U.S. Department of Justice

Federal Bureau of Investigation
Washington, D.C. 20535

October 26, 2015

MR. JOHN GREENEWALD, JR.
[redacted]

FOIPA Request No.: 1302877-000
Subject: FBI INVESTIGATING AND RESEARCHING THE TOR WEB BROWSER

Dear Mr. Greenewald:

Records responsive to your request were previously processed under the provisions of the Freedom of Information Act (FOIA). Enclosed is one CD containing 21 pages of previously processed documents and a copy of the Explanation of Exemptions. These documents represent the first interim release of information responsive to your FOIA request. This release is being provided to you at no charge.

Additional responsive material has been reviewed pursuant to Title 5, U.S. Code, Section 552, and this material is being withheld in its entirety by the FBI pursuant to subsection (b)(7)(A).
5 U.S.C. § 552(b)(7)(A) exempts from disclosure:

> records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information ... could reasonably be expected to interfere with enforcement proceedings...

The records responsive to your request are law enforcement records; there is a pending or prospective law enforcement proceeding relevant to these responsive records, and release of the information in these responsive records could reasonably be expected to interfere with enforcement proceedings. For a further explanation of this exemption, see the enclosed Explanation of Exemptions.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S. C. § 552(c) (2006 & Supp. IV (2010). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

For questions regarding our determinations, visit the www.fbi.gov/foia website under “Contact Us.” The FOIPA Request Number listed above has been assigned to your request. Please use this number in all correspondence concerning your request. Your patience is appreciated.

You may file an appeal by writing to the Director, Office of Information Policy (OIP), U.S. Department of Justice, 1425 New York Ave., NW, Suite 11050, Washington, D.C. 20530-0001, or you may submit an appeal through OIP's eFOIA portal at http://www.justice.gov/oip/efoia-portal.html. Your appeal must be received by OIP within sixty (60) days from the date of this letter in order to be considered timely. The envelope and the letter should be clearly marked "Freedom of Information Appeal." Please cite the FOIPA Request Number assigned to your request so that it may be identified easily.

Sincerely,

David M. Hardy
Section Chief,
Record/Information
  Dissemination Section
Records Management Division

Enclosures (2)

EXPLANATION OF EXEMPTIONS

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

(b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;

(b)(2) related solely to the internal personnel rules and practices of an agency;

(b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

(b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(b)(9) geological and geophysical information and data, including maps, concerning wells.

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

(d)(5) information compiled in reasonable anticipation of a civil action proceeding;

(j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;

(k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;

(k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;

(k)(4) required by statute to be maintained and used solely as statistical records;

(k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service he release of which would compromise the testing or examination process;

(k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

[redacted] (CTD) (FBI)

From: [redacted] (CTD)(FBI)
Sent: Thursday, July 18, 2013 2:11 PM
To: [redacted]
Subject: Onion Pi White Paper --- ~~SECRET//NOFORN~~ [redacted] (S)

SentinelCaseId: NON-RECORD

b1
b3
b6
b7C
b7E

```
Classification: ~~SECRET//NOFORN~~ [redacted] (S)

~~Classified By: F12M89K55~~
~~Derived From: FBI NSISC-20090615~~
~~Declassify On: 20381231~~
=====================================================
```

All:

Here is my Onion Pi white paper. Please let me know if you have any questions, feedback, suggestions, etc. Thanks,

[redacted]

b1
b3
b6
b7C
b7E

SigDev Onion Pi.docx

[redacted]

```
==============================[redacted]=
Classification: ~~SECRET//NOFOR~~[redacted] (S)
```

Counterterrorism Division
Electronic Communications Analysis Unit (ECAU)
16 July 2013

b1
b3
b7E

Onion Pi

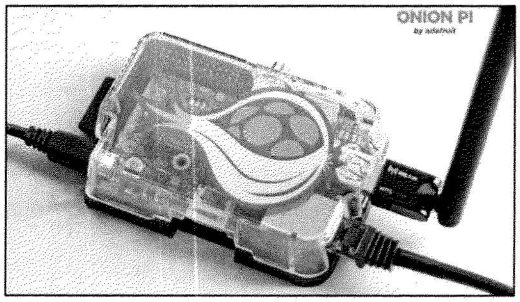
Summary: ~~(S//NF)~~ As of June 2013, Adafruit Industries developed a portable proxy device integrating the Tor network with a Raspberry Pi microcomputer, according to open-source reporting. The device is designed to automatically route all internet traffic through the Tor network, which applies layers of encryption to prevent snooping and hops a series of servers to obscure location. [redacted] (S)

Details: ~~(S//NF)~~ Technically savvy FBI subjects have indicated an awareness of this newly-created device and an eagerness to test its effectiveness [redacted] (S)

Adafruit Industries
(U) According to its website, Adafruit Industries, founded in 2005 by an MIT engineer, is focused on designing electronic devices for all ages and skill levels, as well as creating an online resource for learning about electronics.
(U) Source: Adafruit.com.

Raspberry Pi
(U) According to its website, Raspberry Pi is a cheap ($35) single-board minicomputer designed to teach children the basics of programming. It incorporates USB, HDMI, Ethernet, and SD card ports.
(U) Source: raspberrypi.org.

Significance: ~~(S//NF)~~ While the Tor network is a well-known operational security tool among extremists, this is the first commercially available device that applies Tor to an entire wireless hotspot. Starting in 2010, Tor developers launched their own similar project called Onionbox, with a targeted cost of around $75, but open-source research indicates that the router is still in beta-testing and has yet to be marketed for sale.[4] [redacted]



b1
b3
b7E

b1
b3
b6
b7C
b7E

[redacted] While the Onion Pi improves the ease and portability of accessing the Tor network, it is too early to tell whether extremist actors will widely adopt the device to conceal nefarious activity.

(U) ECAU POC: IA [redacted]

[redacted] (S)

[1] (U) Internet site; Adafruit.com; "Onion Pi;" 17 June 2013; UNCLASSIFIED; UNCLASSIFIED; (U) http://learn.adafruit.com/onion-pi/overview

[redacted] (S)

(U) Internet site; Torproject.org; "Status/Progress of TorRouter?;" 29 March 2012; UNCLASSIFIED; UNCLASSIFIED; (U) https://lists.torproject.org/pipermail/tor-talk/2012-march/023799.html

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1227613-0

Total Deleted Page(s) = 1
Page 13 ~ b1; b3;

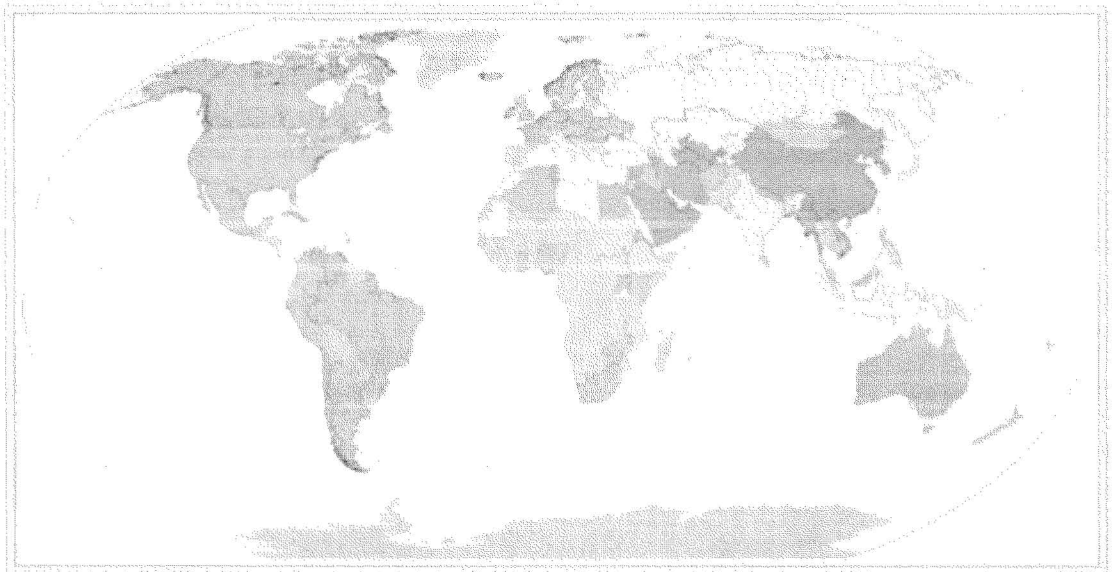
```
XXXXXXXXXXXXXXXXXXXXXXXX
X   Deleted Page(s)    X
X   No Duplication Fee X
X   For this Page      X
XXXXXXXXXXXXXXXXXXXXXXXX
```

Federal Bureau of Investigation

Proxy Servers & Tor

Good Intentions…

- **Anonymity to security-conscious, whistle blowers, etc.**
- **Circumvent state-wide internet censorship**



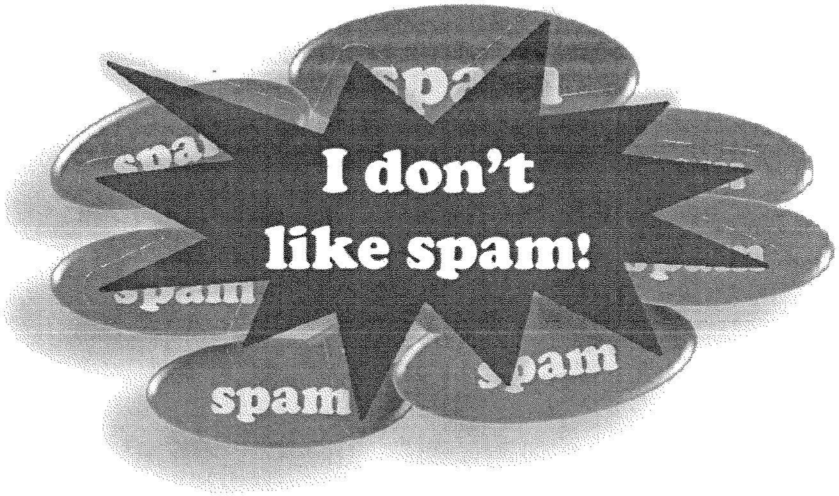
Internet censorship by country

▨ Persuasive censorship
▨ Substantial censorship
□ Selective censorship
▨ Under surveillance
▨ No evidence of censorship
▨ Not classified / No data

Internet censorship in Tunisia, Egypt, and Libya has changed since the Arab Spring of 2011.

Abusive/Criminal Use of Proxy Servers

- Proxies have been used to conduct:
  - Crimes against children
  - Exchange illegal documents and files (e.g., identity theft)
  - Network intrusions
  - Spamming



Proxy Use by Extremists

- **Posts Warn About FBI Surveillance of Jihadist Websites (U//~~FOUO~~)**
  - On 6 August 2004, "abdalrhman24" on the *Arab Dialogue Forum* and "iraq123" on the *Al-Anbar Network*forum posted identical messages asking participants to be careful of "FBI-surveilled websites."
  - The posts advised participants to use a proxy to avoid being detected and traced.

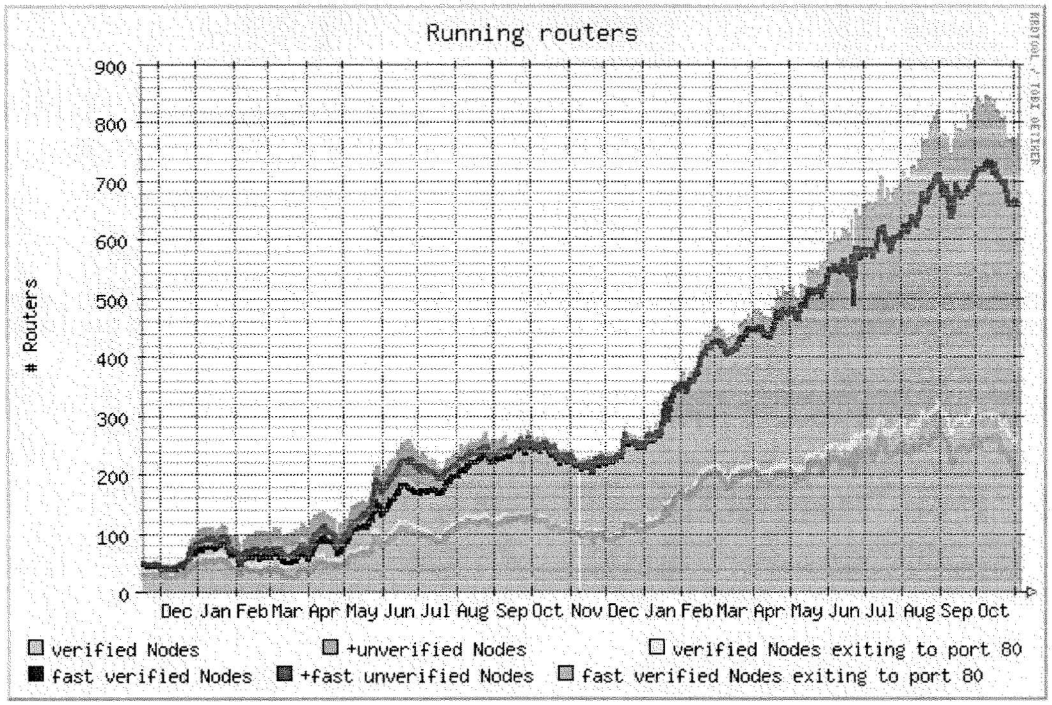
Proxy Use by Extremists

- **Poster Analyzes Jihadist Websites, Advises Participants (U//~~FOUO~~)**
  - October 10, 2005: … for the internationally renowned al-Hisbah forum, … Al-Hammam al-Battar of the *Islamic Renewal Organization's forum* stated: "I repeat to the members not to enter this site without a proxy, and to the administration of the website I urge you to cancel the feature of storing IP addresses because of the danger it poses to the supporters of jihad."

Pros and Cons of Tor

- Pros
  - Free service
  - Encrypted traffic (inside the Tor network)
  - Offers very good anonymity if properly configured
- Cons
  - Set-up can be difficult
  - Not ideal for certain applications (e.g., videos)
  - Anonymity but not data security
  - Can be slow

Growth of Tor



Growth of Tor nodes from December 2004 to October 2006

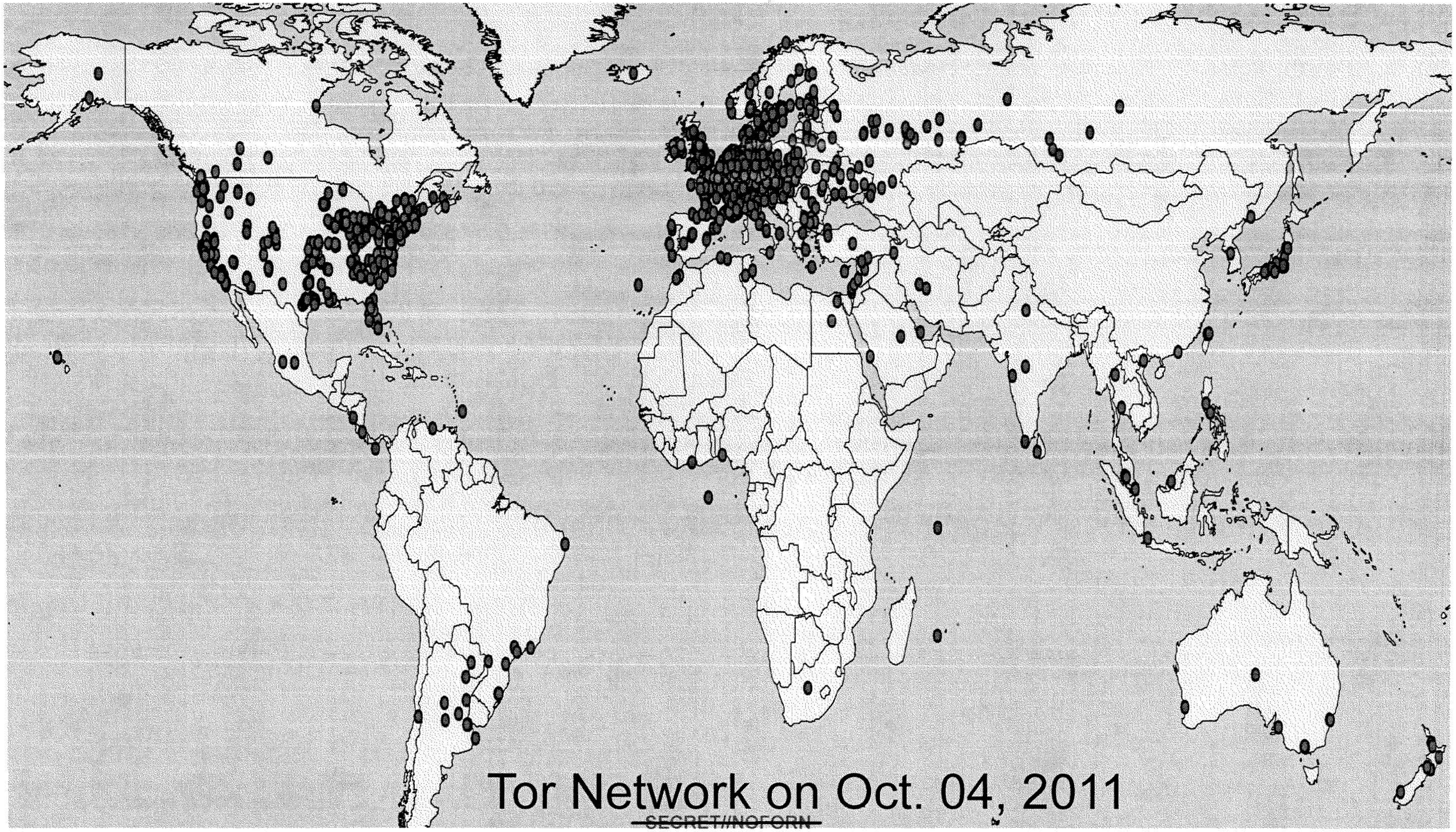
The Onion Router

[redacted]

b7E

~~SECRET//NOFORN~~

The Onion Router



Tor Network on Oct. 04, 2011

~~SECRET//NOFORN~~

Tor-Related Products

b7E

- [redacted]

- [redacted]

Tor's Hidden Services

- Hidden services – offer the possibility of various Web services within the Tor network
  - [redacted]

b7E

Where are they?

Why we might not be seeing increased Tor use by bad guys

b7E

- The Human Factor
  - Forgetfulness
  - Lazy
  - Tor is slow
  - In-depth, detailed instructions typically are in English
  - Somewhat sophisticated
- The Technical Aspect

[redacted]

Until Next time

Questions?
Comments?

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1227613-0

Total Deleted Page(s) = 3
Page 3 ~ Duplicate;
Page 4 ~ Duplicate;
Page 5 ~ Duplicate;

```
XXXXXXXXXXXXXXXXXXXXXXXX
X   Deleted Page(s)    X
X   No Duplication Fee X
X   For this Page      X
XXXXXXXXXXXXXXXXXXXXXXXX
```

From: [redacted] (DI) (FBI)
Sent: Monday, November 05, 2012 3:44 PM
To: [redacted] (DI) (FBI); [redacted] (DI) (FBI)
Subject: RE: Tor --- UNCLASSIFIED//~~FOUO~~

b6
b7C

Classification: UNCLASSIFIED//~~FOUO~~
===

Thanks very much [redacted]

From: [redacted] (DI) (FBI)
Sent: Monday, November 05, 2012 3:35 PM
To: [redacted] (DI) (FBI)
Subject: FW: Tor --- UNCLASSIFIED//~~FOUO~~

Classification: UNCLASSIFIED//~~FOUO~~
===

FYI

From: [redacted] (DI) (FBI)
Sent: Monday, November 05, 2012 11:25 AM
To: [redacted] (DI) (FBI); [redacted] (DI) (FBI)
Subject: Tor --- UNCLASSIFIED//~~FOUO~~

b6
b7C
b7E

Classification: UNCLASSIFIED//~~FOUO~~
===

[redacted] –

Per our talk in the car on Friday about Tor, I've reached out to a couple people and compiled the below to be passed up to [redacted]

IA [redacted] (Criminal Proceeds Laundering Unit, Criminal Division) and I have been working with IA [redacted] (Violent Crimes/Crimes Against Children Intelligence Unit, Criminal Division) to identify hidden services [redacted] The information below comes from IA [redacted] efforts working the Tor issue.

- [redacted] require different investigative approaches.
  - [redacted]

- [redacted]

b6
b7C
b7E

- The most abundant crimes occurring on Tor hidden services are: sexual exploitation of children, money laundering, trafficking of weapons and drugs, and computer intrusions, however many other violations have been observed on Tor.
- [redacted]
- Tor is spelled "Tor" rather than "TOR." A section of Tor's Web site explains this: https://www.torproject.org/docs/faq.

IA [redacted] also provided the write-up below that explains some more about Hidden Services and Tor.
<< File: Identifying Tor Hidden Services.docx >>
IA [redacted]
CybIS/Domestic Threats Cyber Intelligence Unit
[redacted]
BB [redacted]
[redacted]

```
============================================================
Classification: UNCLASSIFIED//FOUO

============================================================
Classification: UNCLASSIFIED//FOUO

============================================================
Classification: UNCLASSIFIED//FOUO
```

About Tor

Tor is an open-source circuit-based distributed overlay network designed to obfuscate the physical and logical location of servers hosting online services and people's Internet activity. The physical and logical location of servers hosting online services are able to be hidden via Tor's hidden service protocol. Web sites using the hidden service protocol use a nondescript 16-character URL (determined by its public key) followed by the pseudo-domain ".onion" (*i.e.* [redacted] The URLs of Tor hidden service Web sites must be advertized for others to know its existence. URLs of Tor hidden services are generally advertized via communication between users or postings on other Tor hidden service Web sites. b7E

To access Tor hidden service Web sites, users must use a Tor-connected Web browser or a third-party service capable of acting as an intermediary to Tor (i.e. [redacted] Third-party services such as [redacted] allow users to access Tor hidden service Web sites using a non Tor-enabled browser by going through a Tor-connected proxy server operated by the third party service [redacted] works by [redacted] [redacted]

[redacted] (S) b1 b3

~~SECRET~~

b1
b3

(S)

[redacted]

Sample of Criminal Content on Hidden Services

[redacted]

b7E

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1227613-0

Total Deleted Page(s) = 2
Page 3 ~ b1; b3; b7A; b7E;
Page 4 ~ b1; b3; b7A;

```
XXXXXXXXXXXXXXXXXXXXXXXX
X   Deleted Page(s)    X
X   No Duplication Fee X
X   For this Page      X
XXXXXXXXXXXXXXXXXXXXXXXX
```

Identification of Tor Hidden Services

About Tor

Tor is an open-source circuit-based distributed overlay network designed to obfuscate the physical and logical location of servers hosting online services and people's Internet activity. The physical and logical location of servers hosting online services are able to be hidden via Tor's hidden service protocol. Web sites using the hidden service protocol use a nondescript 16-character URL (determined by its public key) followed by the pseudo-domain ".onion" (*i.e.* [redacted] The URLs of Tor hidden service Web sites must be advertized for others to know its existence. URLs of Tor hidden services are generally advertized via communication between users or postings on other Tor hidden service Web sites. b7E

To access Tor hidden service Web sites, users must use a Tor-connected Web browser or a third-party service capable of acting as an intermediary to Tor (i.e. [redacted]. Third-party services such as [redacted] allow users to access Tor hidden service Web sites using a non Tor-enabled browser by going through a Tor-connected proxy server operated by the third party service. [redacted] works by [redacted]

[redacted]

b1
b3
b7A