stop trying.~~ Oh and this email will be behind ~~behind~~ behind the Italy server.

**Shoutouts:**

- [Redacted] - For being myself ;-)
- [Redacted] For always being a self centered little bitchy ass fat woman. Go die. :-)
- [Redacted] for being a cool science teacher
- [Redacted] - For getting me fit
- [Redacted] - For being the best teacher ever at Timberline. I love you!-

b6 4,6  
b7C 4,6  
b7E -7

Isn't it funny how most people beleive this theory about if I was really doing it I wouldn't put my name? Or is that just what I want you to think?

b7E -7

-----  
Peace Homies!

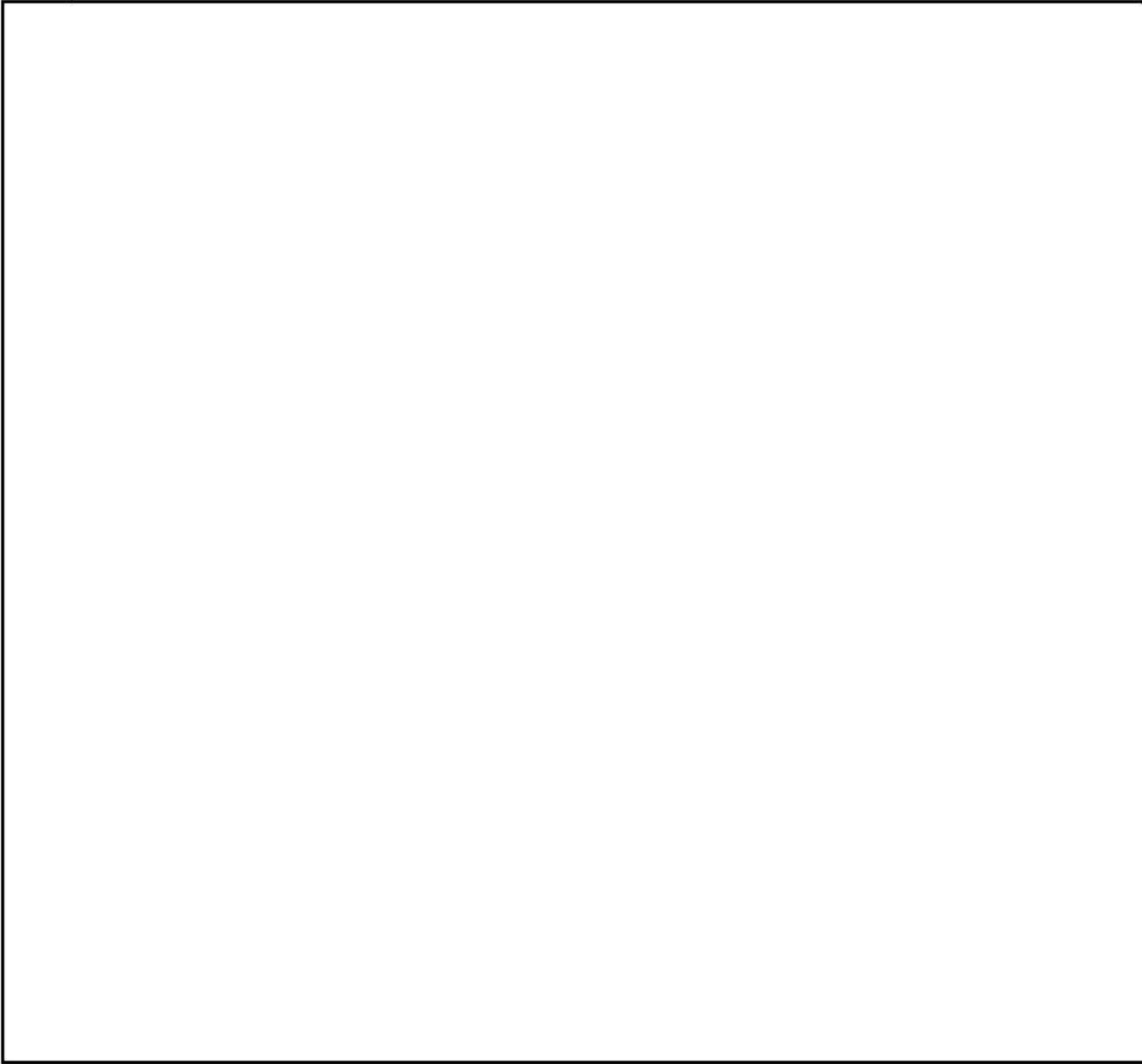


Black markings not FOIA redactions

PS - One of the bombs is not "inside" the school, but it could be in a bush, tree, roof, underground or anywhere.

PPS - The Model United Nations is SHIT!

This time I have chosen  be the original reciever of this email.



b7E -7

[Redacted]

[Redacted]

b6 -4  
b7C -4

**From:** [Redacted]  
**Sent:** Tuesday, June 05, 2007 5:04 PM  
**To:** [Redacted]  
**Subject:** FW: MAIL DELIVERY DELAYED

Here is the second one. [Redacted]

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

**From:** [Redacted]  
**Sent:** Tuesday, June 05, 2007 4:36 PM  
**To:** [Redacted]  
**Cc:** [Redacted]

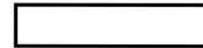
b6 -6  
b7C -6

[Redacted]

b6 -4  
b7C -4

**Subject:** MAIL DELIVERY DELAYED

— This message from gmail has been delayed 2 days. Please ignore these messages. And any messages sent before this.



Black markings not FOIA redactions

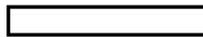


b6 -4,5,6  
b7C -4,5,6

**From:** [Redacted]  
**Sent:** Wednesday, June 06, 2007 9:03 AM  
**To:** [Redacted]  
**Subject:** Dear Mr. [Redacted]

ENJOY YOUR LIFE ENDING.

I



From: [Redacted]  
Sent: Wednesday, June 06, 2007 9:07 AM  
To: [Redacted]  
Subject: FW: ooo Should you read this. It could be a bomb threat!

b6 -4  
b7C -4

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

From: [Redacted]  
Sent: Wednesday, June 06, 2007 9:03 AM  
To: [Redacted]  
Cc: [Redacted]

b6 -6  
b7C -6



b6 -4  
b7C -4

**Subject:** ooo Should you read this. It could be a bomb threat!

Well hello Timberline, today is June 06, 2007 and I'M just emailing you to say that the school will blow today. And that's final! There are 2 bombs this time (I ran short on money to buy things at the home depot). They will go off at exactly 10:45:00 AM. One is located on a portable. And the other is somewhere else.

Keep trying to "trace" this email. The only thing you will be able to track is that it came from Italy. There is no other information that leads it back to the United States in any way so get over it.

You should hire Bill Gates to track it for you. HAHAHAHA. He will just tell you that it came from over seas, so if you have close relations with the POPE you might get some information. But other than that, have fun looking for Italy. :-)

Also, stop advising teachers to not show this email to classmates. Everyone would be ammused by this email and I might stop if you do.

Funny how I can trick you all into thinking that I included my name to show that it isn't me, because who the hell would put their name? Or is that just what I want you to think.

And yet again, this email was sent from over seas to a newly made email account that has already been deleted of all information by the time you read this email. Get your ass on a plane to Italy if you want it to stop.

Some Random Shoutouts:

[Redacted] For being so cool. I'M just so cool.

b6 -6  
b7C -6

STUDENT STORE'S SALE IS A RIP OFF. SMOOTHIES SHOULD BE \$1.00! AND MY CUP OF



NOODLES I LOVE AND BUY EVERY DAMN DAY SHOULD BE FREE!

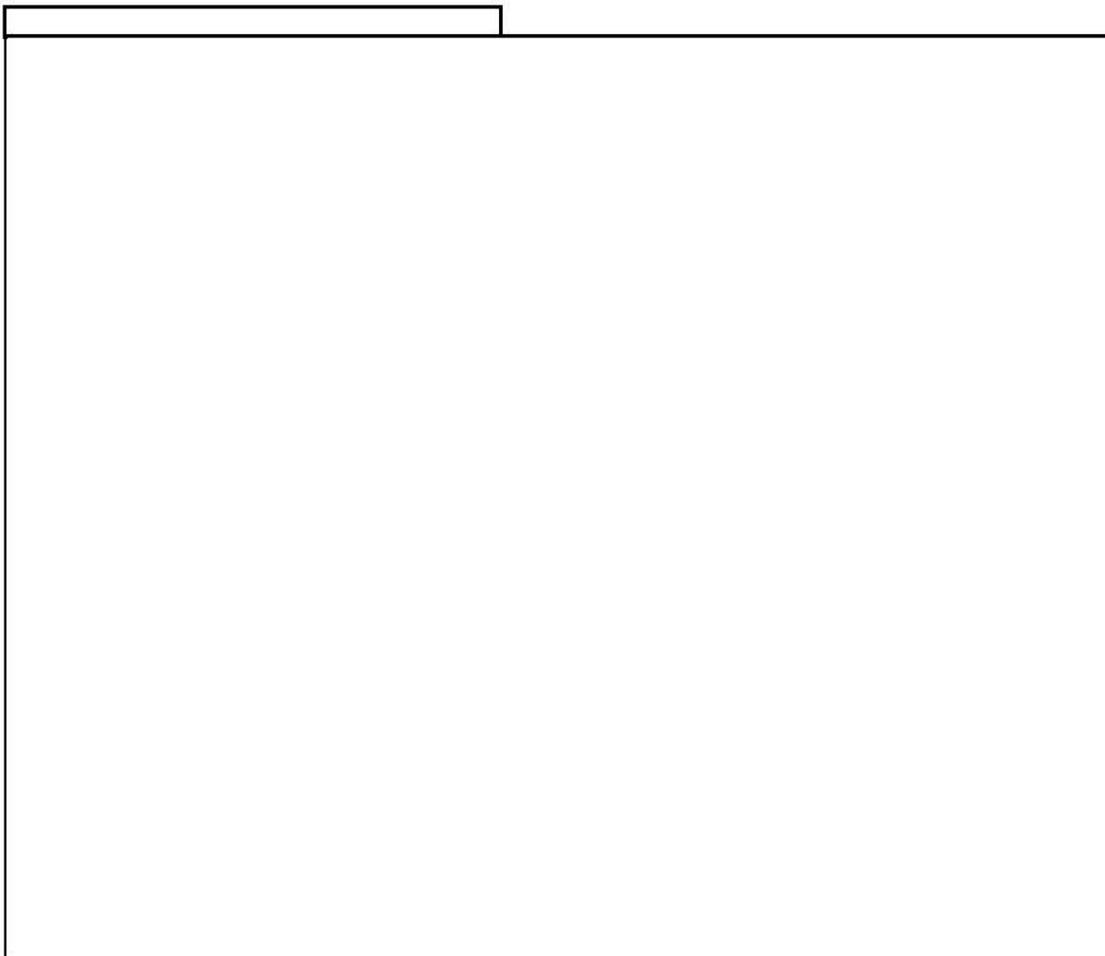
S - I am in  advisory. Or am i.

b6 -4  
b7C -4

-----  
FREE PARIS!



**From:**  
**To:**  
**Cc:**



b6 -6  
b7C -6

b6 -4  
b7C -4

**Sent:** Thursday, June 07, 2007 7:20 AM  
**Subject:** Oh noes! Anotha bomba threat! Whatcha gonna dooo!

Hello Timberline teachers & staff. Today is June 7, 2007. I think you know what this email is going to say. There are 3 bombs planted in the school and they're all different kinds. I have premade these weeks in advance and tested the timers to make sure they work to the exact millisecond. Locking the doors was a good plan, but too late.

One bomb is located in a locker room. In a locker, under a pile of gym clothes of mine. I won't say which locker room but I think you get the drift. There is one located on the roof, attached to a certain position on the ceiling so the roof caves in, this is a high explosive bomb and should be handled with care. Finally, the last bomb could be in any room, area, anywhere!. Lets hope it's not "YOUR" classroom!

They will go off anytime from 8:30AM to 9:00 AM.

## Black markings not FOIA redactions

Since you all must not listen well, let me tell you again. This email was sent from overseas, across the atlantic ocean from Italy. Actually North Italy to be specific. Maybe when your idiotic technology staff, washington state police/patrol, FBI finish "tracing" or "tracking" this email they will find out the same thing I have told you. It's coming from Italy located on a Dedicated Server under someone elses name that lives in Italy. There is no way to trace any other information other than that. The closest you will get is figuring out who owns the server [REDACTED] already.

I hope everyone has a wonderful, [REDACTED] and you can all kiss my ass.

## Special Shoutouts Requested By Friends:

- [REDACTED] is a fucking bitch and needs to go lose some weight before she gives anyone detetion again.
- Emo's are gay
- Gay people can go suck a fucking cock because all they do is get off to guys in the locker room
- [REDACTED] - For Being a fucking retard.
- [REDACTED] - coolest teacher ever
- FBI - you're all retards [REDACTED] to this fucking email. ITS CALLED ITALY DUMBASSES.
- [REDACTED] from the office needs to pluck her beard
- Italy is the shit
- Bombs are easy to make. I even looked up and printed how to do it at school!
- [REDACTED] is a cool teacher.
- [REDACTED] Cool teacher.

b6 -4  
b7C -4

## Winning Shoutout On Myspace Contest:

[REDACTED] is the most nasty, monkey looking, idiot teacher at this school. His breath stinks, someone give him a tic tak.

PS - You better just give away that prize money now, no one has any information!

PPS - Stop hiding information from students. They have every right to know what is going on in their school. They're in it you know. Stop being pussy's and let people know. Don't you think I wouldn't tell anyone. Well DUH! That's stupid if you tell. But I'M glad to say, I have heard multiple rumors and there are many different people thinking It's someone else. so good luck. Have fun calling Italy.

-YANKES RULE - YOUR MOM

PARIS WAS RELEASED FROM JAIL THIS MORNING! WOOOOOO!

Sincerely, [REDACTED]

b6 -6  
b7C -6BC50-111  
6/7/2007



---

**From:** [Redacted]  
**To:** [Redacted]  
**Sent:** Thursday, June 07, 2007 7:20 AM  
**Subject:** You have been chosen.

b6 -4,6  
b7C -4,6

You have been chosen to be the original recipient of the bomb email. Please take full pride because this was completely random.



[Redacted]

b6 -1  
b7C -1

**From:** [Redacted]  
**Sent:** Monday, October 29, 2007 12:35 PM  
**To:** [Redacted]  
**Subject:** RE: Questions regarding the Timberline Case

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

I will be on leave on Thursday - (I know [Redacted] planned it this way) -

But these are the questions I had sent before [Redacted] dressed me down for contacting the CA directly.

Good luck!

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

**From:** [Redacted] (IR) (FBI)  
**Sent:** Thursday, June 28, 2007 10:07 AM  
**To:** [Redacted]  
**Cc:** [Redacted]  
**Subject:** Questions regarding the Timberline Case

b6 -1  
b7C -1

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

[Redacted]

Hello! I helped [Redacted] on the Timberline Case.

As I indicated at the time - we are trying to apply some word count content analysis techniques to analyzing threats and helping us get some characteristics of subjects.

I am sure you guys are busy, but a few questions if you have the time for the Case Agents would be helpful. I am trying to align the case investigative activity and subjects activity with the word counts.

- When was the Bathroom Note? What did it say?
- The handwritten note was hand delivered to the Principal? When? Can we get a copy of it?
- When was [Redacted] interviewed?
- Was the Subject ever interviewed or questioned even peripherally during the investigation?
- Any information about the relationship between [Redacted] and Subject?
- Subject and [Redacted]
- Subject and [Redacted]
- Subject acted alone? Anyone else "know"? Did he brag at all?
- Subject posted three of the threatening Emails to the Olympian comments page - which ones and when? (Contemporaneously?)
- MySpace Account was opened when?
- IMing the girls - when did he start and when did he end?

b6 -4,6  
b7C -4,6

- I believe [Redacted] told me the IPAV was successful when he responded to the advanced copy of the article - could you provide details of this?
- If they ever construct a timeline - it would be good to have

b6 -1,6  
b7C -1,6

Because there is so much behavior here, and the victimology appears to be important [Redacted], this will be a great teaching/learning case. Your input/information will help us do a better job next time.

Thanks again.

[Redacted]

[Redacted]

**From:** [Redacted]  
**Sent:** Friday, October 26, 2007 2:24 PM  
**To:** [Redacted]  
**Subject:** FW: Lacey PD / Behavioral Science Unit

UNCLASSIFIED  
NON-RECORD

b6 -1  
b7C -1

[Redacted]

Will this work for you?

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

**From:** [Redacted]  
**Sent:** Friday, October 26, 2007 11:23 AM  
**To:** [Redacted]  
**Subject:** Lacey PD / Behavioral Science Unit

UNCLASSIFIED  
NON-RECORD

[Redacted] - Detective [Redacted] Lacey PD is available November 1 at 10a.m. Please have Behavior Unit conference me at my desk or cell phone if our Search Warrant executes on 11/1/07. [Redacted] will have the file ready during the meeting at [Redacted] desk / [Redacted] cell.

b6 -1,5  
b7C -1,5

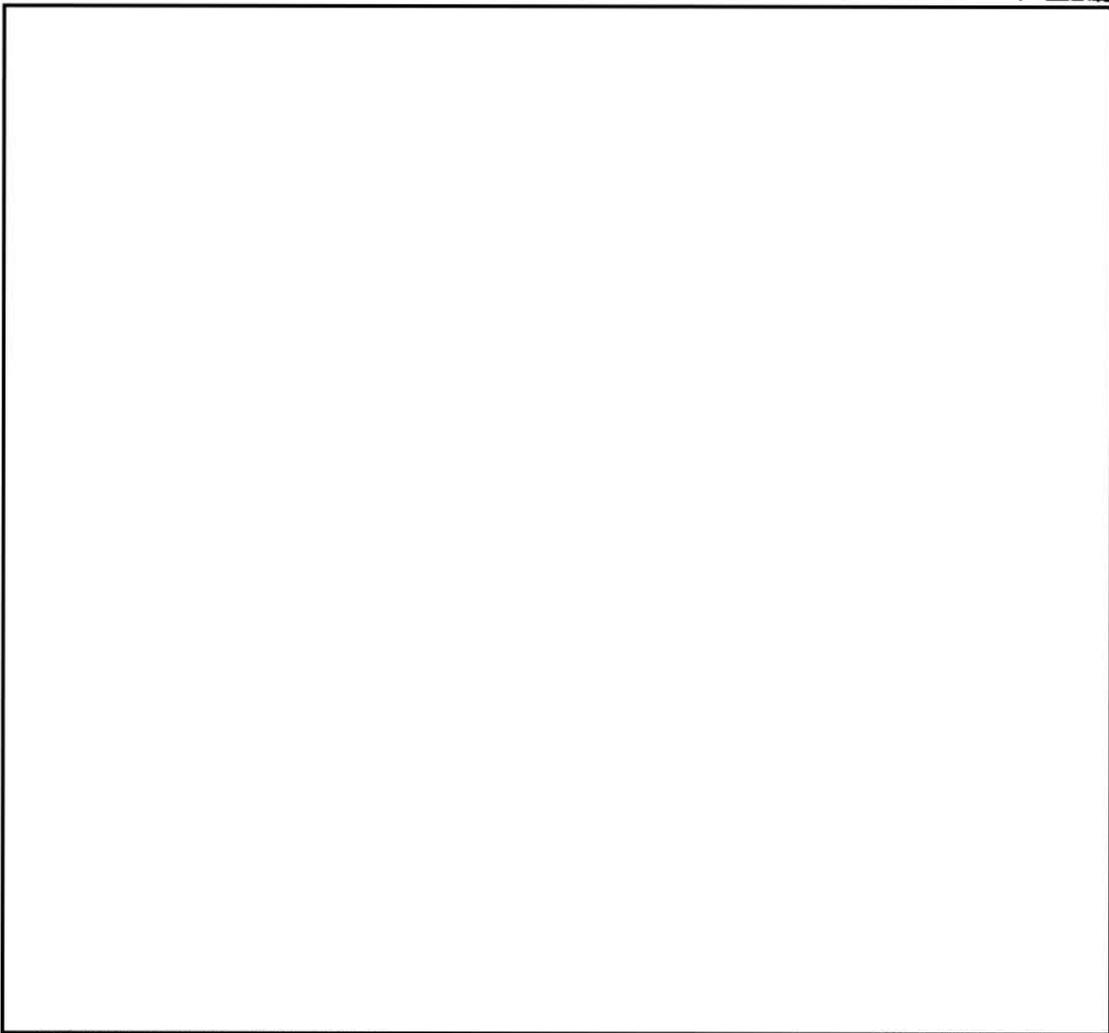
SA [Redacted]  
Squad CY1  
Seattle Field Office

[Redacted] (Fax)  
[Redacted]

UNCLASSIFIED

UNCLASSIFIED

From:  
To:  
Cc:



b6 -4  
b7C -4

Sent: Tuesday, June 12, 2007 7:34 AM  
Subject: B O M B S !

Hello Timberline staff, students, and whoever else is reading this. Today is Tuesday, June 12, 2007 and guess what. There are 3 bombs in the school. I guess guarding it and locking it down doesn't really help. Because they are being sneaked in by backpacks. One is hidden in a bush or some tree or somewhere, I'M not specifying, one of in a bag in some classroom. And one could be anywhere.

I hope everyone keeps their arms and legs because it would be very hard to explain to a parent how you let them get blown up.

The bombs will go off at exactly 10:10 AM. I hope everyone gets out in time!

Visit my myspace - <http://www.myspace.com/timberlinebombinfo> [over 3100 profile views in 3 days, 150+ friends and counting :-)]



# FBI FACSIMILE COVER SHEET

### PRECEDENCE

- Immediate
- Priority
- Routine

### CLASSIFICATION

- Top Secret
- Secret
- Confidential
- Sensitive
- Unclassified

Time Transmitted: \_\_\_\_\_

Sender's Initials: [Redacted]

Number of Pages: 12  
(including cover sheet)

b6 -1  
b7C -1

To: CIRG/NCAC Date: 6/8/07

Facsimile Number: [Redacted]

Attn: SSA [Redacted]

From: Seattle  
Name of Office

Subject: Timberline High School  
Bomb Threats

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

Originator's Name: SSA [Redacted] Telephone: [Redacted]

b6 -1  
b7C -1

Originator's Facsimile Number: [Redacted]

Approved: \_\_\_\_\_

Brief Description of Communication Faxed: copies of email threats

### WARNING

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



07-3955

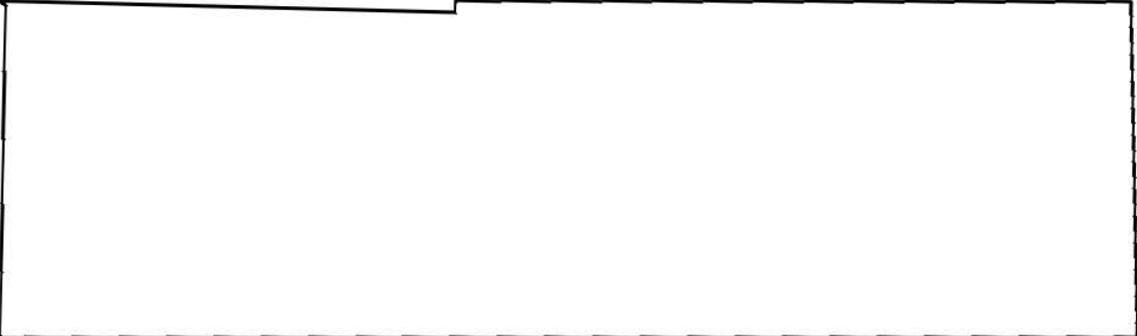


From:  
To:  
Cc:



Sent: Sun 6/3/2007 8:55 PM

b6 -4,6  
b7C -4,



b6 -4  
b7C -

Subject: Read Please  
Attachments:

I will be blowing up your school Monday, June 4, 2007. 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 starting at 9:15 AM. The bombs are in secret hiding places throughout the building I have specified.

Have fun.

-Your Mom

Oh and ps. The email server for your district will be offline starting at 8:45 am.



From: [Redacted]  
Sent: Tuesday, June 05, 2007 7:33 AM  
To: [Redacted]  
Subject: Read this or die.

b6 -4,5,  
b7C -4,5

Now that the school is scared from yesturdays fake bomb threat it's now time to get serious. There are actually 5 bombs planted throughout the school. One in a gym locker room, the girls. It's in a locker hidden under a pile of clothes. The other four I will only say the general location. One in the Language Hall, One in the math hall, One underneath a portable taped with strong ducttape. This bomb will go off if any vibrations are felt. And the last one, Is in a locker. It is enclosed in a soundproof package, and litteraly undetectable. I have used a variety of chemicals to make the bombs. They are all different kinds.

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

Good luck.

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

PS - FREE PARIS HILTON!

[Redacted]

[Redacted]

From: [Redacted]

Sent: Tuesday, June 05, 2007 5:04 PM

To: [Redacted]

Subject: FW: Bomb Threat Email. Should you open it? You better if you want to live nigga's!

b6 -  
b7C -

[Redacted] Here is the first one that came in and I will send the next one after this. Thanks [Redacted]

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

From: [Redacted]

Sent: Tuesday, June 05, 2007 4:33 PM

To: [Redacted]

Cc:

[Redacted]

b6 -6  
b7C -

b6 -4  
b7C -

Subject: Bomb Threat Email. Should you open it? You better if you want to live nigga's!

Hello Again. Seeing as how you're too stupid to trace the email back lets get serious. There are 6 bombs. One in a locker in the math hall, and the rest are scatted around the portables, commons, kitchen, etc. They will go off at any time between 10:45AM and 11:15AM.

Seriously, you are not going to catch me. So just give up.

Maybe you should hire Bill Gates to tell you that it is coming from Italy. HAHAHA Oh wait I already told you that. So stop pretending to be "tracing it" because I have already told you it's coming from Italy. That is where any trace will stop so just stop trying. Oh and this email will be behind a proxy behind the Italy server.

**Shoutouts:**

- [Redacted] For being myself ;-)
- [Redacted] For always being a self centered little bitchy ass fat woman. Go die. :-)
- [Redacted] for being a cool science teacher
- [Redacted] - For getting me fit
- [Redacted] - For being the best teacher ever at Timberline. I love you!

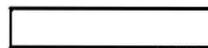
b6 -4,6  
b7C -4,6

Isn't it funny how most people beleive this theory about if I was really doing it I wouldn't put my name? Or is that just what I want you to think?

-----  
Peace Homies!

JUN-08-2007 10:01

FBI SEATTLE SQUAD 8



P.03

Page 2 of 2

b6 -1  
b7C -1

Message

PS - One of the bombs is not "inside" the school, but it could be in a bush, tree, roof, underground or anywhere.

PPS - The Model United Nations is SHIT!

This time I have chosen a random teacher to be the original reciever of this email.

JUN-05-2007 10:01  
message

FBI SEATTLE SQUAD 8

[redacted] P.04

b6 -1  
b7C -1

[redacted]

b6 -4  
b7C -4

From: [redacted]  
Sent: Tuesday, June 05, 2007 5:04 PM  
To: [redacted]  
Subject: FW: MAIL DELIVERY DELAYED

Here is the second one. [redacted]  
-----Original Message-----

b6 -6  
b7C -6

From: [redacted]  
Sent: Tuesday, June 05, 2007 4:36 PM  
To: [redacted]  
Cc: [redacted]

[redacted]

b6 -4  
b7C -4

Subject: MAIL DELIVERY DELAYED

This message from gmail has been delayed 2 days. Please ignore these messages. And any messages sent before this.

JUN-08-2007 10:01

FBI SEATTLE SQUAD 8

[REDACTED]

P.05

b6 -1  
b7C -1

[REDACTED]

b6 -4,5,6  
b7C -4,5,6

**From:** [REDACTED]  
**Sent:** Wednesday, June 06, 2007 9:03 AM  
**To:** [REDACTED]  
**Subject:** Dear Mr. Principle

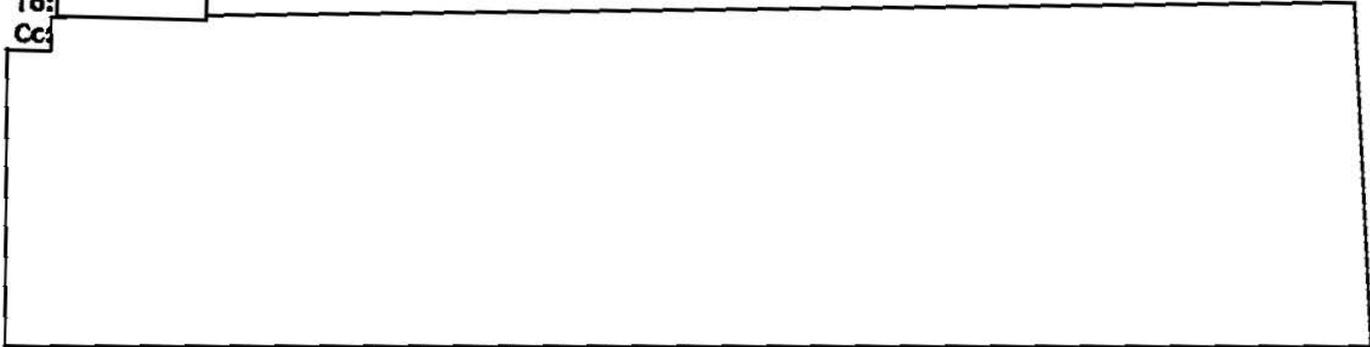
ENJOY YOUR LIFE ENDING.



From: [Redacted]  
Sent: Wednesday, June 06, 2007 9:07 AM  
To: [Redacted]  
Subject: FW: ooo Should you read this. It could be a bomb threat!

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

From: [Redacted]  
Sent: Wednesday, June 06, 2007 9:03 AM  
To: [Redacted]  
Cc: [Redacted]



Subject: ooo Should you read this. It could be a bomb threat!

Well hello Timberline, today is June 06, 2007 and I'M just emailing you to say that the school will blow today. And that's final! There are 2 bombs this time (I ran short on money to buy things at the home depot). They will go off at exactly 10:45:00 AM. One is located on a portable. And the other is somewhere else.

Keep trying to "trace" this email. The only thing you will be able to track is that it came from Italy. There is no other information that leads it back to the United States in any way so get over it.

You should hire Bill Gates to track it for you. HAHAAHAHA. He will just tell you that it came from over seas, so if you have close relations with the POPE you might get some information. But other than that, have fun looking for Italy. :-)

Also, stop advising teachers to not show this email to classmates. Everyone would be amused by this email and I might stop if you do.

Funny how I can trick you all into thinking that I included my name to show that it isn't me, because who the hell would put their name? Or is that just what I want you to think.

And yet again, this email was sent from over seas to a newly made email account that has already been deleted of all information by the time you read this email. Get your ass on a plane to Italy if you want it to stop.

Some Random Shoutouts:

[Redacted] - For being so cool, I'M just so cool.

STUDENT STORE'S SALE IS A RIP OFF. SMOOTHIES SHOULD BE \$1.00! AND MY CUP OF

JUN-06-2007 18:02

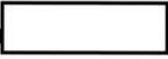
FBI SEATTLE SQUAD 8



P.07

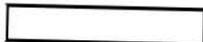
b6 -1  
b7C -1

NOODLES I LOVE AND BUY EVERY DAMN DAY SHOULD BE FREE!

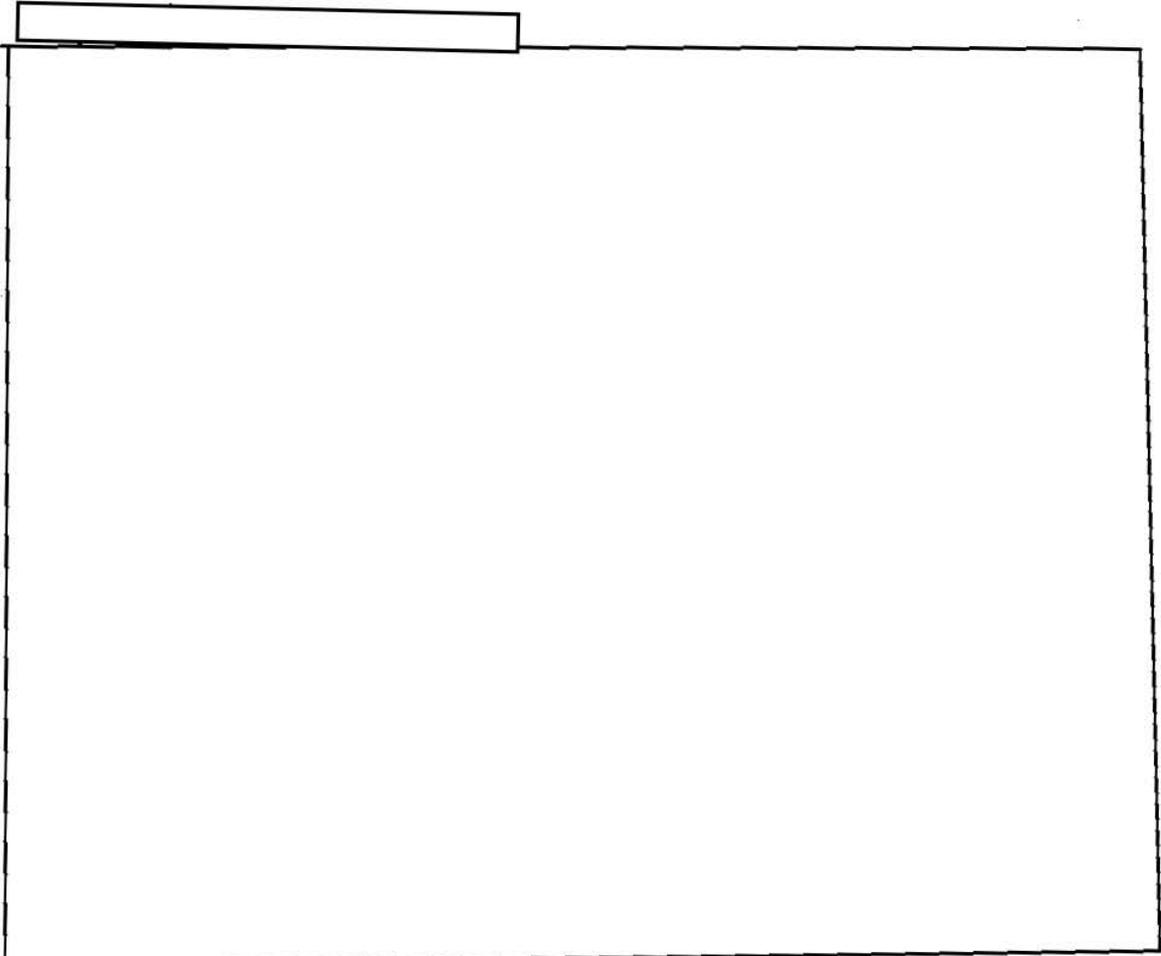
S - I am in  advisory. Or am i.

b6 -4  
b7C -4

-----  
FREE PARIS!



**From:**  
**To:**  
**Cc:**



b6 -6  
b7C -

b6 -4  
b7C -4

**Sent:** Thursday, June 07, 2007 7:20 AM  
**Subject:** Oh noes! Anotha bomba threat! Whatcha gonna dooo!

Hello Timberline teachers & staff. Today is June 7, 2007. I think you know what this email is going to say. There are 3 bombs planted in the school and they're all different kinds. I have premade these weeks in advance and tested the timers to make sure they work to the exact millisecond. Locking the doors was a good plan, but too late.

One bomb is located in a locker room. In a locker, under a pile of gym clothes of mine. I won't say which locker room but I think you get the drift. There is one located on the roof, attached to a certain position on the ceiling so the roof caves in, this is a high explosive bomb and should be handled with care. Finally, the last bomb could be in any room, area, anywhere!. Lets hope it's not "YOUR" classroom!

They will go off anytime from 8:30AM to 9:00 AM.



# FBI FACSIMILE COVER SHEET

### PRECEDENCE

- Immediate
- Priority
- Routine

### CLASSIFICATION

- Top Secret
- Secret
- Confidential
- Sensitive
- Unclassified

Time Transmitted: \_\_\_\_\_  
 Sender's Initials: \_\_\_\_\_  
 Number of Pages: 15  
 (including cover sheet)

To: CIRG/NCAVC  
Name of Office

Date: 6/14/2007

Facsimile Number: [Redacted]

Attn: SSA  
Name Room Telephone

From: Seattle  
Name of Office

Subject: Timberline High School

b6 -1  
b7C -1

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

Originator's Name: SSA [Redacted] Telephone: [Redacted]

Originator's Facsimile Number: [Redacted]

Approved: \_\_\_\_\_

b7E -2

Brief Description of Communication Faxed: Chat logs, [Redacted]  
Subject's response, Press release

### WARNING

Information attached to the cover sheet is U.S. Government Property. If you are not the intended recipient of this information, disclosure, reproduction, distribution, or use of this information is prohibited (18.U.S.C. § 641). Please notify the sender if you have received this communication in error. RCFR 129



Shaping our community together

CITY OF LACEY

POST OFFICE BOX 3400 LACEY, WA 98509-3400

- CITY COUNCIL
- VIRGIL S. CLARKSON  
*Mayor*
- NANCY J. PETERSON  
*Deputy Mayor*
- ANN BURGMAN
- JOHN DARBY
- MARY DEAN
- THOMAS L. NELSON
- GRAEME SACKRISON

CITY MANAGER  
GREG J. CUOIO

Press Release

Date: June 14, 2007  
 Time: 0230 AM  
 From: Commander John Suessman  
 Re: Bomb Threat at Timberline High School Case # 2007-3989

The Lacey Police Department has made an arrest in the string of bomb threats directed at Timberline High School. A 10th grade male student from Timberline High School was taken into custody at approximately 2 A.M. this date. He was arrested at his home pursuant to a search warrant. Computer equipment was also seized. The arrest was made without incident. No explosives were found at the residence. The subject is believed to be responsible for e-mailing seven bomb threats to the school from June 4<sup>th</sup> through June 13<sup>th</sup>, 2007. The suspects name is being withheld because he is a juvenile. He is being booked at Juvenile Detention for, (7) counts of Threats to Bomb a School which is a Class B felony. Additional felony charges in this case are Identity Theft, and Felony Harassment (Threats to Kill).

RCW 9.61.160

Threats to bomb or injure property – Penalty.

(1) It shall be unlawful for any person to threaten to bomb or otherwise injure any public or private school building, any place of worship or public assembly, any governmental property, or any other building, common carrier, or structure, or any place used for human occupancy; or to communicate or repeat any information concerning such a threatened bombing or injury, knowing such information to be false and with intent to alarm the person or persons to whom the information is communicated or repeated.

(2) It shall not be a defense to any prosecution under this section that the threatened bombing or injury was a hoax.

(3) A violation of this section is a class B felony punishable according to chapter 9A.20 RCW.

The Lacey Police Department appreciates the assistance they have received from North Thurston Public Schools, the Staff and Students at Timberline High School, the Washington State Patrol, Thurston County Prosecutors Office, FBI, Assistant US Attorney, countless citizens, and parents that became involved by providing tips and information which was helpful during this investigation.

Commander Suessman will be available after 9 A.M. 360-459-4333



Received: by 10.114.60.19 with SMTP id i19mr6660495waa.1181658876181; Tue, 12 Jun 2007 07:34:36 -0700 (PDT)

Received: by 10.141.4.21 with HTTP; Tue, 12 Jun 2007 07:34:36 -0700 (PDT)

Message-ID: <5feb9a6f0706120734i219b59a8id604ca58fa3df74d@mail.gmail.com>

Date: Tue, 12 Jun 2007 16:34:36 +0200

From: [Redacted]

To: [Redacted]

Subject: B O M B S I

Cc: [Redacted]

b6 -4  
b7C -4

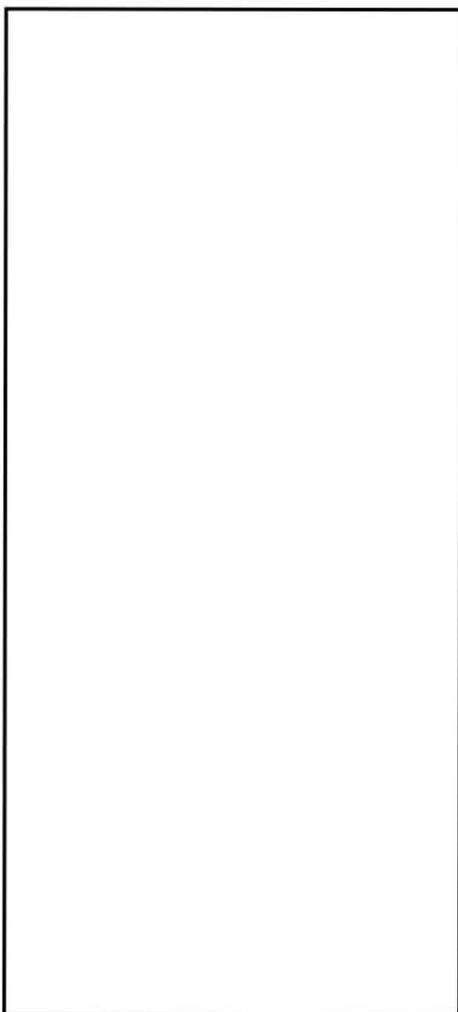
JUN-14-2007 12:46

FBI SEATTLE SQUAD 8



P.05

b6 -1  
b7C -1

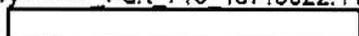


b6 -4  
b7C -4

MIME-Version: 1.0

Content-Type: multipart/alternative;

boundary="-----Part\_718\_16713022.1181858876156"

Return-Path: 

X-OriginalArrivalTime: 12 Jun 2007 14:34:37.0632 (UTC) FILETIME=[CDB6AC00:01C7ACFE]

Visit the email website - <http://bombemails.hyperphp.com>

Bomb email website also has some pictures of what [Redacted] does in his spare time.

b6 -4

b7C -4

Shoutouts By Request:

[Redacted] is #1! WOOO!  
Did [Redacted] lose weight?  
Dude do these all year

Published June 14, 2007

### **Police arrest teen suspected of threatening Lacey high school**

Police have arrested a teen suspected of making almost daily bomb threats that forced evacuations at Timberline High School in Lacey.

Police say the sophomore from the school was arrested about two this morning at his home in Lacey. Officers seized his computer. They did not find any explosives.

The boy is held in juvenile detention facing seven counts of threatening to bomb a school.

After a Tuesday night meeting with police, school officials and parents, a 17-hundred dollar reward had been offered to catch the person responsible for making a string of e-mail threats since May 30th.

(KIRO-TV)