



# governmentattic.org

*"Rummaging in the government's attic"*

Description of document: Records regarding retrieval and sanitizing of US Patent and Trademark Office (USPTO) and Department of Commerce computers that staff used to download Wikileaks documents, 2010-2011

Requested date: 11-December-2010

Released date: 30-September-2011

Posted date: 24-October-2011

Date/date range of document: 01-December-2010 – 05-January-2011\*

Source of document: Freedom of Information Act Request  
Department of Commerce  
Departmental Freedom of Information Act Officer  
Office of Management and Organization  
1401 Constitution Ave. NW  
Washington, D.C. 20230  
Email: [EFOIA@doc.gov](mailto:EFOIA@doc.gov)

Note: \*Some documents updated

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



**UNITED STATES DEPARTMENT OF COMMERCE**  
**Chief Financial Officer**  
**Assistant Secretary for Administration**  
Washington, D.C. 20230

September 30, 2011

RE: Freedom of Information Act Request CRRIF 11-091

This is in final response to your Freedom of Information Act Request dated, December 11, 2010 for a copy of any records including emails concerning the retrieval and sanitizing of USPTO or Commerce Department computers that staff have used to download Wikileaks documents.

We are enclosing responsive documents. Portions of ten documents are being withheld pursuant to 5 U.S.C. § 552 (b)(2), which protects records related solely to the internal personnel rules and practices of an agency. Portions of six documents are being withheld pursuant to 5 U.S.C. § 552 (b)(2), which protects records related solely to the internal personnel rules and practices of an agency with portions that are non-responsive to your request being blacked out and marked "NR". Portions of three documents are being withheld pursuant to 5 U.S.C. § 552 (b)(2), which protects records related solely to the internal personnel rules and (b)(6), which protects personal privacy information and "NR", which is the non-responsive information and is blacked out and marked appropriately. Portions of two documents contain information that is non-responsive to your request and these portions have been marked accordingly. Portions of one document is being withheld pursuant to 5 U.S.C. § 552 (b)(5), which protects internal Federal government documents which are both pre-decisional and deliberative. Portions of two documents are being withheld pursuant to 5 U.S.C. § 552 (b)(5), which protects pre-decisional and deliberative information, (b)(6), which protects personal privacy and portions are non-responsive to your request and this information has been marked appropriately. Portions of two documents are being withheld pursuant to 5 U.S.C. § 552 (b)(5) and (b)(6), which protects pre-decisional and deliberative information and personal privacy information. Portions of two documents are being withheld pursuant to 5 U.S.C. § 552 (b)(5) and (b)(6), which protects information that is attorney-client and personal privacy information. Portions of ten documents are being withheld pursuant to 5 U.S.C. § 552 (b)(6) & NR, which protects personal privacy and non-responsive information and this information has been marked accordingly. Portions of 68 documents are being withheld pursuant to 5 U.S.C. § 552 (b)(6), which protects personal privacy information. Portions of 67 documents are being withheld pursuant to 5 U.S.C. § 552 (b)(6) and (b)(2), which protects personal privacy information and information related solely to the internal personnel rules and practices of an agency. Portions of ten documents are being withheld pursuant to (b)(6) and (b)(6)(b)(7)( ), which protects personal privacy information and information compiled for law enforcement purposes. Portions of three documents are being withheld pursuant to 5 U.S.C. § 552 (b)(2), (b)(6) and (b)(6)(b)(7)( c). Seven documents in their entirety are being withheld pursuant to 5 U.S.C. § 552 (b)(5), which protects 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. The privileges being used are the attorney-client privilege and the attorney work-product privilege. Fourteen documents are being withheld in their entirety pursuant to 5 U.S.C. § 552 (b)(5), the privileges being used are the attorney-client privilege and the deliberative process

privilege. One document in its entirety is being withheld pursuant to 5 U.S.C. § 552 (b)(5) and the privilege being used is the deliberative process privilege. Six documents are being withheld in their entirety pursuant to 5 U.S.C. § 552 (b)(5) and the privileges being used are the deliberative process privilege, the attorney client privilege and the attorney work-product privilege.

Portions of two documents originating at the U.S. Department of Homeland Security (DHS) have been sent to DHS for disclosure review and determination and direct response to you. If you have any questions regarding these documents, you may contact the Deputy Chief FOIA Officer, Ms. Catherine Papoi at (866) 431-0486 or (703) 235-0790 or via email at [foia@dhs.gov](mailto:foia@dhs.gov).

You have the right to appeal this partial denial of the FOIA request. An appeal must be received within 30 calendar days of the date of this letter by the Assistant General Counsel for Administration (Office), Room 5898-C, U.S. Department of Commerce, 14<sup>th</sup> and Constitution Avenue, N.W. Washington, D.C. 20230. Your appeal may also be sent by e-mail to [FOIAAppeals@doc.gov](mailto:FOIAAppeals@doc.gov) or by facsimile (fax) to 202-482-2552. The appeal must include a copy of the original request, this response to the request and a statement of the reason why withheld records should be made available and why denial of the records was in error. The submission (including e-mail and fax submissions) is not complete without the required attachments. The appeal letter, the envelope, the e-mail subject line, and the fax cover sheet should be clearly marked "Freedom of Information Act Appeal." The e-mail, fax machine, and Office are monitored only on working days during normal business hours (8:30 a.m. to 5:00 p.m., Eastern Time, Monday through Friday). FOIA appeals posted to the e-mail box, fax machine or Office after normal business hours will be deemed received on the next normal business day.

Sincerely,

A handwritten signature in black ink that reads "Brenda Dolan". The signature is fluid and cursive, with the first name "Brenda" being more prominent than the last name "Dolan".

Brenda Dolan  
Departmental FOIA Officer

Enclosures

Release

Rep CC



## Clark, Roger

---

**From:** JACK WARD [JMWARD@bis.doc.gov]  
**Sent:** Wednesday, December 01, 2010 5:33 PM  
**To:** Clark, Roger  
**Subject:** Re: Question

Thanks for the information Roger. I surely appreciate it.

\*\*\*\*\*  
This message was sent from my Blackberry Mobile Device  
\*\*\*\*\*

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

**From:** "Clark, Roger" <RClark@doc.gov>  
**To:** WARD, JACK <JMWARD@bis.doc.gov>

**Sent:** 12/1/2010 5:08:23 PM  
**Subject:** FW: Question

FYI

**From:** Clark, Roger  
**Sent:** Wednesday, December 01, 2010 5:08 PM  
**To:** DeMegret, Andre  
**Subject:** Question

In this hypothetical scenario, the user potentially has U.S. Government classified information on their home PC. As a DOC official, I have no authority over personal PCs. However, as a law enforcement official I'm sure you are aware of the possible consequences of having classified information on a personal machine that is not located in a secure space. I would suggest to this hypothetical user that if they have a security clearance that the hypothetical incident be reported to their servicing security officer and that the hard drive be wiped using a DOD approved tool such as BC-Wipe.

Media sources that are reporting on the incident are viewed as ok as long as the person does not access the source documents whether that be on the actual WikiLeaks site or via a link to another site hosting the documents.

v/r  
Roger Clark  
Senior Advisor  
National & Cyber Security  
Office of the Chief Information Officer  
U.S. Department of Commerce  
Phone: (202) 482-0121  
Email: [rclark@doc.gov](mailto:rclark@doc.gov)<<mailto:rclark@doc.gov>>

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

**From:** ANDRE DEMEGRET [<mailto:ADEMEGRE@bis.doc.gov>]<[\[mailto:ADEMEGRE@bis.doc.gov\]](mailto:[mailto:ADEMEGRE@bis.doc.gov])>

**Sent:** Wednesday, December 01, 2010 2:00 PM

**To:** DOC-CIRT

Subject: Fwd: Guidance regarding WikiLeaks ( -forwarded)

What is the guidance with regard to the hypothetical viewing of these documents on a personal home PC or portable device? Also, what is the guidance with respect to viewing online media sources that may report the contents of the leaked documents in whole or in part or in summary?

## Clark, Roger

---

From: Clark, Roger  
Sent: Wednesday, December 01, 2010 6:02 PM  
To: Ward, Jack  
Subject: Re: Question

Thought the question was interesting considering the source and thought it might help your investigation.

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

From: JACK WARD <[JMWARD@bis.doc.gov](mailto:JMWARD@bis.doc.gov)>  
To: Clark, Roger  
Sent: Wed Dec 01 17:33:26 2010  
Subject: Re: Question

Thanks for the information Roger. I surely appreciate it.

\*\*\*\*\*  
This message was sent from my Blackberry Mobile Device  
\*\*\*\*\*

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

From: "Clark, Roger" <[RClark@doc.gov](mailto:RClark@doc.gov)>  
To: WARD, JACK <[JMWARD@bis.doc.gov](mailto:JMWARD@bis.doc.gov)>

Sent: 12/1/2010 5:08:23 PM  
Subject: FW: Question

FYI

From: Clark, Roger  
Sent: Wednesday, December 01, 2010 5:08 PM  
To: DeMegret, Andre  
Subject: Question

In this hypothetical scenario, the user potentially has U.S. Government classified information on their home PC. As a DOC official, I have no authority over personal PCs. However, as a law enforcement official I'm sure you are aware of the possible consequences of having classified information on a personal machine that is not located in a secure space. I would suggest to this hypothetical user that if they have a security clearance that the hypothetical incident be reported to their servicing security officer and that the hard drive be wiped using a DOD approved tool such as BC-Wipe.

Media sources that are reporting on the incident are viewed as ok as long as the person does not access the source documents whether that be on the actual Wikileaks site or via a link to another site hosting the documents.

v/r

Roger Clark  
Senior Advisor  
National & Cyber Security  
Office of the Chief Information Officer  
U.S. Department of Commerce  
Phone: (202) 482-0121  
Email: [rclark@doc.gov](mailto:rclark@doc.gov)<<mailto:rclark@doc.gov>>

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

From: ANDRE DEMEGRET [<mailto:ADEMEGRE@bis.doc.gov>] <[mailto:\[mailto:ADEMEGRE@bis.doc.gov\]](mailto:[mailto:ADEMEGRE@bis.doc.gov])>

Sent: Wednesday, December 01, 2010 2:00 PM

To: DOC-CIRT

Subject: Fwd: Guidance regarding WikiLeaks ( -forwarded)

What is the guidance with regard to the hypothetical viewing of these documents on a personal home PC or portable device? Also, what is the guidance with respect to viewing online media sources that may report the contents of the leaked documents in whole or in part or in summary?

## Clark, Roger

---

**From:** Clark, Roger  
**Sent:** Wednesday, December 01, 2010 8:37 PM  
**To:** DeMegret, Andre  
**Subject:** Re: Question

No problem glad I was helpful

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

**From:** ANDRE DEMEGRET <[ADEMEGRE@bis.doc.gov](mailto:ADEMEGRE@bis.doc.gov)>  
**To:** Clark, Roger  
**Sent:** Wed Dec 01 20:35:39 2010  
**Subject:** Re: Question

Ok, great, thanks. No need for concern, the question was preventative. An individual on my staff had a college professor suggest the class read the documents. She immediately came to me, and we went to you for guidance.

Thanks again.

Andre.

>>> "Clark, Roger" <[RClark@doc.gov](mailto:RClark@doc.gov)> 12.1.2010 17:07:39 >>>

In this hypothetical scenario, the user potentially has U.S. Government classified information on their home PC. As a DOC official, I have no authority over personal PCs. However, as a law enforcement official I'm sure you are aware of the possible consequences of having classified information on a personal machine that is not located in a secure space. I would suggest to this hypothetical user that if they have a security clearance that the hypothetical incident be reported to their servicing security officer and that the hard drive be wiped using a DOD approved tool such as BC-Wipe.

Media sources that are reporting on the incident are viewed as ok as long as the person does not access the source documents whether that be on the actual WikiLeaks site or via a link to another site hosting the documents.

v/r

Roger Clark  
Senior Advisor  
National & Cyber Security  
Office of the Chief Information Officer  
U.S. Department of Commerce  
Phone: (202) 482-0121  
Email: [rclark@doc.gov](mailto:rclark@doc.gov)<<mailto:rclark@doc.gov>>

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

**From:** ANDRE DEMEGRET [<mailto:ADEMEGRE@bis.doc.gov>]<[mailto:\[mailto:ADEMEGRE@bis.doc.gov\]](mailto:[mailto:ADEMEGRE@bis.doc.gov])>

**Sent:** Wednesday, December 01, 2010 2:00 PM

**To:** DOC-CIRT

**Subject:** Fwd: Guidance regarding Wikileaks ( -forwarded)

What is the guidance with regard to the hypothetical viewing of these documents on a personal home PC or portable device? Also, what is the guidance with respect to viewing online media sources that may report the contents of the leaked documents in whole or in part or in summary?

## Clark, Roger

---

**From:** Clark, Roger  
**Sent:** Wednesday, December 01, 2010 5:08 PM  
**To:** DeMegret, Andre  
**Subject:** Question

In this hypothetical scenario, the user potentially has U.S. Government classified information on their home PC. As a DOC official, I have no authority over personal PCs. However, as a law enforcement official I'm sure you are aware of the possible consequences of having classified information on a personal machine that is not located in a secure space. I would suggest to this hypothetical user that if they have a security clearance that the hypothetical incident be reported to their servicing security officer and that the hard drive be wiped using a DOD approved tool such as BC-Wipe.

Media sources that are reporting on the incident are viewed as ok as long as the person does not access the source documents whether that be on the actual WikiLeaks site or via a link to another site hosting the documents.

v/r  
Roger Clark  
Senior Advisor  
National & Cyber Security  
Office of the Chief Information Officer  
U.S. Department of Commerce  
Phone: (202) 482-0121  
Email: [rclark@doc.gov](mailto:rclark@doc.gov)

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

**From:** ANDRE DEMEGRET [<mailto:ADEMEGRE@bis.doc.gov>]  
**Sent:** Wednesday, December 01, 2010 2:00 PM  
**To:** DOC-CIRT  
**Subject:** Fwd: Guidance regarding Wikileaks ( -forwarded)

What is the guidance with regard to the hypothetical viewing of these documents on a personal home PC or portable device? Also, what is the guidance with respect to viewing online media sources that may report the contents of the leaked documents in whole or in part or in summary?

**Clark, Roger**

---

**From:** smoses@eda.doc.gov  
**Sent:** Friday, December 10, 2010 1:41 PM  
**To:** Clark, Roger  
**Subject:** Custody Form for WikiLeaks

Roger,

Attached are the custody forms with my signature.

File(s) will be available for download until **09 January 2011**:

File: Custody Form HD WikiLeaks.pdf, 1,086.68 KB [Fingerprint: bf38a8b63c7ee57f4ce43b4843cc163e]

You have received attachment link(s) within this email sent via Proofpoint Secure File Transfer. To retrieve the attachment(s), please click on the link(s).

Accellion File Transfer



## Clark, Roger

---

**From:** Clark, Roger  
**Sent:** Monday, December 13, 2010 9:21 AM  
**To:** Moses, Sandranette  
**Subject:** RE: Custody Form for WikiLeaks

Got it thanks

**From:** [smoses@eda.doc.gov](mailto:smoses@eda.doc.gov) [mailto:[smoses@eda.doc.gov](mailto:smoses@eda.doc.gov)]  
**Sent:** Friday, December 10, 2010 1:41 PM  
**To:** Clark, Roger  
**Subject:** Custody Form for WikiLeaks

Roger,

Attached are the custody forms with my signature.

File(s) will be available for download until **09 January 2011**:

File: [Custody Form HD WikiLeaks.pdf](#), 1,086.68 KB [Fingerprint: bf38a8b63c7ee57f4ce43b4843cc163e]

You have received attachment link(s) within this email sent via Proofpoint Secure File Transfer. To retrieve the attachment(s), please click on the link(s).

[Accellion File Transfer](#)

**Clark, Roger**

---

**From:** Szykman, Simon  
**Sent:** Tuesday, November 30, 2010 5:03 PM  
**To:** Clark, Roger  
**Subject:** FW: Wikileaks Site Block \*\*\*Situational Awareness\*\*\*

**Importance:** High

FYI, Roger, another bureau response.

- Simon

--  
Chief Information Officer  
U.S. Department of Commerce

**From:** Renee Macklin [<mailto:Renee.Macklin@trade.gov>]  
**Sent:** Tuesday, November 30, 2010 5:01 PM  
**To:** Szykman, Simon  
**Cc:** Neal, Earl  
**Subject:** FW: Wikileaks Site Block \*\*\*Situational Awareness\*\*\*  
**Importance:** High

Hi Simon,

I hate to bother you but Earl is out. I am seeking to understand if these procedures are what all the other Federal agencies are using for Wikileaks.

ITA blocked the site on Monday but we had some folks access the site on Friday. Some of the people that accessed the sites are in different countries, so we can't just walk up and take their drives. I assume that I would need someone with a clearance to get the drives based on the data. I am having a hard time believing that this is how other federal agencies are dealing with this issue. Then again I should not be surprised.

Is this the guidance from DHS or Justice?

Renee A. Macklin  
Chief Information Officer  
International Trade Administration  
202-482-3801  
202-482-4066 Fax  
[Renee.Macklin@trade.gov](mailto:Renee.Macklin@trade.gov)

**From:** Paul Murray  
**Sent:** Tuesday, November 30, 2010 4:19 PM  
**To:** Michael Tippin; Curt Shaffer; Willie Turner  
**Cc:** Chuck Hicks; Howard Levitas/OCIO; Renee Macklin  
**Subject:** FW: Wikileaks Site Block \*\*\*Situational Awareness\*\*\*  
**Importance:** High

As expected and of course it comes late day!

**From:** members of the Federation of Department of Commerce CIRTs and CIRCs  
[\[mailto:FEDCIRT@LIST.COMMERCE.GOV\]](mailto:FEDCIRT@LIST.COMMERCE.GOV) **On Behalf Of** Nguyen, Vu  
**Sent:** Tuesday, November 30, 2010 4:17 PM  
**To:** [FEDCIRT@LIST.COMMERCE.GOV](mailto:FEDCIRT@LIST.COMMERCE.GOV)  
**Subject:** Re: Wikileaks Site Block \*\*\*Situational Awareness\*\*\*  
**Importance:** High

Federation Team Members,

The following action is to be taken on all PC's identified as accessing the WikiLeaks.org site since Friday, Nov 26<sup>th</sup>:

- 1) Immediately disconnect the PC from the network
- 2) Remove the hard drive and replace with a new hard drive.
- 3) Do not copy user data from the removed drive to the new drive.
- 4) Label the removed hard drive with the user name.
- 5) Label the removed hard drive as potentially having classified material.
- 6) The drive should be treated as containing Secret material.
- 7) Store the removed hard drive in a GSA approved safe until further guidance is provided or forward the hard drive (packaged in accordance with the DOC Security Manual for transporting Secret material) to:

Roger Clark  
Senior Advisor  
National & Cyber Security  
U.S. Department of Commerce  
1401 Constitution Avenue, NW, Room 6625  
Washington, DC 20230

- 8) Report completion to the DOC-CIRT.

Thanks,  
Vu T. Nguyen  
Office of the Chief Information Officer  
Advanced Cyber Threat and Forensic Analysis Team Lead  
U.S. Department of Commerce  
E-mail: [vnguyen@doc.gov](mailto:vnguyen@doc.gov)  
SIPRNet: [vnguyen@doc.sgov.gov](mailto:vnguyen@doc.sgov.gov)  
Phone: (202) 482-6401  
Blackberry: (202) 834-9123

**From:** Nguyen, Vu  
**Sent:** Tuesday, November 30, 2010 11:57 AM  
**To:** 'FEDCIRT@LIST.COMMERCE.GOV'  
**Cc:** Clark, Roger; Whiteside, Fred; DOC-CIRT  
**Subject:** Wikileaks Site Block \*\*\*Situational Awareness\*\*\*  
**Importance:** High

Federation Team Members,

Due to recent reports of classified information residing on the Wikileaks.org website, all OU's are to immediately block access to the site via URL filter or DNS black-hole. Report completion of this task to DOC-CIRT by COB today.

In addition to the site-block, a report is required noting the number of PC's and a listing of users that have accessed the site since Friday, November 26, 2010. It is possible that these PC's could inadvertently contain classified information.

Thanks,  
Vu T. Nguyen  
Office of the Chief Information Officer  
Advanced Cyber Threat and Forensic Analysis Team Lead  
U.S. Department of Commerce  
E-mail: [vnguyen@doc.gov](mailto:vnguyen@doc.gov)  
SIPRNet: [vnguyen@doc.sgov.gov](mailto:vnguyen@doc.sgov.gov)  
Phone: (202) 482-6401  
Blackberry: (202) 834-9123

## Clark, Roger

---

**From:** Szykman, Simon  
**Sent:** Tuesday, November 30, 2010 5:03 PM  
**To:** Clark, Roger  
**Subject:** FW: Wikileaks Site Block \*\*\*Situational Awareness\*\*\*  
**Importance:** High

FYI, Roger, another bureau response.

- Simon

--  
Chief Information Officer  
U.S. Department of Commerce

**From:** Renee Macklin [<mailto:Renee.Macklin@trade.gov>]  
**Sent:** Tuesday, November 30, 2010 5:01 PM  
**To:** Szykman, Simon  
**Cc:** Neal, Earl  
**Subject:** FW: Wikileaks Site Block \*\*\*Situational Awareness\*\*\*  
**Importance:** High

Hi Simon,

I hate to bother you but Earl is out. I am seeking to understand if these procedures are what all the other Federal agencies are using for Wikileaks.

ITA blocked the site on Monday but we had some folks access the site on Friday. Some of the people that accessed the sites are in different countries, so we can't just walk up and take their drives. I assume that I would need someone with a clearance to get the drives based on the data. I am having a hard time believing that this is how other federal agencies are dealing with this issue. Then again I should not be surprised.

Is this the guidance from DHS or Justice?

Renee A. Macklin  
Chief Information Officer  
International Trade Administration  
202-482-3801  
202-482-4066 Fax  
[Renee.Macklin@trade.gov](mailto:Renee.Macklin@trade.gov)

**From:** Paul Murray  
**Sent:** Tuesday, November 30, 2010 4:19 PM  
**To:** Michael Tippin; Curt Shaffer; Willie Turner  
**Cc:** Chuck Hicks; Howard Levitas/OCIO; Renee Macklin  
**Subject:** FW: Wikileaks Site Block \*\*\*Situational Awareness\*\*\*  
**Importance:** High

As expected and of course it comes late day!

**From:** members of the Federation of Department of Commerce CIRTs and CIRCs  
[mailto:FEDCIRT@LIST.COMMERCE.GOV] **On Behalf Of** Nguyen, Vu  
**Sent:** Tuesday, November 30, 2010 4:17 PM  
**To:** FEDCIRT@LIST.COMMERCE.GOV  
**Subject:** Re: Wikileaks Site Block \*\*\*Situational Awareness\*\*\*  
**Importance:** High

Federation Team Members,

The following action is to be taken on all PC's identified as accessing the WikiLeaks.org site since Friday, Nov 26<sup>th</sup>:

- 1) Immediately disconnect the PC from the network
- 2) Remove the hard drive and replace with a new hard drive.
- 3) Do not copy user data from the removed drive to the new drive.
- 4) Label the removed hard drive with the user name.
- 5) Label the removed hard drive as potentially having classified material.
- 6) The drive should be treated as containing Secret material.
- 7) Store the removed hard drive in a GSA approved safe until further guidance is provided or forward the hard drive (packaged in accordance with the DOC Security Manual for transporting Secret material) to:

Roger Clark  
Senior Advisor  
National & Cyber Security  
U.S. Department of Commerce  
1401 Constitution Avenue, NW, Room 6625  
Washington, DC 20230

- 8) Report completion to the DOC-CIRT.

Thanks,

Vu T. Nguyen  
Office of the Chief Information Officer  
Advanced Cyber Threat and Forensic Analysis Team Lead  
U.S. Department of Commerce  
E-mail: [vnguyen@doc.gov](mailto:vnguyen@doc.gov)  
SIPRNet: [vnguyen@doc.sgov.gov](mailto:vnguyen@doc.sgov.gov)  
Phone: (202) 482-6401  
Blackberry: (202) 834-9123

**From:** Nguyen, Vu  
**Sent:** Tuesday, November 30, 2010 11:57 AM  
**To:** 'FEDCIRT@LIST.COMMERCE.GOV'  
**Cc:** Clark, Roger; Whiteside, Fred; DOC-CIRT  
**Subject:** Wikileaks Site Block \*\*\*Situational Awareness\*\*\*  
**Importance:** High

Federation Team Members,

Due to recent reports of classified information residing on the Wikileaks.org website, all OU's are to immediately block access to the site via URL filter or DNS black-hole. Report completion of this task to DOC-CIRT by COB today.

In addition to the site-block, a report is required noting the number of PC's and a listing of users that have accessed the site since Friday, November 26, 2010. It is possible that these PC's could inadvertently contain classified information.

Thanks,  
Vu T. Nguyen  
Office of the Chief Information Officer  
Advanced Cyber Threat and Forensic Analysis Team Lead  
U.S. Department of Commerce  
E-mail: [vnguyen@doc.gov](mailto:vnguyen@doc.gov)  
SIPRNet: [vnguyen@doc.sgov.gov](mailto:vnguyen@doc.sgov.gov)  
Phone: (202) 482-6401  
Blackberry: (202) 834-9123

## **Clark, Roger**

---

**From:** Macklin, Renee  
**Sent:** Tuesday, November 30, 2010 5:01 PM  
**To:** Szykman, Simon  
**Cc:** Neal, Earl  
**Subject:** FW: Wikileaks Site Block \*\*\*Situational Awareness\*\*\*

**Importance:** High

Hi Simon,

I hate to bother you but Earl is out. I am seeking to understand if these procedures are what all the other Federal agencies are using for Wikileaks.

ITA blocked the site on Monday but we had some folks access the site on Friday. Some of the people that accessed the sites are in different countries, so we can't just walk up and take their drives. I assume that I would need someone with a clearance to get the drives based on the data. I am having a hard time believing that this is how other federal agencies are dealing with this issue. Then again I should not be surprised.

Is this the guidance from DHS or Justice?

Renee A. Macklin  
Chief Information Officer  
International Trade Administration  
202-482-3801  
202-482-4066 Fax  
[Renee.Macklin@trade.gov](mailto:Renee.Macklin@trade.gov)

**From:** Paul Murray  
**Sent:** Tuesday, November 30, 2010 4:19 PM  
**To:** Michael Tippin; Curt Shaffer; Willie Turner  
**Cc:** Chuck Hicks; Howard Levitas/OCIO; Renee Macklin  
**Subject:** FW: Wikileaks Site Block \*\*\*Situational Awareness\*\*\*  
**Importance:** High

As expected and of course it comes late day!

**From:** members of the Federation of Department of Commerce CIRTs and CIRCs  
[\[mailto:FEDCIRT@LIST.COMMERCE.GOV\]](mailto:FEDCIRT@LIST.COMMERCE.GOV) **On Behalf Of** Nguyen, Vu  
**Sent:** Tuesday, November 30, 2010 4:17 PM  
**To:** [FEDCIRT@LIST.COMMERCE.GOV](mailto:FEDCIRT@LIST.COMMERCE.GOV)  
**Subject:** Re: Wikileaks Site Block \*\*\*Situational Awareness\*\*\*  
**Importance:** High

Federation Team Members,

The following action is to be taken on all PC's identified as accessing the WikiLeaks.org site since Friday, Nov 26<sup>th</sup>:

- 1) Immediately disconnect the PC from the network
- 2) Remove the hard drive and replace with a new hard drive.



- 3) Do not copy user data from the removed drive to the new drive.
- 4) Label the removed hard drive with the user name.
- 5) Label the removed hard drive as potentially having classified material.
- 6) The drive should be treated as containing Secret material.
- 7) Store the removed hard drive in a GSA approved safe until further guidance is provided or forward the hard drive (packaged in accordance with the DOC Security Manual for transporting Secret material) to:

Roger Clark  
Senior Advisor  
National & Cyber Security  
U.S. Department of Commerce  
1401 Constitution Avenue, NW, Room 6625  
Washington, DC 20230

- 8) Report completion to the DOC-CIRT.

Thanks,

Vu T. Nguyen  
Office of the Chief Information Officer  
Advanced Cyber Threat and Forensic Analysis Team Lead  
U.S. Department of Commerce  
E-mail: [vnguyen@doc.gov](mailto:vnguyen@doc.gov)  
SIPRNet: [vnguyen@doc.sgov.gov](mailto:vnguyen@doc.sgov.gov)  
Blackberry: (202) 834-9123

**From:** Nguyen, Vu  
**Sent:** Tuesday, November 30, 2010 11:57 AM  
**To:** 'FEDCIRT@LIST.COMMERCE.GOV'  
**Cc:** Clark, Roger; Whiteside, Fred; DOC-CIRT  
**Subject:** Wikileaks Site Block \*\*\*Situational Awareness\*\*\*  
**Importance:** High

Federation Team Members,

Due to recent reports of classified information residing on the Wikileaks.org website, all OU's are to immediately block access to the site via URL filter or DNS black-hole. Report completion of this task to DOC-CIRT by COB today.

In addition to the site-block, a report is required noting the number of PC's and a listing of users that have accessed the site since Friday, November 26, 2010. It is possible that these PC's could inadvertently contain classified information.

Thanks,  
Vu T. Nguyen  
Office of the Chief Information Officer  
Advanced Cyber Threat and Forensic Analysis Team Lead  
U.S. Department of Commerce  
E-mail: [vnguyen@doc.gov](mailto:vnguyen@doc.gov)  
SIPRNet: [vnguyen@doc.sgov.gov](mailto:vnguyen@doc.sgov.gov)

Phone: (202) 482-6401

Blackberry: (202) 834-9123

**Clark, Roger**

---

**From:** Macklin, Renee  
**Sent:** Tuesday, November 30, 2010 5:01 PM  
**To:** Szykman, Simon  
**Cc:** Neal, Earl  
**Subject:** FW: Wikileaks Site Block \*\*\*Situational Awareness\*\*\*

**Importance:** High

Hi Simon,

I hate to bother you but Earl is out. I am seeking to understand if these procedures are what all the other Federal agencies are using for Wikileaks.

ITA blocked the site on Monday but we had some folks access the site on Friday. Some of the people that accessed the sites are in different countries, so we can't just walk up and take their drives. I assume that I would need someone with a clearance to get the drives based on the data. I am having a hard time believing that this is how other federal agencies are dealing with this issue. Then again I should not be surprised.

Is this the guidance from DHS or Justice?

Renee A. Macklin  
Chief Information Officer  
International Trade Administration  
202-482-3801  
202-482-4066 Fax  
[Renee.Macklin@trade.gov](mailto:Renee.Macklin@trade.gov)

**From:** Paul Murray  
**Sent:** Tuesday, November 30, 2010 4:19 PM  
**To:** Michael Tippin; Curt Shaffer; Willie Turner  
**Cc:** Chuck Hicks; Howard Levitas/OCIO; Renee Macklin  
**Subject:** FW: Wikileaks Site Block \*\*\*Situational Awareness\*\*\*  
**Importance:** High

As expected and of course it comes late day!

**From:** members of the Federation of Department of Commerce CIRTs and CIRCs  
[\[mailto:FEDCIRT@LIST.COMMERCE.GOV\]](mailto:FEDCIRT@LIST.COMMERCE.GOV) **On Behalf Of** Nguyen, Vu  
**Sent:** Tuesday, November 30, 2010 4:17 PM  
**To:** [FEDCIRT@LIST.COMMERCE.GOV](mailto:FEDCIRT@LIST.COMMERCE.GOV)  
**Subject:** Re: Wikileaks Site Block \*\*\*Situational Awareness\*\*\*  
**Importance:** High

Federation Team Members,

The following action is to be taken on all PC's identified as accessing the WikiLeaks.org site since Friday, Nov 26<sup>th</sup>:

- 1) Immediately disconnect the PC from the network
- 2) Remove the hard drive and replace with a new hard drive.

- 3) Do not copy user data from the removed drive to the new drive.
- 4) Label the removed hard drive with the user name.
- 5) Label the removed hard drive as potentially having classified material.
- 6) The drive should be treated as containing Secret material.
- 7) Store the removed hard drive in a GSA approved safe until further guidance is provided or forward the hard drive (packaged in accordance with the DOC Security Manual for transporting Secret material) to:

Roger Clark  
Senior Advisor  
National & Cyber Security  
U.S. Department of Commerce  
1401 Constitution Avenue, NW, Room 6625  
Washington, DC 20230

- 8) Report completion to the DOC-CIRT.

Thanks,

Vu T. Nguyen  
Office of the Chief Information Officer  
Advanced Cyber Threat and Forensic Analysis Team Lead  
U.S. Department of Commerce  
E-mail: [vnguyen@doc.gov](mailto:vnguyen@doc.gov)  
SIPRNet: [vnguyen@doc.sgov.gov](mailto:vnguyen@doc.sgov.gov)

Blackberry: (202) 834-9123

**From:** Nguyen, Vu  
**Sent:** Tuesday, November 30, 2010 11:57 AM  
**To:** 'FEDCIRT@LIST.COMMERCE.GOV'  
**Cc:** Clark, Roger; Whiteside, Fred; DOC-CIRT  
**Subject:** Wikileaks Site Block \*\*\*Situational Awareness\*\*\*  
**Importance:** High

Federation Team Members,

Due to recent reports of classified information residing on the Wikileaks.org website, all OU's are to immediately block access to the site via URL filter or DNS black-hole. Report completion of this task to DOC-CIRT by COB today.

In addition to the site-block, a report is required noting the number of PC's and a listing of users that have accessed the site since Friday, November 26, 2010. It is possible that these PC's could inadvertently contain classified information.

Thanks,  
Vu T. Nguyen  
Office of the Chief Information Officer  
Advanced Cyber Threat and Forensic Analysis Team Lead  
U.S. Department of Commerce  
E-mail: [vnguyen@doc.gov](mailto:vnguyen@doc.gov)  
SIPRNet: [vnguyen@doc.sgov.gov](mailto:vnguyen@doc.sgov.gov)

Phone: (202) 482-6401

• Blackberry: (202) 834-9123

## Clark, Roger

---

**From:** Bell, David  
**Sent:** Friday, December 03, 2010 1:59 PM  
**To:** Clark, Roger  
**Subject:** FW: OMB Memo re: Safeguarding and Wikileaks

Roger, below is the Monday email to Earl I referenced in our meeting.

Thanks for meeting with us today, believe our joint partnership on this will stop the bleeding and proactively move the Dept forward in this critical area. I also believe if we achieve the results that are possible, our team effort could be a best practice for other D&As to emulate.

Dave

---

**From:** Neal, Earl  
**Sent:** Tuesday, November 30, 2010 1:13 PM  
**To:** Bell, David  
**Cc:** Broadbent, Alfred; Dorsey, Eric; Lee, George; Negretti, Alexander; Clark, Roger  
**Subject:** RE: OMB Memo re: Safeguarding and Wikileaks

Hi Dave,

I couldn't agree more with your assessment that we need to partner on this issue. I have a meeting scheduled for 3:00pm with the OCIO senior staff including Simon to discuss our response to the issue. Additionally, we have notified the Commerce IT community to take action to block access to the sites and to begin discovery actions on PC's that may now contain compromised information, and we are seeking guidance from USCERT on how to respond to the event.

I recommend that as the owners of most of the classified systems used by DOC, NTIA should be involved in our assessment action. I'll let you know what comes out of my meeting this afternoon.

*Earl B. Neal*

*Associate CIO, IT Security and Critical Infrastructure*

Office of the CIO

US. Department of Commerce

[eneal@doc.gov](mailto:eneal@doc.gov)

202-482-4708

---

**From:** Bell, David  
**Sent:** Tuesday, November 30, 2010 1:03 PM  
**To:** Neal, Earl  
**Cc:** Broadbent, Alfred; Dorsey, Eric; Lee, George; Negretti, Alexander  
**Subject:** FW: OMB Memo re: Safeguarding and Wikileaks

Earl, re the OMB guidance for a departmental review of classified information safeguarding procedures that went out yesterday (below), this seems to be another excellent opportunity for OSY and OCIO to team up again for a joint effort to

accomplish this new requirement. While OSY has the lead for classified information and classified access, your office has the lead for information systems and systems access.

As you know, the guidance calls for counterintelligence, security, and information assurance experts to conduct this departmental review. I met with our folks today, and we are ready to meet with OCIO staff to develop some milestones to get this done.

One question - Should NTIA be a part of this review team?

If you agree this is the way forward, please advise who will be the OCIO POC and we'll work with that person to get this review moving of DOC's implementation of procedures for safeguarding classified information.

Dave

David K. Bell CPP, PSP  
Deputy Director  
Office of Security  
U.S. Department of Commerce  
1401 Constitution Ave NW  
Washington, DC 20230  
(202) 482-4371 office  
(202) 501-6355 fax

SECURITY IS EVERYONE'S RESPONSIBILITY!

---

**From:** Dorsey, Eric  
**Sent:** Monday, November 29, 2010 12:11 PM  
**To:** Bell, David  
**Cc:** Bryant, Michael  
**Subject:** FW: OMB Memo re: Safeguarding and Wikileaks

Dave – I'm sure this will come through to you very soon.

OMB's suggestion is exactly what our Duty Hours Inspection Program allows us to do. We have outlined in this program that Security, IT Security, and IIP would work together when/if we find inconsistencies in classified system usage. ISOO is well aware of our program, but we still await the technology needed to get us to the last phase of this most important program.

Mike will be providing a copy of the OMB document to Roger Clark (and the NTIA gang) to reinforce the need to keep move this program forward.

Eric.

**From:** Bryant, Michael  
**Sent:** Monday, November 29, 2010 12:03 PM

**To:** Dorsey, Eric  
**Subject:** FW: OMB Memo re: Safeguarding and Wikileaks

Sir,

FYI

**Michael Bryant**

Program Manager

Counterespionage Division

Office of Security

Office: 202-482-6380

Cell: 202-213-9567

Fax: 202-482-1098

[mbryant@doc.gov](mailto:mbryant@doc.gov)

Security is Everyone's Responsibility!

---

**From:** John Bell [<mailto:John.Bell@nara.gov>]  
**Sent:** Monday, November 29, 2010 11:24 AM  
**To:** John Bell  
**Subject:** OMB Memo re: Safeguarding and Wikileaks

The Director of the Office of Management and Budget has issued a memorandum for the heads of Executive departments and agencies regarding WikiLeaks and the mishandling of classified information. Here is a link to the memo:

<http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/wikileaks.pdf>

As noted in the memo, OMB and ISOO will be establishing processes to evaluate and assist agency security programs. As always, feel free to contact me with any questions.

Respectfully,

John



John F. Bell  
Program Analyst  
Information Security Oversight Office  
Phone: 202-357-5109  
Email: [John.Bell@nara.gov](mailto:John.Bell@nara.gov)

## Moses, Sandranette

---

**From:** Moses, Sandranette  
**Sent:** Wednesday, December 08, 2010 8:53 AM  
**To:** Clark, Roger  
**Subject:** RE: Receipt

Can you scan it and send it, fax or you want me to come to your office?

Sandranette Moses  
IT Specialist - Programmer Analyst  
EDA IT Security Officer  
DOC - Economic Development Administration  
Office of Information Technology  
(202) 482- 2463

---

**From:** Clark, Roger [<mailto:RClark@doc.gov>]  
**Sent:** Wednesday, December 08, 2010 8:44 AM  
**To:** Moses, Sandranette  
**Subject:** RE: Receipt

Yep – need your signature

---

**From:** Moses, Sandranette [<mailto:SMoses@eda.doc.gov>]  
**Sent:** Wednesday, December 08, 2010 8:43 AM  
**To:** Clark, Roger  
**Cc:** Ford, Kenneth; Farraj Feijoo, Ricardo  
**Subject:** RE: Receipt

Thank You Did you get the custody form filled out yet?

Sandranette Moses  
IT Specialist - Programmer Analyst  
EDA IT Security Officer  
DOC - Economic Development Administration  
Office of Information Technology  
(202) 482- 2463

---

**From:** Clark, Roger [<mailto:RClark@doc.gov>]  
**Sent:** Wednesday, December 08, 2010 8:04 AM  
**To:** Moses, Sandranette  
**Cc:** Ford, Kenneth; Farraj Feijoo, Ricardo  
**Subject:** RE: Receipt

Ken has the drives. He believes he can have the data transferred by Thursday or Friday at the latest.

---

**From:** Moses, Sandranette [<mailto:SMoses@eda.doc.gov>]  
**Sent:** Tuesday, December 07, 2010 8:50 AM  
**To:** Clark, Roger  
**Cc:** Ford, Kenneth; Farraj Feijoo, Ricardo  
**Subject:** RE: Receipt

Sounds great. Thank you.

Sandranette Moses  
IT Specialist - Programmer Analyst

EDA IT Security Officer  
DOC - Economic Development Administration  
Office of Information Technology  
(202) 482- 2463

**From:** Clark, Roger [<mailto:RClark@doc.gov>]  
**Sent:** Tuesday, December 07, 2010 8:27 AM  
**To:** Moses, Sandranette  
**Cc:** Ford, Kenneth; Farraj Feijoo, Ricardo  
**Subject:** RE: Receipt

My team and I will be off-site this morning. I will have them look into retrieving the files this afternoon and will give you a better timeline once they see how much info they have to review/transfer.

---

**From:** Moses, Sandranette [<mailto:SMoses@eda.doc.gov>]  
**Sent:** Monday, December 06, 2010 5:05 PM  
**To:** Clark, Roger  
**Subject:** RE: Receipt

Roger,

I am following up on providing the location of the user folders that have their personal files on the hard drives that you have in custody. The location for both is c:\documents and settings\ "User name".

Please provide me an estimate on when you can release their personal files.

Thank you,

Sandranette Moses  
IT Specialist - Programmer Analyst  
EDA IT Security Officer  
DOC - Economic Development Administration  
Office of Information Technology  
(202) 482- 2463

---

**From:** Clark, Roger [<mailto:RClark@doc.gov>]  
**Sent:** Wednesday, December 01, 2010 4:41 PM  
**To:** Moses, Sandranette  
**Subject:** Receipt

This email is to document receipt of 1 FedEx package Tracking # 1ZA54 643 01 9281 4325. Unopened package is stored in the safe within 6625.

v/r  
Roger Clark  
Senior Advisor  
National & Cyber Security  
Office of the Chief Information Officer  
U.S. Department of Commerce  
Phone: (202) 482-0121  
Email: [rclark@doc.gov](mailto:rclark@doc.gov)

## Moses, Sandranette

---

From: rclark@doc.gov  
Sent: Wednesday, December 08, 2010 9:11 AM  
To: Moses, Sandranette  
Subject: receipt

Here is the receipts for the 2 drives.

File(s) will be available for download until **07 January 2011**:

File: Receipt.pdf, 262.09 KB [Fingerprint: ae2d34afd9170c2f8f1fe49579f8d97a]

You have received attachment link(s) within this email sent via Proofpoint Secure File Transfer. To retrieve the attachment(s), please click on the link(s).

Accellion File Transfer

## Moses, Sandranette

---

**From:** Moses, Sandranette  
**Sent:** Friday, December 03, 2010 8:40 AM  
**To:** Clark, Roger  
**Subject:** RE: Did you get a name for Chicago yet??

Roger,

I have the other hard drive. When will you be in the office. I will be available between 10am and 11am then after lunch around 2:00pm

Sandranette Moses  
IT Specialist - Programmer Analyst  
EDA IT Security Officer  
DOC - Economic Development Administration  
Office of Information Technology  
(202) 482- 2463

**From:** Clark, Roger [<mailto:RClark@doc.gov>]  
**Sent:** Thursday, December 02, 2010 10:07 AM  
**To:** Moses, Sandranette  
**Subject:** Did you get a name for Chicago yet??

v/r  
Roger Clark  
Senior Advisor  
National & Cyber Security  
Office of the Chief Information Officer  
U.S. Department of Commerce  
Phone: (202) 482-0121  
Email: [rclark@doc.gov](mailto:rclark@doc.gov)

## Moses, Sandranette

---

**From:** Moses, Sandranette  
**Sent:** Thursday, December 02, 2010 7:52 AM  
**To:** Clark, Roger  
**Subject:** RE: Receipt

Thank you

Sandranette Moses  
IT Specialist - Programmer Analyst  
EDA IT Security Officer  
DOC - Economic Development Administration  
Office of Information Technology  
(202) 482- 2463

---

**From:** Clark, Roger [<mailto:RClark@doc.gov>]  
**Sent:** Wednesday, December 01, 2010 4:41 PM  
**To:** Moses, Sandranette  
**Subject:** Receipt

This email is to document receipt of 1 FedEx package Tracking # 1ZA54 643 01 9281 4325. Unopened package is stored in the safe within 6625.

v/r  
Roger Clark  
Senior Advisor  
National & Cyber Security  
Office of the Chief Information Officer  
U.S. Department of Commerce  
Phone: (202) 482-0121  
Email: [rclark@doc.gov](mailto:rclark@doc.gov)

## Moses, Sandranette

---

**From:** Moses, Sandranette  
**Sent:** Wednesday, December 01, 2010 2:19 PM  
**To:** Clark, Roger  
**Subject:** RE: Pulled User Drives

Great

Sandranette Moses  
IT Specialist - Programmer Analyst  
EDA IT Security Officer  
DOC - Economic Development Administration  
Office of Information Technology  
(202) 482- 2463

---

**From:** Clark, Roger [<mailto:RClark@doc.gov>]  
**Sent:** Wednesday, December 01, 2010 1:55 PM  
**To:** Moses, Sandranette  
**Subject:** FW: Pulled User Drives

Hey – if you need data from one of the drives let me know and my guys can pull it for you. See below except you don't have to go through the help desk. Otherwise, after a period of time to be determined by OSY, the drives will be wiped.

---

**From:** Clark, Roger  
**Sent:** Wednesday, December 01, 2010 1:47 PM  
**To:** Rogers, William; Blackwood, Wayne  
**Cc:** DOC-CIRT; Farraj Feijoo, Ricardo; Ford, Kenneth; Nguyen, Vu  
**Subject:** Pulled User Drives

If you receive a request from a user to recover their data, ask them to submit a ticket to the help desk identifying the document(s) or directories that need to be recovered. Please advise the user that the OCIO National Security Program will review the files for potential classified information and if none is found, they will return a CD with the files. We will provide the CD to the help desk for delivery to the user. The process may take up to 2-3 days.

Have the help desk folks forward me all the data recovery requests (remember I don't have access to heat) so I can assign the work to the staff. Let me know if you have any other questions.

v/r  
Roger Clark  
Senior Advisor  
National & Cyber Security  
Office of the Chief Information Officer  
U.S. Department of Commerce  
Phone: (202) 482-0121  
Email: [rclark@doc.gov](mailto:rclark@doc.gov)

**Clark, Roger**

---

**From:** Bell, David  
**Sent:** Friday, December 03, 2010 1:59 PM  
**To:** Clark, Roger  
**Subject:** FW: OMB Memo re: Safeguarding and Wikileaks

Roger, below is the Monday email to Earl I referenced in our meeting.

Thanks for meeting with us today, believe our joint partnership on this will stop the bleeding and proactively move the Dept forward in this critical area. I also believe if we achieve the results that are possible, our team effort could be a best practice for other D&As to emulate.

Dave

---

**From:** Neal, Earl  
**Sent:** Tuesday, November 30, 2010 1:13 PM  
**To:** Bell, David  
**Cc:** Broadbent, Alfred; Dorsey, Eric; Lee, George; Negretti, Alexander; Clark, Roger  
**Subject:** RE: OMB Memo re: Safeguarding and Wikileaks

Hi Dave,

I couldn't agree more with your assessment that we need to partner on this issue. I have a meeting scheduled for 3:00pm with the OCIO senior staff including Simon to discuss our response to the issue. Additionally, we have notified the Commerce IT community to take action to block access to the sites and to begin discovery actions on PC's that may now contain compromised information, and we are seeking guidance from USCERT on how to respond to the event.

I recommend that as the owners of most of the classified systems used by DOC, NTIA should be involved in our assessment action. I'll let you know what comes out of my meeting this afternoon.

*Earl B. Neal*

*Associate CIO, IT Security and Critical Infrastructure*

Office of the CIO

US Department of Commerce

[eneal@doc.gov](mailto:eneal@doc.gov)

202-482-4708

---

**From:** Bell, David  
**Sent:** Tuesday, November 30, 2010 1:03 PM  
**To:** Neal, Earl  
**Cc:** Broadbent, Alfred; Dorsey, Eric; Lee, George; Negretti, Alexander  
**Subject:** FW: OMB Memo re: Safeguarding and Wikileaks

Earl, re the OMB guidance for a departmental review of classified information safeguarding procedures that went out yesterday (below), this seems to be another excellent opportunity for OSY and OCIO to team up again for a joint effort to



accomplish this new requirement. While OSY has the lead for classified information and classified access, your office has the lead for information systems and systems access.

As you know, the guidance calls for counterintelligence, security, and information assurance experts to conduct this departmental review. I met with our folks today, and we are ready to meet with OCIO staff to develop some milestones to get this done.

One question - Should NTIA be a part of this review team?

If you agree this is the way forward, please advise who will be the OCIO POC and we'll work with that person to get this review moving of DOC's implementation of procedures for safeguarding classified information.

Dave

David K. Bell CPP, PSP  
Deputy Director  
Office of Security  
U.S. Department of Commerce  
1401 Constitution Ave NW  
Washington, DC 20230  
(202) 482-4371 office  
(202) 501-6355 fax

SECURITY IS EVERYONE'S RESPONSIBILITY!

---

**From:** Dorsey, Eric  
**Sent:** Monday, November 29, 2010 12:11 PM  
**To:** Bell, David  
**Cc:** Bryant, Michael  
**Subject:** FW: OMB Memo re: Safeguarding and Wikileaks

Dave - I'm sure this will come through to you very soon.

OMB's suggestion is exactly what our Duty Hours Inspection Program allows us to do. We have outlined in this program that Security, IT Security, and IIP would work together when/if we find inconsistencies in classified system usage. ISOO is well aware of our program, but we still await the technology needed to get us to the last phase of this most important program.

Mike will be providing a copy of the OMB document to Roger Clark (and the NTIA gang) to reinforce the need to keep move this program forward.

Eric.

**From:** Bryant, Michael  
**Sent:** Monday, November 29, 2010 12:03 PM

**To:** Dorsey, Eric  
**Subject:** FW: OMB Memo re: Safeguarding and Wikileaks

Sir,

FYI

**Michael Bryant**

Program Manager

Counterespionage Division

Office of Security

Office: 202-482-6380

Cell: 202-213-9567

Fax: 202-482-1098

[mbryant@doc.gov](mailto:mbryant@doc.gov)

Security is Everyone's Responsibility!

---

**From:** John Bell [<mailto:John.Bell@nara.gov>]  
**Sent:** Monday, November 29, 2010 11:24 AM  
**To:** John Bell  
**Subject:** OMB Memo re: Safeguarding and Wikileaks

The Director of the Office of Management and Budget has issued a memorandum for the heads of Executive departments and agencies regarding WikiLeaks and the mishandling of classified information. Here is a link to the memo:

<http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/wikileaks.pdf>

As noted in the memo, OMB and ISOO will be establishing processes to evaluate and assist agency security programs. As always, feel free to contact me with any questions.

Respectfully,

John

John F. Bell  
Program Analyst  
Information Security Oversight Office  
Phone: 202-357-5109  
Email: [John.Bell@nara.gov](mailto:John.Bell@nara.gov)

These are docs  
the D.O.C &  
HHS and R  
Have sent to  
DHS to DHS for  
direct Reply

Clark, Roger

---

From: Neal, Earl  
Sent: Tuesday, December 07, 2010 8:52 AM  
To: Clark, Roger  
Subject: FW: Follow-up on Wikileaks  
Attachments: Security Reminder Message.pdf

Interesting approach to cleanup and remediation.

Earl B. Neal  
Associate CIO, IT Security and Critical Infrastructure Office of the CIO US. Department of  
Commerce eneal@doc.gov  
202-482-4708

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

Sent to another  
agency for direct  
reply

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

From: Galik, Daniel (HHS/ASA) [mailto:Daniel.Galik@hhs.gov]  
Sent: Monday, December 06, 2010 3:49 PM  
To: 'Christopher Lowe'; Sandra.Jamshidi@osd.mil;  
'manning.tonya@dol.gov'; 'Phillip Loranger'; 'Pat Howard'; 'John  
Streufert'; 'Collis (OCIO) Woods'; 'Marian P Cody';  
kurt.garbars@gsa.gov; Edward.Roback@do.treas.gov;  
kevin.deeley@usdoj.gov; Andrew.orndorff@dot.gov; 'Earl Neal'; Coose,  
Matt; 'John T. Smith'; 'Michael J COL MIL USA CIO/G-6 Jones';  
'jerry.davis4@va.gov'; 'Lawrence K Ruffin'; 'West, Robert'  
Subject: RE: Follow-up on Wikileaks

Sorry to bother you all on this topic, as it has been widely discussed via emails to the NIST forum over the past week. My leadership has asked me to verify if the other Departments have all forwarded the OMB email/memo from Friday night to all of your employees and contractors. (I've pasted the OMB General Counsel recommended guidance below).

Would you mind letting me know if your Department forwarded this "NOTICE" below to all your employees/contractors, (and also if you are blocking wikileaks)?

I would really appreciate it.

Within HHS, I recommended to all operating divisions/bureaus that we block wikileaks.org early last week; (but not all my components have implemented the block).

HHS has also not yet forwarded the OMB recommended "NOTICE" in any type of formal communications to our employees.

Sincere thanks.

Dan Galik  
HHS CISO  
202-205-5906

Email/Memo sent Friday by the Office of Management and Budget GC:

AGENCY NOTICE TO EMPLOYEES AND CONTRACTORS CONCERNING SAFEGUARDING OF CLASSIFIED INFORMATION AND USE OF GOVERNMENT INFORMATION TECHNOLOGY SYSTEMS

The recent disclosure of U.S. Government documents by Wikileaks has resulted in damage to our national security. Each federal employee and contractor is obligated to protect classified information pursuant to all applicable laws, and to use government information technology systems in accordance with agency procedures so that the integrity of such systems is not compromised.

Unauthorized disclosures of classified documents (whether in print, on a blog, or on websites) do not alter the documents' classified status or automatically result in declassification of the documents. To the contrary, classified information, whether or not already posted on public websites or disclosed to the media, remains classified, and must be treated as such by federal employees and contractors, until it is declassified by an appropriate U.S. Government authority.

Federal employees and contractors therefore are reminded of the following obligations with respect to the treatment of classified information and the use of non-classified government information technology systems:

\* Except as authorized by their agencies and pursuant to agency procedures, federal employees or contractors shall not, while using

computers or other devices (such as Blackberries or Smart Phones) that access the web on non-classified government systems, access documents that are marked classified (including classified documents publicly available on the Wikileaks and other websites), as doing so risks that material still classified will be placed onto non-classified systems. This requirement applies to access that occurs either through agency or contractor computers, or through employees' or contractors' personally owned computers that access non-classified government systems. This requirement does not restrict employee or contractor access to non-classified, publicly available news reports (and other non-classified material) that may in turn discuss classified material, as distinguished from access to underlying documents that themselves are marked classified (including if the underlying classified documents are available on public websites or otherwise in the public domain).

\* Federal employees or contractors shall not access classified material unless a favorable determination of the person's eligibility for access has been made by an agency head or the agency head's designee, the person has signed and approved non-disclosure agreement, the person has a need to know the information, and the person has received contemporaneous training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.

\* Classified information shall not be removed from official premises or disclosed without proper authorization.

\* Federal employees and contractors who believe they may have inadvertently accessed or downloaded classified or sensitive information on computers that access the web via non-classified government systems, or without prior authorization, should contact their information security offices for assistance.

Thank you for your cooperation, and for your vigilance to these responsibilities..

Sent to another agency  
for direct reply



**Clark, Roger**

---

**From:** Neal, Earl  
**Sent:** Monday, December 06, 2010 10:56 AM  
**To:** Clark, Roger; Whiteside, Fred  
**Cc:** Szykman, Simon  
**Subject:** FW: Classified Information Security Reminder

DHS is a little late to the game with this one.

*Earl B. Neal*

*Associate CIO, IT Security and Critical Infrastructure*

Office of the CIO

US. Department of Commerce

[eneal@doc.gov](mailto:eneal@doc.gov)

202-482-4708

---

sent to  
another agency  
for direct reply

Sent to another agency  
for direct reply

PW

NR

log CC

## Moses, Sandranette

---

**From:** Clark, Roger [RClark@doc.gov]  
**Sent:** Wednesday, December 01, 2010 1:20 PM  
**To:** Moses, Sandranette  
**Cc:** Ahrnsbrak, Darice  
**Subject:** RE: WikiLeaks Issue

Thanks – do you want to deliver the drive to me and I can store in my safe? If so, I'm in Room 6625. I will check with Jonathan to see if we can get further information.

---

**From:** Moses, Sandranette [mailto:SMoses@eda.doc.gov]  
**Sent:** Wednesday, December 01, 2010 1:19 PM  
**To:** Clark, Roger  
**Cc:** Ahrnsbrak, Darice  
**Subject:** RE: WikiLeaks Issue

Roger,

We have the hard drive of the user below. ... The status of the other IP address is that it is the network address (router address) for that region. We are trying to determine why this is being seen accessing the site not a desktop/server. We have to talk more with Jonathan in NOC (HCHB Net Administrator) unless you have more information on the IP address that can further help.

Thank you,

Sandranette Moses  
IT Specialist - Programmer Analyst  
EDA IT Security Officer  
DOC - Economic Development Administration  
Office of Information Technology  
(202) 482- 2463

---

**From:** Clark, Roger [mailto:RClark@doc.gov]  
**Sent:** Tuesday, November 30, 2010 4:30 PM  
**To:** Moses, Sandranette  
**Cc:** Ahrnsbrak, Darice  
**Subject:** RE: WikiLeaks Issue

Thank you.

*Not Responsive*

## Moses, Sandranette

---

**From:** Clark, Roger [RClark@doc.gov]  
**Sent:** Wednesday, December 01, 2010 1:53 PM  
**To:** Moses, Sandranette  
**Subject:** RE: WikiLeaks Issue

It is up to you – but it needs to be stored in a safe.

**From:** Moses, Sandranette [mailto:SMoses@eda.doc.gov]  
**Sent:** Wednesday, December 01, 2010 1:50 PM  
**To:** Clark, Roger  
**Subject:** RE: WikiLeaks Issue

I can wait until we receive both drives. Will the HDs be returned?

Sandranette Moses  
IT Specialist - Programmer Analyst  
EDA IT Security Officer  
DOC - Economic Development Administration  
Office of Information Technology  
(202) 482- 2463

**From:** Clark, Roger [mailto:RClark@doc.gov]  
**Sent:** Wednesday, December 01, 2010 1:20 PM  
**To:** Moses, Sandranette  
**Cc:** Ahrnsbrak, Darice  
**Subject:** RE: WikiLeaks Issue

Thanks – do you want to deliver the drive to me and I can store in my safe? If so, I'm in Room 6625. I will check with Jonathan to see if we can get further information.

**From:** Moses, Sandranette [mailto:SMoses@eda.doc.gov]  
**Sent:** Wednesday, December 01, 2010 1:19 PM  
**To:** Clark, Roger  
**Cc:** Ahrnsbrak, Darice  
**Subject:** RE: WikiLeaks Issue

Roger,

We have the hard drive of the user below. ... The status of the other IP address is that it is the network address (router address) for that region. We are trying to determine why this is being seen accessing the site not a desktop/server. We have to talk more with Jonathan in NOC (HCHB Net Administrator) unless you have more information on the IP address that can further help.

Thank you,

Sandranette Moses  
IT Specialist - Programmer Analyst  
EDA IT Security Officer  
DOC - Economic Development Administration  
Office of Information Technology  
(202) 482- 2463

*Not Responsive*

PW

(b)(2) (b)(6)

4

NR

leg cc

3

## Moses, Sandranette

---

**From:** Tarlan, Hossein  
**Sent:** Wednesday, December 01, 2010 1:43 PM  
**To:** Moses, Sandranette  
**Cc:** Jayakody, Ananda; Ahrnsbrak, Darice  
**Subject:** RE: WikiLeaks Issue

Ok, (S)(b) (S)(b)

This is [REDACTED] machine in Chicago, the machine name is [REDACTED].

I also removed the full IP address from Roger's email for security reasons,,,,

Regards,

---

**From:** Moses, Sandranette  
**Sent:** Wednesday, December 01, 2010 1:37 PM  
**To:** Tarlan, Hossein  
**Cc:** Jayakody, Ananda; Ahrnsbrak, Darice  
**Subject:** FW: WikiLeaks Issue

See e-mail below. Mystery is over. Wrong IP. Please provide user. In a separate e-mail.

Sandranette Moses  
IT Specialist - Programmer Analyst  
EDA IT Security Officer  
DOC - Economic Development Administration  
Office of Information Technology  
(202) 482- 2463

---

**From:** Clark, Roger [<mailto:RCClark@doc.gov>]  
**Sent:** Wednesday, December 01, 2010 1:34 PM  
**To:** Moses, Sandranette  
**Cc:** Ahrnsbrak, Darice  
**Subject:** RE: WikiLeaks Issue

(S)(Z)

Just talked to Jon – the IP address we are looking for is [REDACTED] not [REDACTED] Sorry for the confusion.

---

**From:** Moses, Sandranette [<mailto:SMoses@eda.doc.gov>]  
**Sent:** Wednesday, December 01, 2010 1:19 PM  
**To:** Clark, Roger  
**Cc:** Ahrnsbrak, Darice  
**Subject:** RE: WikiLeaks Issue

Roger,

We have the hard drive of the user below. ... The status of the other IP address is that it is the network address (router address) for that region. We are trying to determine why this is being seen accessing the site not a desktop/server. We have to talk more with Jonathan in NOC (HCHB Net Administrator) unless you have more information on the IP address that can further help.

Thank you,

Sandranette Moses  
IT Specialist - Programmer Analyst  
EDA IT Security Officer  
DOC - Economic Development Administration  
Office of Information Technology  
(202) 482- 2463

[REDACTED]

[REDACTED]

*Not Responsive*

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



**Clark, Roger**

---

**From:** Galik, Daniel (HHS/ASA) [Daniel.Galik@hhs.gov]  
**Sent:** Monday, December 06, 2010 5:13 PM  
**To:** Neal, Earl  
**Subject:** RE: Follow-up on Wikileaks

No, but I think there is still a lot of ongoing legal debate around this topic.

Thanks for responding!

Dan

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

**From:** Neal, Earl [mailto:ENeal@doc.gov]  
**Sent:** Monday, December 06, 2010 4:52 PM  
**To:** Galik, Daniel (HHS/ASA)  
**Subject:** RE: Follow-up on Wikileaks

Hi Dan,

Yes. The OMB guidance was sent out today by our General Counsel. We had already notified our employees and placed site blocks by mid-week. Do you have any idea why it took OMB until Friday to send out guidance?

Earl B. Neal

Associate CIO, IT Security and Critical Infrastructure Office of the CIO US. Department of Commerce  
eneal@doc.gov  
202-482-4708

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

**From:** Galik, Daniel (HHS/ASA) [mailto:Daniel.Galik@hhs.gov]  
**Sent:** Monday, December 06, 2010 3:49 PM  
**To:** 'Christopher Lowe'; 'Sandra M CAPT NII/DoD-CIO Jamshidi'; 'manning.tonya@dol.gov'; 'Phillip Loranger'; 'Pat Howard'; 'John Streufert'; 'Collis (OCIO) Woods'; 'Marian P Cody'; 'kurt.garbars@gsa.gov'; 'Ed Roback'; 'Kevin Deeley'; 'andrew.orndorff@dot.gov'; Neal, Earl; 'Matt Coose'; 'John T. Smith'; 'Michael J COL MIL USA CIO/G-6 Jones'; 'jerry.davis4@va.gov'; 'Lawrence K Ruffin'; 'West, Robert'  
**Subject:** RE: Follow-up on Wikileaks

For the Department/Agency CISOs....

Sorry to bother you all on this topic, as it has been widely discussed via emails to the NIST forum over the past week. My leadership has asked me to verify if the other Departments have all forwarded the OMB email/memo from Friday night to all of your employees and contractors. (I've pasted the OMB General Counsel recommended guidance below).

Would you mind letting me know if your Department forwarded this "NOTICE" below to all your employees/contractors, (and also if you are blocking wikileaks)?

I would really appreciate it.

Within HHS, I recommended to all operating divisions/bureaus that we block wikileaks.org early last week; (but not all my components have implemented the block).

HHS has also not yet forwarded the OMB recommended "NOTICE" in any type of formal communications to our employees.

Sincere thanks.

Dan Galik  
HHS CISO  
202-205-5906

= = = = =

Email/Memo sent Friday by the Office of Management and Budget GC:

AGENCY NOTICE TO EMPLOYEES AND CONTRACTORS CONCERNING SAFEGUARDING OF CLASSIFIED INFORMATION AND USE OF GOVERNMENT INFORMATION TECHNOLOGY SYSTEMS

The recent disclosure of U.S. Government documents by Wikileaks has resulted in damage to our national security. Each federal employee and contractor is obligated to protect classified information pursuant to all applicable laws, and to use government information technology systems in accordance with agency procedures so that the integrity of such systems is not compromised.

Unauthorized disclosures of classified documents (whether in print, on a blog, or on websites) do not alter the documents' classified status or automatically result in declassification of the documents. To the contrary, classified information, whether or not already posted on public websites or disclosed to the media, remains classified, and must be treated as such by federal employees and contractors, until it is declassified by an appropriate U.S. Government authority.

Federal employees and contractors therefore are reminded of the following obligations with respect to the treatment of classified information and the use of non-classified government information technology systems:

\* Except as authorized by their agencies and pursuant to agency procedures, federal employees or contractors shall not, while using computers or other devices (such as Blackberries or Smart Phones) that access the web on non-classified government systems, access documents that are marked classified (including classified documents publicly available on the Wikileaks and other websites), as doing so risks that material still classified will be placed onto non-classified systems. This requirement applies to access that occurs either through agency or contractor computers, or through employees' or contractors' personally owned computers that access non-classified government systems. This requirement does not restrict employee or contractor access to non-classified, publicly available news reports (and other non-classified material) that may in turn discuss classified material, as distinguished from access to underlying documents that themselves are marked classified (including if the underlying classified documents are available on public websites or otherwise in the public domain).

\* Federal employees or contractors shall not access classified material unless a favorable determination of the person's eligibility for access has been made by an agency head or the agency head's designee, the person has signed and approved non-disclosure agreement, the person has a need to know the information, and the person has received contemporaneous training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.

\* Classified information shall not be removed from official premises or disclosed without proper authorization.

\* Federal employees and contractors who believe they may have inadvertently accessed or downloaded classified or sensitive information on computers that access the web via non-classified government systems, or without prior authorization, should contact their information security offices for assistance.

Thank you for your cooperation, and for your vigilance to these responsibilities.

**Clark, Roger**

---

**From:** Neal, Earl  
**Sent:** Monday, December 06, 2010 4:52 PM  
**To:** Galik, Daniel (HHS/ASA)  
**Subject:** RE: Follow-up on Wikileaks

Hi Dan,

Yes. The OMB guidance was sent out today by our General Counsel. We had already notified our employees and placed site blocks by mid-week. Do you have any idea why it took OMB until Friday to send out guidance?

Earl B. Neal  
Associate CIO, IT Security and Critical Infrastructure Office of the CIO US. Department of Commerce  
eneal@doc.gov  
202-482-4708

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

**From:** Galik, Daniel (HHS/ASA) [mailto:Daniel.Galik@hhs.gov]  
**Sent:** Monday, December 06, 2010 3:49 PM  
**To:** 'Christopher Lowe'; 'Sandra M CAPT NII/DoD-CIO Jamshidi'; 'manning.tonya@dol.gov'; 'Phillip Loranger'; 'Pat Howard'; 'John Streufert'; 'Collis (OCIO) Woods'; 'Marian P Cody'; 'kurt.garbars@gsa.gov'; 'Ed Roback'; 'Kevin Deeley'; 'andrew.orndorff@dot.gov'; Neal, Earl; 'Matt Coose'; 'John T. Smith'; 'Michael J COL MIL USA CIO/G-6 Jones'; 'jerry.davis4@va.gov'; 'Lawrence K Ruffin'; 'West, Robert'  
**Subject:** RE: Follow-up on Wikileaks

For the Department/Agency CISOs....

Sorry to bother you all on this topic, as it has been widely discussed via emails to the NIST forum over the past week. My leadership has asked me to verify if the other Departments have all forwarded the OMB email/memo from Friday night to all of your employees and contractors. (I've pasted the OMB General Counsel recommended guidance below).

Would you mind letting me know if your Department forwarded this "NOTICE" below to all your employees/contractors, (and also if you are blocking wikileaks)?

I would really appreciate it.

Within HHS, I recommended to all operating divisions/bureaus that we block wikileaks.org early last week; (but not all my components have implemented the block).

HHS has also not yet forwarded the OMB recommended "NOTICE" in any type of formal communications to our employees.

Sincere thanks.

Dan Galik  
HHS CISO  
202-205-5906

= = = = =

Email/Memo sent Friday by the Office of Management and Budget GC:

AGENCY NOTICE TO EMPLOYEES AND CONTRACTORS CONCERNING SAFEGUARDING OF CLASSIFIED INFORMATION  
AND USE OF GOVERNMENT INFORMATION TECHNOLOGY SYSTEMS

The recent disclosure of U.S. Government documents by WikiLeaks has resulted in damage to our national security. Each federal employee and contractor is obligated to protect classified information pursuant to all applicable laws, and to use government information technology systems in accordance with agency procedures so that the integrity of such systems is not compromised.

Unauthorized disclosures of classified documents (whether in print, on a blog, or on websites) do not alter the documents' classified status or automatically result in declassification of the documents. To the contrary, classified information, whether or not already posted on public websites or disclosed to the media, remains classified, and must be treated as such by federal employees and contractors, until it is declassified by an appropriate U.S. Government authority.

Federal employees and contractors therefore are reminded of the following obligations with respect to the treatment of classified information and the use of non-classified government information technology systems:

\* Except as authorized by their agencies and pursuant to agency procedures, federal employees or contractors shall not, while using computers or other devices (such as Blackberries or Smart Phones) that access the web on non-classified government systems, access documents that are marked classified (including classified documents publicly available on the WikiLeaks and other websites), as doing so risks that material still classified will be placed onto non-classified systems. This requirement applies to access that occurs either through agency or contractor computers, or through employees' or contractors' personally owned computers that access non-classified government systems. This requirement does not restrict employee or contractor access to non-classified, publicly available news reports (and other non-classified material) that may in turn discuss classified material, as distinguished from access to underlying documents that themselves are marked classified (including if the underlying classified documents are available on public websites or otherwise in the public domain).

\* Federal employees or contractors shall not access classified material unless a favorable determination of the person's eligibility for access has been made by an agency head or the agency head's designee, the person has signed and approved non-disclosure agreement, the person has a need to know the information, and the person has received contemporaneous training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.

\* Classified information shall not be removed from official premises or disclosed without proper authorization.

\* Federal employees and contractors who believe they may have inadvertently accessed or downloaded classified or sensitive information on computers that access the web via non-classified government systems, or without prior authorization, should contact their information security offices for assistance.

Thank you for your cooperation, and for your vigilance to these responsibilities.

11-091

PW

(b)(2)

16

requester cc

Missing Network Device?

**Subject:** Missing Network Device?

**From:** David Kustaborder <kusty@nist.gov>

**Date:** Wed, 1 Dec 2010 09:44:18 -0500

**To:** "Antonishek, John K." <john.antonishek@nist.gov>

find\_ip (b)(2)

Time now is: Wed Dec 1 09:33:01 2010

Information since: Sat Oct 2 10:33:01 2010

Information for IP address (b)(2)

== ARP Database

---

== IT Asset Inventory Database

---

633663 (Desktop), (b)(2), 470., (b)(2)

**Antonishek, John K.**

---

**From:** Antonishek, John K.  
**Sent:** Wednesday, December 01, 2010 8:54 PM  
**To:** [REDACTED]  
**Cc:** siirt; Glenn, K. Robert; Richter, Gale C.  
**Subject:** RE: Clean up plan

For the future, when we have to do these activities to our own computers, please either work in pairs or have someone else in the team perform the work on your own computer.

Merely for appearances sake and the other person will be more "distant" to the issue and may catch something that you may miss because you're too close to the issue (emotions often cloud thought processes).

Thanks!

-John

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

**From:** [REDACTED]  
**Sent:** Wednesday, December 01, 2010 2:03 PM  
**To:** Antonishek, John K.  
**Cc:** siirt  
**Subject:** RE: Clean up plan

For the record...

I have executed all of the steps on my local desktop machine [REDACTED] Eraser is currently running.

1. identify the browser used; in that browser, clear cache, history, temporary files, etc.
  - Firefox; cache cleared, history cleared, temporary files deleted
2. verify if the user stored any downloaded files elsewhere (thumb drives, CDs, DVDs, etc)
  - nothing stored anywhere else
3. verify that nothing was forwarded via other methods, such as Email, IM, etc. to other people
  - nothing was forwarded
4. On windows, install Eraser and erase unused data on each partition involved (eraser will handle sectors and cluster tips automatically) and any files/directories identified in #2; when finished, delete/uninstall eraser program
  - Eraser is being run on all disk drives in machine.

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

**From:** Antonishek, John K.  
**Sent:** Wednesday, December 01, 2010 1:18 PM  
**To:** Glenn, K. Robert  
**Cc:** siirt; Beltz, John; Richter, Gale C.  
**Subject:** Clean up plan

=== DRAFT INSTRUCTIONS ===

1. SIIRT: carve out full network packet traces for those computers identified as connecting to the web site(s) (cross reference list from Firewall Team).



2. SIIRT: analyze full network traces to create a priority of those computers that have the highest potential to contain classified material.

For each computer:

1. identify the browser used; in that browser, clear cache, history, temporary files, etc.
2. verify if the user stored any downloaded files elsewhere (thumb drives, CDs, DVDs, etc)
3. verify that nothing was forwarded via other methods, such as Email, IM, etc. to other people
4. On windows, install Eraser and erase unused data on each partition involved (eraser will handle sectors and cluster tips automatically) and any files/directories identified in #2; when finished, delete/uninstall eraser program

On Linux/Mac, run "dd if=/dev/zero of=large-zero-file; rm large-zero-file" on each filesystem involved (will cause the filesystem to be full for a short amount of time)

While you're performing the steps, document the steps you're taking, responses from the user for your questions, and any errors that may happen (Eraser will give you errors on files that are currently active by the OS, which is normal).

-John

Re: wiki sources (with contact)

**Subject:** Re: wiki sources (with contact)  
**From:** David Kustaborder <kusty@nist.gov>  
**Date:** Thu, 2 Dec 2010 10:20:21 -0500  
**To:** "Antonishek, John K." <john.antonishek@nist.gov>

FYI, I spoke to Ann to try to determine the user of this machine and [REDACTED] (b)(2)

On 12/02/2010 10:02 AM, Antonishek, John K. wrote:

For [REDACTED], I see: (b)(2)

\$ find\_ip [REDACTED]

Time now is: Thu Dec 2 09:41:23 2010

Information since: Sun Oct 3 10:41:22 2010

Information for IP address [REDACTED]

== ARP Database == (b)(2)

Thu Dec 2 09:40:37 2010 [REDACTED]

Ethernet Address info for [REDACTED] (b)(2)

Fri Nov 19 15:46:29 2010 [REDACTED]

== Gaithersburg LANdesk Database ==

9505

[REDACTED] = good sign, matches DNS name

9505, , , , [REDACTED] (b)(2)

\$

Searching web property for service tag number [REDACTED] I get:

<https://admweb.nist.gov/property/display equipment.cfm?key asset id=384823>

Same bldg/room as find\_ip.

Let me know if I got the right computer.

-John

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

From: David Kustaborder [mailto:kusty@nist.gov]

Sent: Wednesday, December 01, 2010 10:29 AM

To: Glenn, K. Robert

Cc: Antonishek, John K.

Subject: wiki sources (with contact)

**Antonishek, John K.**

---

**From:** Glenn, K. Robert  
**Sent:** Friday, December 03, 2010 10:52 AM  
**To:** siirt  
**Cc:** Glenn, K. Robert  
**Subject:** FW: Updated user "script"

SIIRT, see the note from Judy and see what we can do to find that computer and the relevant user.

Thanks,

Rob G.

---

**From:** Schiller, Susannah B.  
**Sent:** Friday, December 03, 2010 10:40 AM  
**To:** Glenn, K. Robert; Brockett, Del  
**Subject:** RE: Updated user "script"

I'm making progress. I've tried everyone in Gburg at least 3 times, and have reached all but 2 of them. I'm getting ready to do second tries for 3 Boulder folks.

A couple of computers aren't used by the people listed. Darrin Santay was able to identify the right guy for his, and I've talked to that person and noted it in my spreadsheet that I'll send.

Judy Terrill checked all the boxes in her office and couldn't find the property number, so she asked that we work with Don Koss to identify where the computer is and who might have used it. The relevant property number is 635896 and the IP address is [REDACTED] (b)(2)

After I take another stab at my Boulder folks, I'm all in favor of sending the remaining people the email. Not sure it's even worth leaving voicemail.

---

**From:** Glenn, K. Robert  
**Sent:** Friday, December 03, 2010 10:31 AM  
**To:** Glenn, K. Robert; Schiller, Susannah B.; Brockett, Del  
**Cc:** Glenn, K. Robert  
**Subject:** RE: Updated user "script"

After 1 attempt yesterday and 2 attempts today, I'm still unable to get in touch with 6 out of 17 users (Susannah ?). I plan on trying 1 more time before lunch. At what point can we leave them a voicemail reassuring them that they are not in trouble; but we need to work with them to have their computer sanitized, and let them know we'll send the details in an email?

Rob G.

---

**From:** Glenn, K. Robert  
**Sent:** Thursday, December 02, 2010 3:48 PM  
**To:** Schiller, Susannah B.; Brockett, Del  
**Cc:** Glenn, K. Robert  
**Subject:** Updated user "script"

Attached is the updated script for users. Mostly minor changes (I included a note so you can mention names of the incident response team). If I notice the user is particularly concerned, I will re-assure them that this inadvertent will not result in them getting into any trouble but we do need them to work with the incident response staff to get this resolved quickly.

The list is almost complete (sans 1 or 2 users) and I'll be sending it shortly, sorted by OU.

Rob G.

Boulder wik 12-8-10 1119ami.txt

From: David Kustaborder [kusty@nist.gov]  
Sent: Wednesday, December 08, 2010 11:19 AM  
To: Beltz, John; Sorensen, Robert  
Subject: Boulder wiki



(b)(2)

Date and Time: Dec 14, 2010 10am

Name: 191hr 1

IP Address: [REDACTED]

MAC Address: [REDACTED]

Property Number: \_\_\_\_\_

Browser Used: Chrome / IE

O/S: Windows XP

(b)(2)

1. Check if the above information matches the information on the user's PC.

2. Did you go to the web site: Link from COB

3. How did you access the site: "

4. Clear the cache: Done

5. Clear the history: Done

6. Clear temporary files: Done

7. Clear local copies of docs downloaded, such as "Page as" copies Done

8. Did the user store any downloaded files elsewhere? No

9. Detail where the information was stored below. N/A

10. Was any of the information forwarded to other people? N/A  
(i.e. Email, IM)

11. Detail what information was forwarded, and where it went. N/A

12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks.

Running Eraser 12/14/10

13. Sanitize or destroy any mobile media or backup storage used N/A

14. Remove SIIRT tools (after #12 is complete) – Eraser: <http://eraser.heidi.ie/>

Complete 12/14/10  
3pm. JTB

3(a) Room 101  
Luton, Essex 2011

Dr. Burns - 1108  
(2)

Publication 4 EMS  
behind it 3A  
for back left.

101

Date and Time: Dec 9, 2010 10:19am.  
Name: Enrico Lucan  
IP Address: [REDACTED]  
MAC Address: [REDACTED] (b)(2)  
Property Number: 651.06103  
Browser Used: Fire Fox  
O/S: Windows XP

1. Check if the above information matches the information on the user's PC.
2. Did you go to the web site: Yes
3. How did you access the site: Through Firefox / Link from Italian Website
4. Clear the cache: \_\_\_\_\_
5. Clear the history: \_\_\_\_\_
6. Clear temporary files: \_\_\_\_\_
7. Clear local copies of docs downloaded, such as "Page as" copies \_\_\_\_\_

8. Did the user store any downloaded files elsewhere? No

9. Detail where the information was stored below. N/A

10. Was any of the information forwarded to other people? N/A  
(i.e. Email, IM)

11. Detail what information was forwarded, and where it went.  
N/A

12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks.

Complete 12/9/10

13. Sanitize or destroy any mobile media or backup storage used N/A

14. Remove SIIRT tools (after #12 is complete) – Eraser: <http://eraser.heidi.ie/>  
Complete 12/9/10 JTB



Date and Time: Dec 9, 2010 2:47pm.  
Name: Nathan Blair.  
IP Address: [REDACTED]  
MAC Address: [REDACTED] (b)(2)  
Property Number: 940819  
Browser Used: Firefox or Chrome - Cleared Both.  
O/S: Windows XP.

1. Check if the above information matches the information on the user's PC. Yes.
2. Did you go to the web site: Not Aware
3. How did you access the site: Not Aware
4. Clear the cache: Done
5. Clear the history: Done
6. Clear temporary files: All But 2
7. Clear local copies of docs downloaded, such as "Page as" copies Done

8. Did the user store any downloaded files elsewhere? No

9. Detail where the information was stored below. N/A

10. Was any of the information forwarded to other people? N/A  
(i.e. Email, IM)

11. Detail what information was forwarded, and where it went. N/A.

12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks.

Done. Running 12/9/10

13. Sanitize or destroy any mobile media or backup storage used

14. Remove SIIRT tools (after #12 is complete) - Eraser: <http://eraser.heidi.ie/>

12/10/10 - 10:22am (RS)

Date and Time: Dec 14, 2010 5pm.

Name: 818mr1

IP Address: [REDACTED]

MAC Address: [REDACTED] (b)(2)

Property Number: 933199

Browser Used: IE

O/S: Windows XP

1. Check if the above information matches the information on the user's PC.

2. Did you go to the web site: No, only attempted

3. How did you access the site: "

4. Clear the cache: Done

5. Clear the history: Done

6. Clear temporary files: Done

7. Clear local copies of docs downloaded, such as "Page as" copies Done

8. Did the user store any downloaded files elsewhere? No

9. Detail where the information was stored below. N/A

10. Was any of the information forwarded to other people? N/A  
(i.e. Email, IM)

11. Detail what information was forwarded, and where it went. N/A

12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks. N/A

Running 12/14/10

13. Sanitize or destroy any mobile media or backup storage used

14. Remove SIIRT tools (after #12 is complete) – Eraser: <http://eraser.heidi.ie/>

Complete  
12/16/10  
Sam JTB.

## Moses, Sandranette

---

**From:** Moses, Sandranette  
**Sent:** Thursday, December 02, 2010 11:27 AM  
**To:** Clark, Roger  
**Subject:** RE: Did you get a name for Chicago yet??

Roger,

(S)(2)

(S)(2)

Sorry! I thought I sent it. The user is [REDACTED] for the machine in Chicago, the machine name is [REDACTED],

Thank you,

Sandranette Moses  
IT Specialist - Programmer Analyst  
EDA IT Security Officer  
DOC - Economic Development Administration  
Office of Information Technology  
(202) 482- 2463

---

**From:** Clark, Roger [<mailto:RClark@doc.gov>]  
**Sent:** Thursday, December 02, 2010 10:07 AM  
**To:** Moses, Sandranette  
**Subject:** Did you get a name for Chicago yet??

v/r  
Roger Clark  
Senior Advisor  
National & Cyber Security  
Office of the Chief Information Officer  
U.S. Department of Commerce  
Phone: (202) 482-0121  
Email: [rclark@doc.gov](mailto:rclark@doc.gov)

PW

(b)(5)

DIP

Requester

## Moses, Sandranette

---

**From:** Clark, Roger [RClark@doc.gov]  
**Sent:** Wednesday, December 01, 2010 1:34 PM  
**To:** Moses, Sandranette  
**Cc:** Ahrnsbrak, Darice  
**Subject:** RE: WikiLeaks Issue

Just talked to Jon – the IP address we are looking for is (b)(2) not (b)(2) Sorry for the confusion.

---

**From:** Moses, Sandranette [mailto:SMoses@eda.doc.gov]  
**Sent:** Wednesday, December 01, 2010 1:19 PM  
**To:** Clark, Roger  
**Cc:** Ahrnsbrak, Darice  
**Subject:** RE: WikiLeaks Issue

Roger,

We have the hard drive of the user below. ... The status of the other IP address is that it is the network address (router address) for that region. We are trying to determine why this is being seen accessing the site not a desktop/server. We have to talk more with Jonathan in NOC (HCHB Net Administrator) unless you have more information on the IP address that can further help.

Thank you,

Sandranette Moses  
IT Specialist - Programmer Analyst  
EDA IT Security Officer  
DOC - Economic Development Administration  
Office of Information Technology  
(202) 482- 2463

---

**From:** Clark, Roger [mailto:RClark@doc.gov]  
**Sent:** Tuesday, November 30, 2010 4:30 PM  
**To:** Moses, Sandranette  
**Cc:** Ahrnsbrak, Darice  
**Subject:** RE: WikiLeaks Issue

Thank you.

NR

NR

**Clark, Roger**

---

**From:** Clark, Roger  
**Sent:** Wednesday, December 01, 2010 1:34 PM  
**To:** Moses, Sandranette  
**Cc:** Ahrensbrak, Darice  
**Subject:** RE: WikiLeaks Issue

Just talked to Jon – the IP address we are looking for is [REDACTED] not [REDACTED] Sorry for the confusion.

**From:** Moses, Sandranette [<mailto:SMoses@eda.doc.gov>]  
**Sent:** Wednesday, December 01, 2010 1:19 PM  
**To:** Clark, Roger  
**Cc:** Ahrensbrak, Darice  
**Subject:** RE: WikiLeaks Issue

Roger,

We have the hard drive of the user below. ... The status of the other IP address is that it is the network address (router address) for that region. We are trying to determine why this is being seen accessing the site not a desktop/server. We have to talk more with Jonathan in NOC (HCHB Net Administrator) unless you have more information on the IP address that can further help.

Thank you,

Sandranette Moses  
IT Specialist - Programmer Analyst  
EDA IT Security Officer  
DOC - Economic Development Administration  
Office of Information Technology  
(202) 482- 2463

**From:** Clark, Roger [<mailto:RClark@doc.gov>]  
**Sent:** Tuesday, November 30, 2010 4:30 PM  
**To:** Moses, Sandranette  
**Cc:** Ahrensbrak, Darice  
**Subject:** RE: WikiLeaks Issue

Thank you.

[REDACTED] NR

[REDACTED] NR

[REDACTED] NR

## Moses, Sandranette

---

**From:** Moses, Sandranette  
**Sent:** Wednesday, December 01, 2010 1:35 PM  
**To:** Clark, Roger  
**Subject:** RE: WikiLeaks Issue

No problem.

Sandranette Moses  
IT Specialist - Programmer Analyst  
EDA IT Security Officer  
DOC - Economic Development Administration  
Office of Information Technology  
(202) 482- 2463

---

**From:** Clark, Roger [<mailto:RClark@doc.gov>]  
**Sent:** Wednesday, December 01, 2010 1:34 PM  
**To:** Moses, Sandranette  
**Cc:** Ahrnsbrak, Darice  
**Subject:** RE: WikiLeaks Issue

Just talked to Jon – the IP address we are looking for is [REDACTED] not [REDACTED] Sorry for the confusion.

---

**From:** Moses, Sandranette [<mailto:SMoses@eda.doc.gov>]  
**Sent:** Wednesday, December 01, 2010 1:19 PM  
**To:** Clark, Roger  
**Cc:** Ahrnsbrak, Darice  
**Subject:** RE: WikiLeaks Issue

Roger,

We have the hard drive of the user below. ... The status of the other IP address is that it is the network address (router address) for that region. We are trying to determine why this is being seen accessing the site not a desktop/server. We have to talk more with Jonathan in NOC (HCHB Net Administrator) unless you have more information on the IP address that can further help.

Thank you,

Sandranette Moses  
IT Specialist - Programmer Analyst  
EDA IT Security Officer  
DOC - Economic Development Administration  
Office of Information Technology  
(202) 482- 2463

---

**From:** Clark, Roger [<mailto:RClark@doc.gov>]  
**Sent:** Tuesday, November 30, 2010 4:30 PM  
**To:** Moses, Sandranette  
**Cc:** Ahrnsbrak, Darice  
**Subject:** RE: WikiLeaks Issue

Thank you.

**Clark, Roger**

---

**From:** Moses, Sandranette [SMoses@eda.doc.gov]  
**Sent:** Wednesday, December 01, 2010 1:35 PM  
**To:** Clark, Roger  
**Subject:** RE: WikiLeaks Issue

No problem.

Sandranette Moses  
IT Specialist - Programmer Analyst  
EDA IT Security Officer  
DOC - Economic Development Administration  
Office of Information Technology  
(202) 482- 2463

**From:** Clark, Roger [mailto:RClark@doc.gov]  
**Sent:** Wednesday, December 01, 2010 1:34 PM  
**To:** Moses, Sandranette  
**Cc:** Ahrnsbrak, Darice  
**Subject:** RE: WikiLeaks Issue

Just talked to Jon – the IP address we are looking for is [REDACTED] not [REDACTED] Sorry for the confusion.

**From:** Moses, Sandranette [mailto:SMoses@eda.doc.gov]  
**Sent:** Wednesday, December 01, 2010 1:19 PM  
**To:** Clark, Roger  
**Cc:** Ahrnsbrak, Darice  
**Subject:** RE: WikiLeaks Issue

Roger,

We have the hard drive of the user below. ... The status of the other IP address is that it is the network address (router address) for that region. We are trying to determine why this is being seen accessing the site not a desktop/server. We have to talk more with Jonathan in NOC (HCHB Net Administrator) unless you have more information on the IP address that can further help.

Thank you,

Sandranette Moses  
IT Specialist - Programmer Analyst  
EDA IT Security Officer  
DOC - Economic Development Administration  
Office of Information Technology  
(202) 482- 2463

**From:** Clark, Roger [mailto:RClark@doc.gov]  
**Sent:** Tuesday, November 30, 2010 4:30 PM  
**To:** Moses, Sandranette  
**Cc:** Ahrnsbrak, Darice  
**Subject:** RE: WikiLeaks Issue

Thank you.

[REDACTED] MR



[REDACTED]

NR

[REDACTED]

[REDACTED]

NR

## Moses, Sandranette

---

**From:** Clark, Roger [RClark@doc.gov]  
**Sent:** Wednesday, December 01, 2010 1:34 PM  
**To:** Moses, Sandranette  
**Cc:** Ahrnsbrak, Darice  
**Subject:** RE: WikiLeaks Issue

(S)(2)

Just talked to Jon – the IP address we are looking for is [REDACTED] not [REDACTED]. Sorry for the confusion.

---

**From:** Moses, Sandranette [mailto:SMoses@eda.doc.gov]  
**Sent:** Wednesday, December 01, 2010 1:19 PM  
**To:** Clark, Roger  
**Cc:** Ahrnsbrak, Darice  
**Subject:** RE: WikiLeaks Issue

Roger,

We have the hard drive of the user below. ... The status of the other IP address is that it is the network address (router address) for that region. We are trying to determine why this is being seen accessing the site not a desktop/server. We have to talk more with Jonathan in NOC (HCHB Net Administrator) unless you have more information on the IP address that can further help.

Thank you,

Sandranette Moses  
IT Specialist - Programmer Analyst  
EDA IT Security Officer  
DOC - Economic Development Administration  
Office of Information Technology  
(202) 482- 2463

---

**From:** Clark, Roger [mailto:RClark@doc.gov]  
**Sent:** Tuesday, November 30, 2010 4:30 PM  
**To:** Moses, Sandranette  
**Cc:** Ahrnsbrak, Darice  
**Subject:** RE: WikiLeaks Issue

Thank you.

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

*Not Responsive*

[REDACTED]

[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]

## Moses, Sandranette

---

**From:** Moses, Sandranette  
**Sent:** Wednesday, December 01, 2010 1:35 PM  
**To:** Clark, Roger  
**Subject:** RE: WikiLeaks Issue

No problem.

Sandranette Moses  
IT Specialist - Programmer Analyst  
EDA IT Security Officer  
DOC - Economic Development Administration  
Office of Information Technology  
(202) 482- 2463

**From:** Clark, Roger [<mailto:RClark@doc.gov>]  
**Sent:** Wednesday, December 01, 2010 1:34 PM  
**To:** Moses, Sandranette  
**Cc:** Ahrnsbrak, Darice  
**Subject:** RE: WikiLeaks Issue

(S)(2)

Just talked to Jon – the IP address we are looking for is [REDACTED] not [REDACTED] Sorry for the confusion.

---

**From:** Moses, Sandranette [<mailto:SMoses@eda.doc.gov>]  
**Sent:** Wednesday, December 01, 2010 1:19 PM  
**To:** Clark, Roger  
**Cc:** Ahrnsbrak, Darice  
**Subject:** RE: WikiLeaks Issue

Roger,

We have the hard drive of the user below. ... The status of the other IP address is that it is the network address (router address) for that region. We are trying to determine why this is being seen accessing the site not a desktop/server. We have to talk more with Jonathan in NOC (HCHB Net Administrator) unless you have more information on the IP address that can further help.

Thank you,

Sandranette Moses  
IT Specialist - Programmer Analyst  
EDA IT Security Officer  
DOC - Economic Development Administration  
Office of Information Technology  
(202) 482- 2463

[REDACTED]

*Not Responsive*

[REDACTED]

[REDACTED]

PW

(b)(5)

DIP

Requester

**Clark, Roger**

---

**From:** Clark, Roger  
**Sent:** Wednesday, December 01, 2010 11:27 AM  
**To:** Casias, Lisa  
**Subject:** Re: Guidance regarding WikiLeaks

We have but some folks beat is to the punch.

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

**From:** Casias, Lisa  
**To:** Clark, Roger  
**Sent:** Wed Dec 01 11:24:01 2010  
**Subject:** FW: Guidance regarding Wikileaks

Why wouldn't you just block the website so the those on our network can't get on the site?

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

**From:** Broadcast, DOC  
**Sent:** Wednesday, December 01, 2010 10:57 AM  
**To:** Broadcast, DOC  
**Subject:** Guidance regarding Wikileaks

**To:** All Commerce Employees and Contractors

Recent reports indicate that a number of government documents have been posted on the WikiLeaks website. These documents may or may not contain information that is considered National Security Information (classified information) and as such, the information is NOT authorized for downloading, viewing, printing, processing, copying, or transmitting via non-classified Government-issued computers, laptops, blackberries, or other communication devices and is not an authorized use of DOC IT equipment. Doing so would introduce potentially classified information onto our unclassified networks and represent a potential security incident.

There has been a rumor that the information is no longer classified since it resides in the public domain. This is NOT true. Executive Order 13526, Section I.1(4)(2) states "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information." The information was neither properly nor improperly "declassified" by the appropriate authority and requires continued classification or reclassification.

Please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents because these documents may contain classified information. Accessing the Wikileaks documents will lead to sanitization of your PC to remove any potentially classified information from the system and result in possible data loss.

If you have questions regarding this broadcast or have accessed the Wikileaks documents, please contact the DOC Computer Incident Response Team at email [doc-cirt@doc.gov](mailto:doc-cirt@doc.gov) or call (202) 482-4000.

---

This message was authorized by the Office of Secretary OSY/OCIO.

Please do not reply to this message. The broadcast email account is not monitored for incoming mail.

**This Page**  
**is**  
**being withheld**  
**under**  
**(b)(5)**  
**pre-decisional/deliberative process**  
**privilege**

PW

(b)(5);(b)(6) &  
DTP

WNR



Requester's CC

**Dahl, Scott**

---

**From:** Dahl, Scott  
**Sent:** Thursday, December 02, 2010 8:00 AM  
**To:** Zinser, Todd  
**Subject:** FW: Updated Talking Points for the EMT Meeting  
**Attachments:** Talking Points for EMT - December-2-2010.docx

**Importance:** High

(b) (5) [REDACTED] I assume that [REDACTED] would raise.

not responsive

[REDACTED]

Speaking of Wikileaks, I think it would behoove us to send out a notice to employees to remind them to be extremely cautious websites they visit and point out the Wikileaks incident as an example of an OIG employee whose computer had to be checked and wiped to ensure that no classified information had been downloaded.

**From:** [REDACTED]  
**Sent:** Thursday, December 02, 2010 6:38 AM  
**To:** Zinser, Todd  
**Cc:** Dahl, Scott; Leiphart, Kristine  
**Subject:** Updated Talking Points for the EMT Meeting  
**Importance:** High

Good Morning Todd,

Attached are the revised talking points for this morning EMT meeting showing the number of DOC employees accessing the WIKI site.

[REDACTED]

[REDACTED]

*Office of Administration*  
*Office of Inspector General*  
(202) 482-[REDACTED]  
(202) 501-[REDACTED] (Fax)



all redactions (b) (6) unless otherwise indicated

**Dahl, Scott**

---

**From:** Dahl, Scott  
**Sent:** Thursday, December 02, 2010 8:13 AM  
**To:** Zinser, Todd  
**Subject:** RE: Updated Talking Points for the EMT Meeting

I see – not TPs, but just head knowledge.

not responsive

**From:** Zinser, Todd  
**Sent:** Thursday, December 02, 2010 8:04 AM  
**To:** Dahl, Scott  
**Subject:** RE: Updated Talking Points for the EMT Meeting

Yes. [REDACTED] is on the agenda to address the IT Security issue which I presume is the Wikileaks issue. I took the info from [REDACTED] as letting me know what can be expected to be discussed and where our infraction stands in the scheme of things. [REDACTED] (b) (5)

PW

(b)(6) & (b)(5)  
D/P

Requester

**Bergersen, Benjamin**

---

**From:** Bergersen, Benjamin  
**Sent:** Thursday, December 02, 2010 11:09 AM  
**To:** [REDACTED]  
**Cc:** Bergersen, Benjamin  
**Subject:** Re: \\\FOUO \\\ IT Services Notice - Wikileaks Potentially Classified Documents. Gentle reminder of Viruses, and Security - a cautionary tale - \\\FOUO \\\

[REDACTED]  
Specific details of what has happened to OIG computers is FOUO, and the numbers of computers.

Parts of the message are public, parts are FOUO.

(b) (5) Also... [REDACTED] - see the OSY's attached memo.

Ben  
Benjamin Bergersen  
Chief Information Officer

Office of Inspector General  
U.S. Commerce Department  
202-482-0611 Main Office  
[benjamin.bergersen@oig.doc.gov](mailto:benjamin.bergersen@oig.doc.gov)

---

**From:** [REDACTED]  
**To:** Bergersen, Benjamin  
**Sent:** Thu Dec 02 11:04:06 2010  
**Subject:** RE: \\\FOUO \\\ IT Services Notice - Wikileaks Potentially Classified Documents. Gentle reminder of Viruses, and Security - a cautionary tale - \\\FOUO \\\

Is "do not distribute outside OIG" because Atlantic magazine and other sources reprinted yesterday's email from the Secretary?

**From:** Bergersen, Benjamin  
**Sent:** Thursday, December 02, 2010 11:03 AM  
**To:** OIG All Employees; OIG Help Desk  
**Subject:** \\\FOUO \\\ IT Services Notice - Wikileaks Potentially Classified Documents. Gentle reminder of Viruses, and Security - a cautionary tale - \\\FOUO \\\  
**Importance:** High

...FOR OFFICIAL USE ONLY....DO NOT DISTRIBUTE OUTSIDE  
OIG...

# IT SERVICES NOTICE

## WHAT IS HAPPENING

There is potentially classified materials on the WikiLeaks web site that Commerce personnel have attempted to view from unclassified computers. This has resulted in dozens of computers DOC wide needing to be wiped by security personnel, including one PC from the OIG. This is a cautionary tale of the OIG person who had to have their computer formatted, and then returned. Don't let it happen to you.

The Department of Commerce is forbidding people to access the Wikileaks web site because our IT systems are not cleared to view, transmit, or store potentially classified documents. (National security classified documents such as "secret", "top secret", or higher.)

Your computer will be confiscated, the hard drive removed, and the drive wiped by OIG personnel with the requisite security clearances.

See attached memo from the Office of the Secretary.

## WHAT THIS MEANS TO YOU

- ✓ Do not attempt to access Wikileaks as you may be accessing potentially classified information above your computer

systems clearance level, above your clearance level, and without a “need to know”.

- ✓ Only access that site if you have an official work order from your supervisor, have the personal security clearance level, have an official “need to know” – not just curiosity, and you are operating from a properly classified area. (This is generally “secret” and “top secret” investigations and audits.)
- ✓ The same formatting of your computer and loss of productivity can occur if you access a potentially bad web site with viruses or worms. The DOC and OIG IT security systems are not full-proof. Use common sense. Stay away from bad web sites that may have viruses, unauthorized PII, unauthorized classified material, or worms.

## QUESTIONS

For additional information or assistance please call the OIG OCIO Helpdesk at (202) 482-1238 or send us an e-mail at [helpdesk@oig.doc.gov](mailto:helpdesk@oig.doc.gov)

Warm Regards,

Ben

Benjamin Bergersen

Chief Information Officer

Office of Inspector General  
U.S. Department of Commerce  
202-482-0611 main office  
[Benjamin.Bergersen@oig.doc.gov](mailto:Benjamin.Bergersen@oig.doc.gov)

...FOR OFFICIAL USE ONLY....DO NOT DISTRIBUTE OUTSIDE  
OIG...

PW

(b)(6) & (b)(5)

A/c

2

Requester's CC

(b) (6)

---

**From:** Dahl, Scott  
**Sent:** Thursday, December 02, 2010, 10:08 AM  
**To:** Green, Wade (b) (6)  
**Subject:** FW: WikiLeaks incident

(b) (5)

---

**From:** Dahl, Scott  
**Sent:** Thursday, December 02, 2010 10:07 AM  
**To:** Leiphart, Kristine  
**Cc:** Bergersen, Benjamin  
**Subject:** WikiLeaks incident

What do you think about sending out to our workforce a reminder to be cautious about what websites they visit on their work computers. There is an every-growing risk of contracting viruses that could infect their and others computers. In addition, we could mention the WikiLeaks incident as an example where visiting a website resulted in one of our computers having to be taken offline and wiped because of concern that classified information on the website may have been downloaded on the employee's computer. I just think it is a cautionary tale that would serve as a beneficial reminder.

Scott S. Dahl  
Deputy Inspector General  
U.S. Department of Commerce  
1401 Constitution Avenue, NW  
Room 7898C  
Washington, DC 20230  
(202) 482-4899



all redactions (b) (6) unless otherwise indicated

[REDACTED]  

---

**From:** [REDACTED]  
**Sent:** Thursday, December 02, 2010 10:21 AM  
**To:** Dahl, Scott  
**Cc:** [REDACTED]  
**Subject:** RE: WikiLeaks incident

(b) (5)

[REDACTED]  
  
[REDACTED]  
  
U.S. Department of Commerce  
Office of Inspector General  
[REDACTED]@oig.doc.gov

\*\*\*\*\*  
The information in this email may be confidential and/or privileged and exempt from disclosure under applicable law. This email is intended to be reviewed only by the individual(s) or organization(s) named above. Do not share, copy or forward without consulting the Office of Counsel. If you are not the intended recipient or an authorized representative of the intended recipient, you are hereby notified that any review, dissemination or copying of this email and its attachments, if any, or the information contained herein is prohibited. If you have received this email in error, please immediately notify the sender by return email and delete this email from your system(s). The Office of Inspector General reserves the right to monitor any communication that is created, received or sent on its network(s).

---

**From:** Dahl, Scott  
**Sent:** Thursday, December 02, 2010 9:08 AM  
**To:** Green, Wade; [REDACTED]  
**Subject:** FW: WikiLeaks incident

[REDACTED] (b) (5)

---

**From:** Dahl, Scott  
**Sent:** Thursday, December 02, 2010 10:07 AM  
**To:** Leiphart, Kristine  
**Cc:** Bergersen, Benjamin  
**Subject:** WikiLeaks incident

What do you think about sending out to our workforce a reminder to be cautious about what websites they visit on their work computers. There is an every-growing risk of contracting viruses that could infect their and others computers. In addition, we could mention the WikiLeaks incident as an example where visiting a website resulted in one of our computers having to be taken offline and wiped because of concern that classified information on the website may have been downloaded on the employee's computer. I just think it is a cautionary tale that would serve as a beneficial reminder.

Scott S. Dahl  
Deputy Inspector General  
U.S. Department of Commerce  
1401 Constitution Avenue, NW  
Room 7898C  
Washington, DC 20230

(202) 482-4899

PW

(b)(4) & NR

Requester's cc

[REDACTED]

---

**From:** [REDACTED]  
**Sent:** Wednesday, December 01, 2010 6:42 AM  
**To:** Leiphart, Kristine; [REDACTED]  
**Cc:** [REDACTED]; Webb, John; McDonnell, Kerry; Bergersen, Benjamin  
**Subject:** Re: It security info need for Thurs EMT meeting

Will do.

---

**From:** Leiphart, Kristine  
**To:** [REDACTED]; [REDACTED]  
**Cc:** [REDACTED]; Webb, John; McDonnell, Kerry; Bergersen, Benjamin  
**Sent:** Tue Nov 30 22:07:30 2010  
**Subject:** It security info need for Thurs EMT meeting

[REDACTED]—Can you please find out how many bureaus and how many people have tried to access the classified WIKI site or any classified sites in the past month? The IT security issue is item #3 on the EMT agenda for Thursday (see attached) and I would like Todd to be equipped with this information. Please cc [REDACTED] on the answer as [REDACTED] is preparing talking points for Todd. Thanks.

[REDACTED]—We need a few talking points for Todd's EMT meeting occurring on Thursday (e.g., reports issued, if any—  
[REDACTED] was supposed to collect that info so please touch base with [REDACTED]. [REDACTED]

not responsive

not  
responsive

Kristine

[REDACTED]

---

**From:** [REDACTED]  
**Sent:** Wednesday, December 01, 2010 6:42 AM  
**To:** Leiphart, Kristine; [REDACTED]  
**Cc:** [REDACTED]; Webb, John; McDonnell, Kerry; Bergersen, Benjamin  
**Subject:** Re: It security info need for Thurs EMT meeting

Will do.

---

**From:** Leiphart, Kristine  
**To:** [REDACTED]; [REDACTED]  
**Cc:** [REDACTED]; Webb, John; McDonnell, Kerry; Bergersen, Benjamin  
**Sent:** Tue Nov 30 22:07:30 2010  
**Subject:** It security info need for Thurs EMT meeting

[REDACTED]—Can you please find out how many bureaus and how many people have tried to access the classified WIKI site or any classified sites in the past month? The IT security issue is item #3 on the EMT agenda for Thursday (see attached) and I would like Todd to be equipped with this information. Please cc [REDACTED] on the answer as [REDACTED] is preparing talking points for Todd. Thanks.

[REDACTED]—We need a few talking points for Todd's EMT meeting occurring on Thursday (e.g., reports issued, if any—  
[REDACTED] was supposed to collect that info so please touch base with [REDACTED]. [REDACTED]

not  
responsive

not  
responsive

Kristine

**Webb, John**

---

**From:** [REDACTED]  
**Sent:** Wednesday, December 01, 2010 4:49 PM  
**To:** Leiphart, Kristine; [REDACTED]  
**Cc:** [REDACTED]; Webb, John; McDonnell, Kerry; Bergersen, Benjamin; [REDACTED]  
**Subject:** Re: It security info need for Thurs EMT meeting

See info below from [REDACTED]  
[REDACTED]

refer to  
Dept

In response to your request, the following information is provided. It should be noted that the information does not cover the 1 month period requested and only dates back to Friday, Nov 26th. Additionally, the numbers are preliminary and the bureaus are continuing to validate these numbers.

OS – 4 users

BIS – 1 user

EDA – 2 users

OIG – 1 user

Credit Union – 1 user

Census – 19 users

USPTO – 22 users

NTIS – 3 users

BEA – 9 users

NIST – 15 users

ITA – 15 users

NOAA -- # pending

All bureaus have reported successfully blocking access to the site as of 9 p.m., Nov 30th.

Updated info –

TA has identified additional users – total now 24, 20 within US and 4 outside US.

Roger

**From:** Leiphart, Kristine

**To:** [REDACTED]; [REDACTED]

all responsive redactions (b) (6)

**Cc:** [REDACTED]; Webb, John; McDonnell, Kerry; Bergersen, Benjamin

**Sent:** Tue Nov 30 22:07:30 2010

**Subject:** It security info need for Thurs EMT meeting

[REDACTED]—Can you please find out how many bureaus and how many people have tried to access the classified WIKI site or any classified sites in the past month? The IT security issue is item #3 on the EMT agenda for Thursday (see attached) and I would like Todd to be equipped with this information. Please cc [REDACTED] on the answer as [REDACTED] is preparing talking points for Todd. Thanks.

[REDACTED]—We need a few talking points for Todd's EMT meeting occurring on Thursday (e.g., reports issued, if any—  
[REDACTED] was supposed to collect that info so please touch base with [REDACTED].

not  
responsive

not  
responsive

Kristine

Bergersen, Benjamin

---

From: [REDACTED]  
Sent: Wednesday, December 01, 2010 4:49 PM  
To: Leiphart, Kristine; [REDACTED]  
Cc: [REDACTED]; Webb, John; McDonnell, Kerry; Bergersen, Benjamin; [REDACTED]  
Subject: Re: It security info need for Thurs EMT meeting

See info below from [REDACTED]  
[REDACTED]

Refer to  
Dept.

In response to your request, the following information is provided. It should be noted that the information does not cover the 1 month period requested and only dates back to Friday, Nov 26th. Additionally, the numbers are preliminary and the bureaus are continuing to validate these numbers.

OS – 4 users

BIS – 1 user

EDA – 2 users

OIG – 1 user

Credit Union – 1 user

Census – 19 users

USPTO – 22 users

NTIS – 3 users

BEA – 9 users

NIST – 15 users

ITA – 15 users

NOAA -- # pending

All bureaus have reported successfully blocking access to the site as of 9 p.m., Nov 30th.

Updated info –

ITA has identified additional users – total now 24, 20 within US and 4 outside US.

Roger

---

From: Leiphart, Kristine

To: [REDACTED]; [REDACTED]



all responsive redactions (b) (6)

**Cc:** [REDACTED]; Webb, John; McDonnell, Kerry; Bergersen, Benjamin

**Sent:** Tue Nov 30 22:07:30 2010

**Subject:** It security info need for Thurs EMT meeting

[REDACTED]—Can you please find out how many bureaus and how many people have tried to access the classified WIKI site or any classified sites in the past month? The IT security issue is item #3 on the EMT agenda for Thursday (see attached) and I would like Todd to be equipped with this information. Please cc [REDACTED] on the answer as [REDACTED] is preparing talking points for Todd. Thanks.

[REDACTED]—We need a few talking points for Todd's EMT meeting occurring on Thursday (e.g., reports issued, if any—  
Melinda was supposed to collect that info so please touch base with [REDACTED]

not responsive

not responsive

Kristine

**McDonnell, Kerry**

---

**From:** [REDACTED]  
**Sent:** Wednesday, December 01, 2010 4:49 PM  
**To:** Leiphart, Kristine; [REDACTED]  
**Cc:** [REDACTED]; Webb, John; McDonnell, Kerry; Bergersen, Benjamin; [REDACTED]  
**Subject:** Re: It security info need for Thurs EMT meeting

See info below from [REDACTED]

refer to Dept In response to your request, the following information is provided. It should be noted that the information does not cover the 1 month period requested and only dates back to Friday, Nov 26th. Additionally, the numbers are preliminary and the bureaus are continuing to validate these numbers.

OS – 4 users  
BIS – 1 user  
EDA – 2 users  
OIG – 1 user  
Credit Union – 1 user  
Census – 19 users  
USPTO – 22 users  
NTIS – 3 users  
BEA – 9 users  
NIST – 15 users  
ITA – 15 users  
NOAA -- # pending

All bureaus have reported successfully blocking access to the site as of 9 p.m., Nov 30th.

Updated info –

ITA has identified additional users – total now 24, 20 within US and 4 outside US.

Roger

**From:** Leiphart, Kristine

**To:** [REDACTED]; [REDACTED]

all responsive redactions (b) (6)

**Cc:** [REDACTED]; Webb, John; McDonnell, Kerry; Bergersen, Benjamin  
**Sent:** Tue Nov 30 22:07:30 2010  
**Subject:** It security info need for Thurs EMT meeting

[REDACTED]—Can you please find out how many bureaus and how many people have tried to access the classified WIKI site or any classified sites in the past month? The IT security issue is item #3 on the EMT agenda for Thursday (see attached) and I would like Todd to be equipped with this information. Please cc [REDACTED] on the answer as [REDACTED] is preparing talking points for Todd. Thanks.

[REDACTED]—We need a few talking points for Todd's EMT meeting occurring on Thursday (e.g., reports issued, if any—  
[REDACTED] was supposed to collect that info so please touch base with [REDACTED]. [REDACTED] not responsive

[REDACTED] not responsive

Kristine

**Webb, John**

---

**From:** [REDACTED]  
**Sent:** Wednesday, December 01, 2010 5:48 PM  
**To:** Leiphart, Kristine; [REDACTED]  
**Cc:** [REDACTED] Webb, John; McDonnell, Kerry; Bergersen, Benjamin; [REDACTED]  
**Subject:** Re: It security info need for Thurs EMT meeting

One more update

refer to  
Dept

NOAA – 80 users -- still reviewing logs

**From:** [REDACTED]  
**To:** Leiphart, Kristine; [REDACTED]  
**Cc:** [REDACTED] Webb, John; McDonnell, Kerry; Bergersen, Benjamin; [REDACTED]  
**Sent:** Wed Dec 01 16:48:45 2010  
**Subject:** Re: It security info need for Thurs EMT meeting

See info below from [REDACTED]

refer to  
Dept

In response to your request, the following information is provided. It should be noted that the information does not cover the 1 month period requested and only dates back to Friday, Nov 26th. Additionally, the numbers are preliminary and the bureaus are continuing to validate these numbers.

OS – 4 users

BIS – 1 user

EDA – 2 users

OIG – 1 user

Credit Union – 1 user

Census – 19 users

USPTO – 22 users

NTIS – 3 users

BEA – 9 users

NIST – 15 users

ITA – 15 users

NOAA -- # pending

refer to  
Dept All bureaus have reported successfully blocking access to the site as of 9 p.m., Nov 30th.

Updated info –

ITA has identified additional users – total now 24, 20 within US and 4 outside US.

Roger

**From:** Leiphart, Kristine

**To:** [REDACTED]; [REDACTED]

**Cc:** [REDACTED]; Webb, John; McDonnell, Kerry; Bergersen, Benjamin

**Sent:** Tue Nov 30 22:07:30 2010

**Subject:** IT security info need for Thurs EMT meeting

[REDACTED]—Can you please find out how many bureaus and how many people have tried to access the classified WIKI site or any classified sites in the past month? The IT security issue is item #3 on the EMT agenda for Thursday (see attached) and I would like Todd to be equipped with this information. Please cc [REDACTED] on the answer as [REDACTED] is preparing talking points for Todd. Thanks.

[REDACTED]—We need a few talking points for Todd's EMT meeting occurring on Thursday (e.g., reports issued, if any—

[REDACTED] was supposed to collect that info so please touch base with [REDACTED]). [REDACTED]

not responsive

not  
responsive

Kristine

[REDACTED]

---

**From:** Thompson, Gwendolyn  
**Sent:** Wednesday, December 01, 2010 5:48 PM  
**To:** Leiphart, Kristine; [REDACTED]  
**Cc:** [REDACTED]; Webb, John; McDonnell, Kerry; Bergersen, Benjamin; [REDACTED]  
**Subject:** Re: It security info need for Thurs EMT meeting

One more update

refer to  
Dept | NOAA – 80 users -- still reviewing logs

---

**From:** [REDACTED]  
**To:** Leiphart, Kristine; [REDACTED]  
**Cc:** [REDACTED]; Webb, John; McDonnell, Kerry; Bergersen, Benjamin; [REDACTED]  
**Sent:** Wed Dec 01 16:48:45 2010  
**Subject:** Re: It security info need for Thurs EMT meeting

See info below from [REDACTED]

[REDACTED]

refer to  
Dept | In response to your request, the following information is provided. It should be noted that the information does not cover the 1 month period requested and only dates back to Friday, Nov 26th. Additionally, the numbers are preliminary and the bureaus are continuing to validate these numbers.

OS – 4 users

BIS – 1 user

EDA – 2 users

OIG – 1 user

Credit Union – 1 user

Census – 19 users

USPTO – 22 users

NTIS – 3 users

BEA – 9 users

NIST – 15 users

ITA – 15 users

NOAA -- # pending

all responsive redactions (b) (6)

refer to  
Dept

All bureaus have reported successfully blocking access to the site as of 9 p.m., Nov 30th.

Updated info –

ITA has identified additional users – total now 24, 20 within US and 4 outside US.

Roger

---

**From:** Leiphart, Kristine

**To:** [REDACTED]; [REDACTED]

**Cc:** [REDACTED]; Webb, John; McDonnell, Kerry; Bergersen, Benjamin

**Sent:** Tue Nov 30 22:07:30 2010

**Subject:** It security info need for Thurs EMT meeting

[REDACTED]—Can you please find out how many bureaus and how many people have tried to access the classified WIKI site or any classified sites in the past month? The IT security issue is item #3 on the EMT agenda for Thursday (see attached) and I would like Todd to be equipped with this information. Please cc [REDACTED] on the answer as [REDACTED] is preparing talking points for Todd. Thanks.

[REDACTED]—We need a few talking points for Todd's EMT meeting occurring on Thursday (e.g., reports issued, if any—  
[REDACTED] was supposed to collect that info so please touch base with [REDACTED]). [REDACTED]

not  
responsive

not  
responsive

Kristine

**McDonnell, Kerry**

---

**From:** [REDACTED]  
**Sent:** Wednesday, December 01, 2010 5:48 PM  
**To:** Leiphart, Kristine; [REDACTED]  
**Cc:** [REDACTED] Webb, John; McDonnell, Kerry; Bergersen, Benjamin; [REDACTED]  
**Subject:** Re: It security info need for Thurs EMT meeting

One more update

refer  
to  
Dept

NOAA -- 80 users -- still reviewing logs

**From:** [REDACTED]  
**To:** Leiphart, Kristine; [REDACTED]  
**Cc:** [REDACTED] Webb, John; McDonnell, Kerry; Bergersen, Benjamin; [REDACTED]  
**Sent:** Wed Dec 01 16:48:45 2010  
**Subject:** Re: It security info need for Thurs EMT meeting

See info below from [REDACTED]

refer  
to  
Dept

In response to your request, the following information is provided. It should be noted that the information does not cover the 1 month period requested and only dates back to Friday, Nov 26th. Additionally, the numbers are preliminary and the bureaus are continuing to validate these numbers.

OS -- 4 users  
BIS -- 1 user  
EDA -- 2 users  
OIG -- 1 user  
Credit Union -- 1 user  
Census -- 19 users  
USPTO -- 22 users  
NTIS -- 3 users  
BEA -- 9 users  
NIST -- 15 users  
ITA -- 15 users  
NOAA -- # pending



refer to  
Dept All bureaus have reported successfully blocking access to the site as of 9 p.m., Nov 30th.

Updated info –

ITA has identified additional users – total now 24, 20 within US and 4 outside US.

Roger

**From:** Leiphart, Kristine

**To:** [REDACTED]; [REDACTED]

**Cc:** [REDACTED] Webb, John; McDonnell, Kerry; Bergersen, Benjamin

**Sent:** Tue Nov 30 22:07:30 2010

**Subject:** It security info need for Thurs EMT meeting

[REDACTED]—Can you please find out how many bureaus and how many people have tried to access the classified WIKI site or any classified sites in the past month? The IT security issue is item #3 on the EMT agenda for Thursday (see attached) and I would like Todd to be equipped with this information. Please cc [REDACTED] on the answer as [REDACTED] is preparing talking points for Todd. Thanks.

[REDACTED]—We need a few talking points for Todd's EMT meeting occurring on Thursday (e.g., reports issued, if any—  
[REDACTED] was supposed to collect that info so please touch base with [REDACTED]). [REDACTED]

not responsive

not  
responsive

Kristine

[REDACTED]

---

From: [REDACTED]  
Sent: Wednesday, December 01, 2010 5:48 PM  
To: Leiphart, Kristine; [REDACTED]  
Cc: [REDACTED]; Webb, John; McDonnell, Kerry; Bergersen, Benjamin; [REDACTED]  
Subject: Re: It security info need for Thurs EMT meeting

One more update

refer to  
Dept NOAA -- 80 users -- still reviewing logs

---

From: [REDACTED]  
To: Leiphart, Kristine; [REDACTED]  
Cc: [REDACTED]; Webb, John; McDonnell, Kerry; Bergersen, Benjamin; Thompson, [REDACTED]  
Sent: Wed Dec 01 16:48:45 2010  
Subject: Re: It security info need for Thurs EMT meeting

See info below from [REDACTED]

refer to  
Dept In response to your request, the following information is provided. It should be noted that the information does not cover the 1 month period requested and only dates back to Friday, Nov 26th. Additionally, the numbers are preliminary and the bureaus are continuing to validate these numbers.

OS -- 4 users

BIS -- 1 user

EDA -- 2 users

OIG -- 1 user

Credit Union -- 1 user

Census -- 19 users

USPTO -- 22 users

NTIS -- 3 users

BEA -- 9 users

NIST -- 15 users

ITA -- 15 users

NOAA -- # pending

refer to  
Dept

All bureaus have reported successfully blocking access to the site as of 9 p.m., Nov 30th.

Updated info –

ITA has identified additional users – total now 24, 20 within US and 4 outside US.

Roger

---

From: Leiphart, Kristine

To: [REDACTED]; [REDACTED]

Cc: [REDACTED]; Webb, John; McDonnell, Kerry; Bergersen, Benjamin

Sent: Tue Nov 30 22:07:30 2010

Subject: IT security info need for Thurs EMT meeting

[REDACTED] --Can you please find out how many bureaus and how many people have tried to access the classified WIKI site or any classified sites in the past month? The IT security issue is item #3 on the EMT agenda for Thursday (see attached) and I would like Todd to be equipped with this information. Please cc [REDACTED] on the answer as [REDACTED] is preparing talking points for Todd. Thanks.

[REDACTED] --We need a few talking points for Todd's EMT meeting occurring on Thursday (e.g., reports issued, if any—

[REDACTED] was supposed to collect that info so please touch base with [REDACTED]. [REDACTED]

not responsive

not  
responsive

Kristine

[REDACTED]

---

**From:** [REDACTED]  
**Sent:** Wednesday, December 01, 2010 5:48 PM  
**To:** Leiphart, Kristine; [REDACTED]  
**Cc:** [REDACTED]; Webb, John; McDonnell, Kerry; Bergersen, Benjamin; [REDACTED]  
**Subject:** Re: It security info need for Thurs EMT meeting

One more update

refer to  
Dept. | NOAA – 80 users – still reviewing logs

---

**From:** [REDACTED]  
**To:** Leiphart, Kristine; [REDACTED]  
**Cc:** [REDACTED]; Webb, John; McDonnell, Kerry; Bergersen, Benjamin; [REDACTED]  
**Sent:** Wed Dec 01 16:48:45 2010  
**Subject:** Re: It security info need for Thurs EMT meeting

See info below from [REDACTED]

refer to  
Dept. | In response to your request, the following information is provided. It should be noted that the information does not cover the 1 month period requested and only dates back to Friday, Nov 26th. Additionally, the numbers are preliminary and the bureaus are continuing to validate these numbers.

OS – 4 users

BIS – 1 user

EDA – 2 users

OIG – 1 user

Credit Union – 1 user

Census – 19 users

USPTO – 22 users

NTIS – 3 users

BEA – 9 users

NIST – 15 users

ITA – 15 users

NOAA – # pending

all responsive OIG redactions (b) (6)

refer to  
Dept.

All bureaus have reported successfully blocking access to the site as of 9 p.m., Nov 30th.

Updated info –

ITA has identified additional users – total now 24, 20 within US and 4 outside US.

Roger

---

**From:** Leiphart, Kristine

**To:** [REDACTED]; [REDACTED]

**Cc:** [REDACTED]; Webb, John; McDonnell, Kerry; Bergersen, Benjamin

**Sent:** Tue Nov 30 22:07:30 2010

**Subject:** IT security info need for Thurs EMT meeting

[REDACTED] –Can you please find out how many bureaus and how many people have tried to access the classified WIKI site or any classified sites in the past month? The IT security issue is item #3 on the EMT agenda for Thursday (see attached) and I would like Todd to be equipped with this information. Please cc [REDACTED] on the answer as she is preparing talking points for Todd. Thanks.

[REDACTED] –We need a few talking points for Todd's EMT meeting occurring on Thursday (e.g., reports issued, if any—  
[REDACTED] was supposed to collect that info so please touch base with [REDACTED].

not responsive

not  
responsive

Kristine

PW

(b)(u)

23

Requester's CC

Talking Points  
Executive Management Team Meeting  
Thursday, December 2, 2010

IT Security Update

refer to Dept

The number of employees who have tried to access the classified WIKI site or any classified sites from Friday, November 26 to present are as follows:

- OS – 4 users
- BIS – 1 user
- EDA – 2 users
- OIG – 1 user
- Census – 19 users
- PTO – 22 users
- NTIS – 3 users
- BEA – 9 users
- NIST – 15 users
- ITA – 15 users
- NOAA – 80 users (still reviewing logs)
- Credit Union – 1 user

Reports Issued This Week

all OIG redactions (b) (6)

[REDACTED]

---

**From:** [REDACTED]  
**Sent:** Friday, December 03, 2010 3:45 PM  
**To:** [REDACTED]  
**Cc:** [REDACTED]  
**Subject:** FW: Wikileaks DNS Change

**Importance:** High

Please see the email below for additional information that is needed in blocking scheme.

[REDACTED]

*Office of the Chief Information Officer  
Office of Inspector General  
U.S. Department of Commerce  
(202) 482-[REDACTED] office  
(202) 680-[REDACTED] cell  
(202) 501-[REDACTED] or (202) 482-[REDACTED] fax  
[REDACTED]@oig.doc.gov*

refer to  
Dept

**From:** members of the Federation of Department of Commerce CIRTs and CIRCs  
[mailto:FEDCIRT@LIST.COMMERCE.GOV] **On Behalf Of** Whiteside, Fred  
**Sent:** Friday, December 03, 2010 2:12 PM  
**To:** FEDCIRT@LIST.COMMERCE.GOV  
**Subject:** Re: Wikileaks DNS Change

Please include the following Wikileaks IP address in your blocking scheme

213.251.145.96

*Fred Whiteside, CIPP, CIPP/G  
Director, Cybersecurity Operations  
Office of Security, Infrastructure and Technology  
Office of the Chief Information Officer  
Department of Commerce  
202-482-4788 (o) 202-288-4671 (m)*

---

**From:** Whiteside, Fred  
**Sent:** Friday, December 03, 2010 1:35 PM  
**To:** (fedcirt@list.osec.doc.gov)  
**Subject:** Wikileaks DNS Change

Federation Team Members...

APR and CNN just announced Wikileaks has changed its DNS domain.



refer to  
Dept

It is now wikileaks.ch (a Swiss domain).

Please ensure your block lists are updated accordingly.

*Fred Whiteside, CIPP, CIPP/G  
Director, Cybersecurity Operations  
Office of Security, Infrastructure and Technology  
Office of the Chief Information Officer  
Department of Commerce  
202-482-4788 (o) 202-288-4671 (m)*

All redactions (b) (6)

[REDACTED]

---

From: [REDACTED]  
Sent: Friday, December 03, 2010 4:16 PM  
To: [REDACTED]  
Cc: [REDACTED]  
Subject: RE: Wikileaks DNS Change

I believe we rely on HCHB DNS for this; a nslookup of wikileaks.ch returns no IP so I think the HCHB DNS admins have already completed this task.

[REDACTED] General Dynamics Information Technology

Office of the Chief Information Officer  
Office of the Inspector General  
U.S. Department of Commerce  
202.482.1238 (Help Desk)  
202.482. [REDACTED] (Office)

From: [REDACTED]  
Sent: Friday, December 03, 2010 3:37 PM  
To: [REDACTED]  
Cc: [REDACTED]  
Subject: FW: Wikileaks DNS Change  
Importance: High

Please see [REDACTED] email below. Please let me know when it has been taken care of.

[REDACTED]

*Office of the Chief Information Officer  
Office of Inspector General  
U.S. Department of Commerce  
(202) 482- [REDACTED] office  
(202) 680- [REDACTED] cell  
(202) 501- [REDACTED] or (202) 482- [REDACTED] fax  
[REDACTED]@oig.doc.gov*

Refer to Dept. [REDACTED] From: members of the Federation of Department of Commerce CIRTs and CIRCs  
[mailto:FEDCIRT@LIST.COMMERCE.GOV] On Behalf Of Whiteside, Fred  
Sent: Friday, December 03, 2010 1:35 PM  
To: FEDCIRT@LIST.COMMERCE.GOV  
Subject: Wikileaks DNS Change

Federation Team Members...

APR and CNN just announced Wikileaks has changed its DNS domain.

Refer to Dept | It is now wikileaks.ch (a Swiss domain).

Please ensure your block lists are updated accordingly.

*Fred Whiteside, CIPP, CIPP/G  
Director, Cybersecurity Operations  
Office of Security, Infrastructure and Technology  
Office of the Chief Information Officer  
Department of Commerce  
202-482-4788 (o) 202-288-4671 (m)*

[REDACTED]  
From: [REDACTED]  
Sent: Friday, December 03, 2010 5:52 PM  
To: [REDACTED]  
Cc: [REDACTED]  
Subject: RE: Wikileaks DNS Change

Thanks [REDACTED]

[REDACTED]  
  
Office of the Chief Information Officer  
Office of Inspector General  
U.S. Department of Commerce  
(202) 482-[REDACTED] office  
(202) 680-[REDACTED] cell  
(202) 501-[REDACTED] or (202) 482-[REDACTED] fax  
[REDACTED]@oig.doc.gov

From: [REDACTED]  
Sent: Friday, December 03, 2010 4:16 PM  
To: [REDACTED]  
Cc: [REDACTED]  
Subject: RE: Wikileaks DNS Change

I believe we rely on HCHB DNS for this; a nslookup of wikileaks.ch returns no IP so I think the HCHB DNS admins have already completed this task.

[REDACTED] General Dynamics Information Technology  
  
Office of the Chief Information Officer  
Office of the Inspector General  
U.S. Department of Commerce  
202.482.[REDACTED] (Help Desk)  
202.482.[REDACTED] (Office)

From: [REDACTED]  
Sent: Friday, December 03, 2010 3:37 PM  
To: [REDACTED]  
Cc: [REDACTED]  
Subject: FW: Wikileaks DNS Change  
Importance: High

Please see [REDACTED] email below. Please let me know when it has been taken care of.

[REDACTED]

Office of the Chief Information Officer  
Office of Inspector General  
U.S. Department of Commerce  
(202) 482-[REDACTED] office  
(202) 680-[REDACTED] cell  
(202) 501-[REDACTED] or (202) 482-[REDACTED] fax  
[REDACTED]@oig.doc.gov

refer to Dept

**From:** members of the Federation of Department of Commerce CIRTs and CIRCs  
[mailto:FEDCIRT@LIST.COMMERCE.GOV] On Behalf Of Whiteside, Fred  
**Sent:** Friday, December 03, 2010 1:35 PM  
**To:** FEDCIRT@LIST.COMMERCE.GOV  
**Subject:** Wikileaks DNS Change

Federation Team Members...

APR and CNN just announced Wikileaks has changed its DNS domain.

It is now wikileaks.ch (a Swiss domain).

Please ensure your block lists are updated accordingly.

Fred Whiteside, CIPP, CIPP/G  
Director, Cybersecurity Operations  
Office of Security, Infrastructure and Technology  
Office of the Chief Information Officer  
Department of Commerce  
202-482-4788 (o) 202-288-4671 (m)

**Clark, Roger**

---

**From:** Alan Willard [AWillard@ntis.gov]  
**Sent:** Wednesday, December 01, 2010 12:38 PM  
**To:** DOC-CIRT  
**Cc:** Clark, Roger; Sinner, Keith  
**Subject:** NTIS Response - Wikileaks Site Block \*\*\*Situational Awareness\*\*\*

DOC-CIRT, Roger Clark;

NTIS identified 3 PC workstations that accessed the wikileaks.org website on 11/29. After reviewing the firewall log files and interviewing the individuals and examining their workstations NTIS is certain that NO files were downloaded from wikileaks.org.

The names of the individuals (all contractors):

 (b)(6)

Please contact me if you need anything else.

Regards,  
Alan Willard

---

Alan R. Willard, CISSP, GSEC  
Chief IT Security Officer  
National Technical Information Service  
Department of Commerce

P 703-605-6440  
C 703-389-1553  
F 703-605-6686

[awillard@ntis.gov](mailto:awillard@ntis.gov)

---

**From:** members of the Federation of Department of Commerce CIRTs and CIRCs  
[mailto:FEDCIRT@LIST.COMMERCE.GOV] **On Behalf Of** Nguyen, Vu  
**Sent:** Tuesday, November 30, 2010 4:17 PM  
**To:** [FEDCIRT@LIST.COMMERCE.GOV](mailto:FEDCIRT@LIST.COMMERCE.GOV)  
**Subject:** Re: Wikileaks Site Block \*\*\*Situational Awareness\*\*\*  
**Importance:** High

Federation Team Members,

The following action is to be taken on all PC's identified as accessing the WikiLeaks.org site since Friday, Nov 26<sup>th</sup>:

- 1) Immediately disconnect the PC from the network
- 2) Remove the hard drive and replace with a new hard drive.
- 3) Do not copy user data from the removed drive to the new drive.
- 4) Label the removed hard drive with the user name.
- 5) Label the removed hard drive as potentially having classified material.

- 6) The drive should be treated as containing Secret material.
- 7) Store the removed hard drive in a GSA approved safe until further guidance is provided or forward the hard drive (packaged in accordance with the DOC Security Manual for transporting Secret material) to:

Roger Clark  
Senior Advisor  
National & Cyber Security  
U.S. Department of Commerce  
1401 Constitution Avenue, NW, Room 6625  
Washington, DC 20230

- 8) Report completion to the DOC-CIRT.

Thanks,  
Vu T. Nguyen  
Office of the Chief Information Officer  
Advanced Cyber Threat and Forensic Analysis Team Lead  
U.S. Department of Commerce  
E-mail: [vnguyen@doc.gov](mailto:vnguyen@doc.gov)  
SIPRNet: [vnguyen@doc.sgov.gov](mailto:vnguyen@doc.sgov.gov)  
Phone: (202) 482-6401  
Blackberry: (202) 834-9123

**From:** Nguyen, Vu  
**Sent:** Tuesday, November 30, 2010 11:57 AM  
**To:** 'FEDCIRT@LIST.COMMERCE.GOV'  
**Cc:** Clark, Roger; Whiteside, Fred; DOC-CIRT  
**Subject:** Wikileaks Site Block \*\*\*Situational Awareness\*\*\*  
**Importance:** High

Federation Team Members,

Due to recent reports of classified information residing on the Wikileaks.org website, all OU's are to immediately block access to the site via URL filter or DNS black-hole. Report completion of this task to DOC-CIRT by COB today.

In addition to the site-block, a report is required noting the number of PC's and a listing of users that have accessed the site since Friday, November 26, 2010. It is possible that these PC's could inadvertently contain classified information.

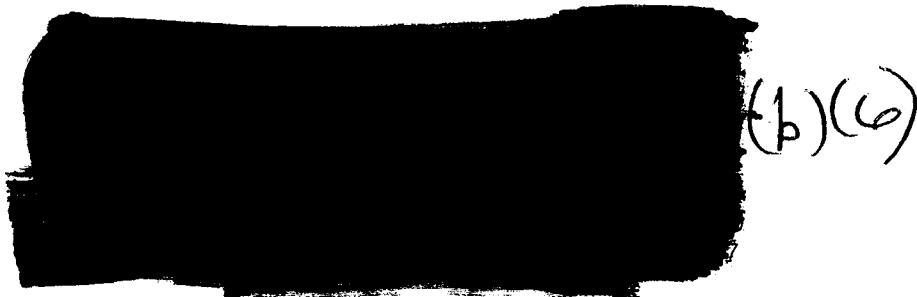
Thanks,  
Vu T. Nguyen  
Office of the Chief Information Officer  
Advanced Cyber Threat and Forensic Analysis Team Lead  
U.S. Department of Commerce  
E-mail: [vnguyen@doc.gov](mailto:vnguyen@doc.gov)  
SIPRNet: [vnguyen@doc.sgov.gov](mailto:vnguyen@doc.sgov.gov)  
Phone: (202) 482-6401  
Blackberry: (202) 834-9123

## Clark, Roger

---

**From:** Callahan, Brian [Brian.Callahan@bea.gov]  
**Sent:** Thursday, December 02, 2010 4:09 PM  
**To:** Clark, Roger  
**Cc:** Solanki, Shashikant; Raville, Michele  
**Subject:** RE: List of User Names

The following BEA employees might have been inadvertently exposed to classified data (wilileaks.org)



---

**From:** Clark, Roger [mailto:RClark@doc.gov]  
**Sent:** Thursday, December 02, 2010 9:41 AM  
**To:** Callahan, Brian  
**Subject:** List of User Names  
**Importance:** High

Brian,

OSY is pushing for the list of user names that accessed the WikiLeaks site so they can schedule an inadvertent disclosure briefing with them. Thanks.

v/r  
Roger Clark  
Senior Advisor  
National & Cyber Security  
Office of the Chief Information Officer  
U.S. Department of Commerce  
Phone: (202) 482-0121  
Email: [rclark@doc.gov](mailto:rclark@doc.gov)



**Clark, Roger**

---

**From:** Clark, Roger  
**Sent:** Thursday, December 02, 2010 4:26 PM  
**To:** Callahan, Brian  
**Cc:** Solanki, Shashikant; Raville, Michele  
**Subject:** RE: List of User Names

Thank you. If you want to discuss technical ways to possibly retrieve data from the pulled drives, give me a call tomorrow and we can discuss.

**From:** Callahan, Brian [<mailto:Brian.Callahan@bea.gov>]  
**Sent:** Thursday, December 02, 2010 4:09 PM  
**To:** Clark, Roger  
**Cc:** Solanki, Shashikant; Raville, Michele  
**Subject:** RE: List of User Names

The following BEA employees might have been inadvertently exposed to classified data (willileaks.org)



---

**From:** Clark, Roger [<mailto:RClark@doc.gov>]  
**Sent:** Thursday, December 02, 2010 9:41 AM  
**To:** Callahan, Brian  
**Subject:** List of User Names  
**Importance:** High

Brian,

OSY is pushing for the list of user names that accessed the WikiLeaks site so they can schedule an inadvertent disclosure briefing with them. Thanks.

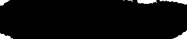
v/r  
Roger Clark  
Senior Advisor  
National & Cyber Security  
Office of the Chief Information Officer  
U.S. Department of Commerce  
Phone: (202) 482-0121  
Email: [rclark@doc.gov](mailto:rclark@doc.gov)

## Clark, Roger

---

**From:** Solanki, Shashikant [Shashikant.Solanki@bea.gov]  
**Sent:** Friday, December 03, 2010 10:34 AM  
**To:** Clark, Roger  
**Cc:** Raville, Michele; Callahan, Brian  
**Subject:** RE: List of User Names

Roger,

 comes off the list. She was blocked access as she had tried to access Wikileaks after we had implemented the Bureau-wide block.

Shashikant (Solly) Solanki  
IT Security Officer  
Office of CIO  
Rm. 3066  
Phone: 202-606-9617

---

**From:** Clark, Roger [mailto:RClark@doc.gov]  
**Sent:** Thursday, December 02, 2010 4:26 PM  
**To:** Callahan, Brian  
**Cc:** Solanki, Shashikant; Raville, Michele  
**Subject:** RE: List of User Names

Thank you. If you want to discuss technical ways to possibly retrieve data from the pulled drives, give me a call tomorrow and we can discuss.

---

**From:** Callahan, Brian [mailto:Brian.Callahan@bea.gov]  
**Sent:** Thursday, December 02, 2010 4:09 PM  
**To:** Clark, Roger  
**Cc:** Solanki, Shashikant; Raville, Michele  
**Subject:** RE: List of User Names

The following BEA employees might have been inadvertently exposed to classified data (wilileaks.org)

 (b)(6)

---

**From:** Clark, Roger [mailto:RClark@doc.gov]  
**Sent:** Thursday, December 02, 2010 9:41 AM  
**To:** Callahan, Brian  
**Subject:** List of User Names  
**Importance:** High

Brian,

OSY is pushing for the list of user names that accessed the WikiLeaks site so they can schedule an inadvertent disclosure briefing with them. Thanks.

v/r

Roger Clark

Senior Advisor

National & Cyber Security

Office of the Chief Information Officer

U.S. Department of Commerce

Phone: (202) 482-0121

Email: [rclark@doc.gov](mailto:rclark@doc.gov)

**Clark, Roger**

---


**From:** Clark, Roger  
**Sent:** Friday, December 03, 2010 1:21 PM  
**To:** Solanki, Shashikant  
**Cc:** Raville, Michele; Callahan, Brian  
**Subject:** RE: List of User Names

Got it thanks

---

**From:** Solanki, Shashikant [<mailto:Shashikant.Solanki@bea.gov>]  
**Sent:** Friday, December 03, 2010 10:34 AM  
**To:** Clark, Roger  
**Cc:** Raville, Michele; Callahan, Brian  
**Subject:** RE: List of User Names

Roger,

 comes off the list. She was blocked access as she had tried to access Wikileaks after we had implemented the Bureau-wide block.

Shashikant (Solly) Solanki  
IT Security Officer  
Office of CIO  
Rm. 3066  
Phone: 202-606-9617

---

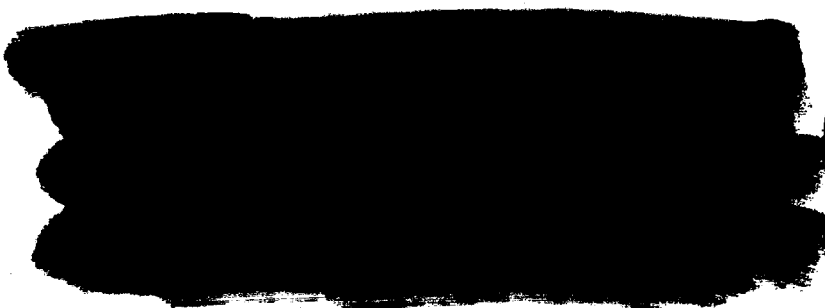
**From:** Clark, Roger [<mailto:RCClark@doc.gov>]  
**Sent:** Thursday, December 02, 2010 4:26 PM  
**To:** Callahan, Brian  
**Cc:** Solanki, Shashikant; Raville, Michele  
**Subject:** RE: List of User Names

Thank you. If you want to discuss technical ways to possibly retrieve data from the pulled drives, give me a call tomorrow and we can discuss.

---

**From:** Callahan, Brian [<mailto:Brian.Callahan@bea.gov>]  
**Sent:** Thursday, December 02, 2010 4:09 PM  
**To:** Clark, Roger  
**Cc:** Solanki, Shashikant; Raville, Michele  
**Subject:** RE: List of User Names

The following BEA employees might have been inadvertently exposed to classified data (willileaks.org)

 (b)(6)

---

**From:** Clark, Roger [<mailto:RClark@doc.gov>]  
**Sent:** Thursday, December 02, 2010 9:41 AM  
**To:** Callahan, Brian  
**Subject:** List of User Names  
**Importance:** High

Brian,

OSY is pushing for the list of user names that accessed the WikiLeaks site so they can schedule an inadvertent disclosure briefing with them. Thanks.

v/r  
Roger Clark  
Senior Advisor  
National & Cyber Security  
Office of the Chief Information Officer  
U.S. Department of Commerce  
Phone: (202) 482-0121  
Email: [rclark@doc.gov](mailto:rclark@doc.gov)

[REDACTED]

---

**From:** [REDACTED]  
**Sent:** Wednesday, December 01, 2010 8:33 AM  
**To:** Bergersen, Benjamin  
**Cc:** [REDACTED]  
**Subject:** Fw: Broadcast Message  
**Attachments:** image001.gif  
**Importance:** High

Do we want to send a OIG All Hands regarding this? Please see the email thread below.

---

**From:** [REDACTED]  
**To:** Bergersen, Benjamin  
**Sent:** Tue Nov 30 18:10:51 2010  
**Subject:** Fw: Broadcast Message

Ben - Please review [REDACTED] recommendation below. I believe it's a good idea and will prep and send with your approval. Thanks.

---

**From:** [REDACTED]  
**To:** [REDACTED]  
**Cc:** [REDACTED]  
**Sent:** Tue Nov 30 18:03:18 2010  
**Subject:** Broadcast Message

[REDACTED]

Do you think a broadcast to all OIG employees letting them know that Wiki Leaks website should not be not access via the OIG equipment or VLAN is something we need to pursue? The Wiki Leaks website may contain classified materials and the OIG VLAN is not certified to create/review/print and/or store any information higher than sensitive.

[REDACTED]

Office of the Chief Information Officer  
Office of Inspector General  
U.S. Department of Commerce  
(202) 482- [REDACTED] office  
(202) 680- [REDACTED] cell  
(202) 501- [REDACTED] or (202) 482- [REDACTED] fax  
[REDACTED]@oig.doc.gov

[REDACTED]

---

**From:** Leiphart, Kristine  
**Sent:** Thursday, December 02, 2010 10:09 AM  
**To:** Dahl, Scott  
**Cc:** Bergersen, Benjamin, [REDACTED]  
**Subject:** RE: WikiLeaks incident

Good idea. We can forward the Departmental message that was sent to all DOC staff this week with a blurb about how OIG needs to exercise special caution.

**From:** Dahl, Scott  
**Sent:** Thursday, December 02, 2010 10:07 AM  
**To:** Leiphart, Kristine  
**Cc:** Bergersen, Benjamin  
**Subject:** WikiLeaks incident

What do you think about sending out to our workforce a reminder to be cautious about what websites they visit on their work computers. There is an every-growing risk of contracting viruses that could infect their and others computers. In addition, we could mention the WikiLeaks incident as an example where visiting a website resulted in one of our computers having to be taken offline and wiped because of concern that classified information on the website may have been downloaded on the employee's computer. I just think it is a cautionary tale that would serve as a beneficial reminder.

Scott S. Dahl  
Deputy Inspector General  
U.S. Department of Commerce  
1401 Constitution Avenue, NW  
Room 7898C  
Washington, DC 20230  
(202) 482-4899

[REDACTED]

---

**From:** Bergersen, Benjamin  
**Sent:** Thursday, December 02, 2010 10:29 AM  
**To:** Leiphart, Kristine; [REDACTED] Bergersen, Benjamin  
**Subject:** Re: WikiLeaks incident - ben to send out

[REDACTED] -  
I will send this out.

Thanks,  
Ben  
Benjamin Bergersen  
Chief Information Officer

Office of Inspector General  
U.S. Commerce Department  
202-482-0611 Main Office  
[benjamin.bergersen@oig.doc.gov](mailto:benjamin.bergersen@oig.doc.gov)

---

**From:** Leiphart, Kristine  
**To:** [REDACTED]  
**Cc:** Bergersen, Benjamin  
**Sent:** Thu Dec 02 10:09:24 2010  
**Subject:** FW: WikiLeaks incident

Please execute.

**From:** Leiphart, Kristine  
**Sent:** Thursday, December 02, 2010 10:09 AM  
**To:** Dahl, Scott  
**Cc:** Bergersen, Benjamin; Slaughter, Ronald  
**Subject:** RE: WikiLeaks incident

Good idea. We can forward the Departmental message that was sent to all DOC staff this week with a blurb about how OIG needs to exercise special caution.

**From:** Dahl, Scott  
**Sent:** Thursday, December 02, 2010 10:07 AM  
**To:** Leiphart, Kristine  
**Cc:** Bergersen, Benjamin  
**Subject:** WikiLeaks incident

What do you think about sending out to our workforce a reminder to be cautious about what websites they visit on their work computers. There is an every-growing risk of contracting viruses that could infect their and others computers. In addition, we could mention the WikiLeaks incident as an example where visiting a website resulted in one of our computers having to be taken offline and wiped because of concern that classified information on the website may have been downloaded on the employee's computer. I just think it is a cautionary tale that would serve as a beneficial reminder.

Scott S. Dahl  
Deputy Inspector General



U.S. Department of Commerce  
1401 Constitution Avenue, NW  
Room 7898C  
Washington, DC 20230  
(202) 482-4899

All redactions (b)(6)

[REDACTED]

---

**From:** Bergersen, Benjamin  
**Sent:** Thursday, December 02, 2010 11:14 AM  
**To:** [REDACTED]; Bergersen, Benjamin; [REDACTED] Leiphart, Kristine  
**Subject:** Security Incident - refresher training and case file today...please  
**Attachments:** WikiLeaks\_2010\_12\_01[1].pdf  
**Importance:** High

[REDACTED] -  
Give refresher training to the employee and find out what his security clearance level is.

Keep all the paperwork in your case file. The IG and Management will want your case file today. (There are executive meetings with the Office of the Secretary committees).

Thanks,  
Ben  
Benjamin Bergersen  
Chief Information Officer

Office of Inspector General  
U.S. Commerce Department  
202-482-0611 Main Office  
[benjamin.bergersen@oig.doc.gov](mailto:benjamin.bergersen@oig.doc.gov)

---

**From:** Bergersen, Benjamin  
**To:** OIG All Employees; OIG Help Desk  
**Sent:** Thu Dec 02 11:02:43 2010  
**Subject:** \\\FOUO \\\ IT Services Notice - Wikileaks Potentially Classified Documents. Gentle reminder of Viruses, and Security - a cautionary tale - \\\FOUO \\\

...FOR OFFICIAL USE ONLY....DO NOT DISTRIBUTE OUTSIDE  
OIG...

# IT SERVICES NOTICE

## WHAT IS HAPPENING

There is potentially classified materials on the WikiLeaks web site that Commerce personnel have attempted to view from

unclassified computers. This has resulted in dozens of computers DOC wide needing to be wiped by security personnel, including one PC from the OIG. This is a cautionary tale of the OIG person who had to have their computer formatted, and then returned. Don't let it happen to you.

The Department of Commerce is forbidding people to access the Wikileaks web site because our IT systems are not cleared to view, transmit, or store potentially classified documents. (National security classified documents such as "secret", "top secret", or higher.)

Your computer will be confiscated, the hard drive removed, and the drive wiped by OIG personnel with the requisite security clearances.

See attached memo from the Office of the Secretary.

## **WHAT THIS MEANS TO YOU**

- ✓ Do not attempt to access Wikileaks as you may be accessing potentially classified information above your computer systems clearance level, above your clearance level, and without a "need to know".
- ✓ Only access that site if you have an official work order from your supervisor, have the personal security clearance level, have an official "need to know" – not just curiosity, and you

are operating from a properly classified area. (This is generally "secret" and "top secret" investigations and audits.)

- ✓ The same formatting of your computer and loss of productivity can occur if you access a potentially bad web site with viruses or worms. The DOC and OIG IT security systems are not full-proof. Use common sense. Stay away from bad web sites that may have viruses, unauthorized PII, unauthorized classified material, or worms.

## QUESTIONS

For additional information or assistance please call the OIG OCIO Helpdesk at (202) 482-1238 or send us an e-mail at [helpdesk@oig.doc.gov](mailto:helpdesk@oig.doc.gov)

Warm Regards,

Ben

Benjamin Bergersen

Chief Information Officer

Office of Inspector General  
U.S. Department of Commerce  
202-482-0611 main office  
[Benjamin.Bergersen@oig.doc.gov](mailto:Benjamin.Bergersen@oig.doc.gov)

...FOR OFFICIAL USE ONLY....DO NOT DISTRIBUTE OUTSIDE  
OIG...

[REDACTED]

---

**From:** [REDACTED]  
**Sent:** Wednesday, December 01, 2010 8:02 AM  
**To:** Zinser, Todd; Dahl, Scott  
**Subject:** Computer

I don't have a computer for the day while it is being wiped clean. I'm going up to run up the to [REDACTED] later this morning.

[REDACTED]

---

From: [REDACTED]  
Sent: Wednesday, December 01, 2010 9:09 AM  
To: [REDACTED]  
Subject: Re: My computer

Confirmed - all is good.

[REDACTED]  
Office of the Inspector General  
U.S. Department of Commerce  
Washington DC  
202.482.[REDACTED]

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

From: [REDACTED]  
To: [REDACTED]  
Sent: Wed Dec 01 09:05:11 2010  
Subject: Re: My computer

[REDACTED],  
[REDACTED] has the pc and I have the hard drives. CCU staff had left I stopped by last night.  
[REDACTED]

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

From: [REDACTED]  
To: [REDACTED]  
Sent: Wed Dec 01 08:54:17 2010  
Subject: My computer

(b) (6) and (b) (7) (C)

Is gone but [REDACTED] ofc doesn't have it. Do you know where it is?

[REDACTED]  
Office of the Inspector General  
U.S. Department of Commerce  
Washington DC  
202.482.[REDACTED]

refer to  
Dept

**From:** Broadcast, DOC [broadcast@doc.gov]  
**Sent:** Wednesday, December 01, 2010 10:57 AM  
**To:** Broadcast, DOC  
**Subject:** Guidance regarding WikiLeaks

To: All Commerce Employees and Contractors

Recent reports indicate that a number of government documents have been posted on the WikiLeaks website. These documents may or may not contain information that is considered National Security Information (classified information) and as such, the information is NOT authorized for downloading, viewing, printing, processing, copying, or transmitting via non-classified Government-issued computers, laptops, blackberries, or other communication devices and is not an authorized use of DOC IT equipment. Doing so would introduce potentially classified information onto our unclassified networks and represent a potential security incident.

There has been a rumor that the information is no longer classified since it resides in the public domain. This is NOT true. Executive Order 13526, Section I.1(4)(2) states "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information." The information was neither properly nor improperly "declassified" by the appropriate authority and requires continued classification or reclassification.

Please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents because these documents may contain classified information. Accessing the WikiLeaks documents will lead to sanitization of your PC to remove any potentially classified information from the system and result in possible data loss.

If you have questions regarding this broadcast or have accessed the WikiLeaks documents, please contact the DOC Computer Incident Response Team at email [doc-cirt@doc.gov](mailto:doc-cirt@doc.gov) or call (202) 482-4000.

This message was authorized by the Office of Secretary OSY/OCIO.

Please do not reply to this message. The broadcast email account is not monitored for incoming mail.

[REDACTED]

---

**From:** [REDACTED]  
**Sent:** Thursday, December 02, 2010 6:38 AM  
**To:** Zinser, Todd  
**Cc:** Dahl, Scott; Leiphart, Kristine  
**Subject:** Updated Talking Points for the EMT Meeting  
**Attachments:** Talking Points for EMT - December-2-2010.docx  
  
**Importance:** High

Good Morning Todd,

Attached are the revised talking points for this morning EMT meeting showing the number of DOC employees accessing the WIKI site.

[REDACTED]

[REDACTED]

**Office of Administration**  
**Office of Inspector General**  
**(202) 482-[REDACTED]**  
**(202) 501-[REDACTED] (Fax)**



**Clark, Roger**

---

**From:** Jayakody, Ananda [Ajayakody@eda.doc.gov]  
**Sent:** Wednesday, December 01, 2010 12:54 PM  
**To:** Batluck, Jonathan  
**Subject:** RE: Re: Possible security hole

Hi Jon,

Please give me an exact time that I should call you so that I can get [REDACTED] scheduled for this.

Thanks  
AJ

**From:** Batluck, Jonathan [mailto:JBatluck@doc.gov]  
**Sent:** Wednesday, December 01, 2010 11:24 AM  
**To:** Jayakody, Ananda  
**Subject:** RE: Re: Possible security hole

I should be available after 12:30 today.

Regards,

Jonathan Batluck  
OCIO - HCHB Network & Telecommunications  
U.S. Dept. of Commerce  
202.482.5556  
[jbatluck@doc.gov](mailto:jbatluck@doc.gov)

**From:** Jayakody, Ananda [mailto:Ajayakody@eda.doc.gov]  
**Sent:** Wednesday, December 01, 2010 11:06 AM  
**To:** Batluck, Jonathan  
**Subject:** FW: Re: Possible security hole

Hi Jon,

[REDACTED] wants to have a conference call between 3 of us. Please let me know when you are available to do so.

Thanks

AJ

---

**From:** Jayakody, Ananda  
**Sent:** Wednesday, December 01, 2010 9:04 AM  
**To:** Batluck, Jonathan  
**Subject:** Re: Possible security hole

Hi Jon,

(b)(6)  
[REDACTED] has been notified that two IP addresses had the access to Wikileaks site and downloaded some documents.

(b)(6)  
One is a Philly workstation and the other one is [REDACTED] which is the Chicago subnet address. I need to discuss this with you and please give me a call because I would like to know how the Chicago subnet address was used.

Thanks

AJ

*ananda jayakody*

**Clark, Roger**

---

**From:** Jayakody, Ananda [Ajayakody@eda.doc.gov]  
**Sent:** Wednesday, December 01, 2010 11:24 AM  
**To:** Batluck, Jonathan  
**Subject:** RE: Re: Possible security hole

Thanks Jon, I will call you then.

Thanks  
A)

**From:** Batluck, Jonathan [mailto:JBatluck@doc.gov]  
**Sent:** Wednesday, December 01, 2010 11:24 AM  
**To:** Jayakody, Ananda  
**Subject:** RE: Re: Possible security hole

I should be available after 12:30 today.

Regards,

Jonathan Batluck  
OCIO - HCHB Network & Telecommunications  
U.S. Dept. of Commerce  
202.482.5556  
[jbatluck@doc.gov](mailto:jbatluck@doc.gov)

**From:** Jayakody, Ananda [mailto:Ajayakody@eda.doc.gov]  
**Sent:** Wednesday, December 01, 2010 11:06 AM  
**To:** Batluck, Jonathan  
**Subject:** FW: Re: Possible security hole

Hi Jon, (b)(6)

[REDACTED] wants to have a conference call between 3 of us. Please let me know when you are available to do so.

Thanks

A)

---

**From:** Jayakody, Ananda  
**Sent:** Wednesday, December 01, 2010 9:04 AM  
**To:** Batluck, Jonathan  
**Subject:** Re: Possible security hole

Hi Jon, (b)(6)

[REDACTED] has been notified that two IP addresses had the access to Wikileaks site and downloaded some documents.

(B)(6)

One is a Philly workstation and the other one is [REDACTED] which is the Chicago subnet address. I need to discuss this with you and please give me a call because I would like to know how the Chicago subnet address was used.

Thanks

AJ

*ananda jayakody*

**Clark, Roger**

---

**From:** Batluck, Jonathan  
**Sent:** Wednesday, December 01, 2010 1:00 PM  
**To:** Jayakody, Ananda  
**Subject:** RE: Re: Possible security hole

AJ,

I just got back now, sorry it went over.

Jonathan Batluck  
OCIO - HCHB Network & Telecommunications  
U.S. Dept. of Commerce  
202.482.5556  
[jbatluck@doc.gov](mailto:jbatluck@doc.gov)

**From:** Jayakody, Ananda [<mailto:Ajayakody@eda.doc.gov>]  
**Sent:** Wednesday, December 01, 2010 12:54 PM  
**To:** Batluck, Jonathan  
**Subject:** RE: Re: Possible security hole

Hi Jon,

Please give me an exact time that I should call you so that I can get Sandy scheduled for this.

Thanks  
A)

**From:** Batluck, Jonathan [<mailto:JBatluck@doc.gov>]  
**Sent:** Wednesday, December 01, 2010 11:24 AM  
**To:** Jayakody, Ananda  
**Subject:** RE: Re: Possible security hole

I should be available after 12:30 today.

Regards,

Jonathan Batluck  
OCIO - HCHB Network & Telecommunications  
U.S. Dept. of Commerce  
202.482.5556  
[jbatluck@doc.gov](mailto:jbatluck@doc.gov)

**From:** Jayakody, Ananda [<mailto:Ajayakody@eda.doc.gov>]  
**Sent:** Wednesday, December 01, 2010 11:06 AM  
**To:** Batluck, Jonathan  
**Subject:** FW: Re: Possible security hole

Hi Jon,

(b)(6)

[REDACTED] wants to have a conference call between 3 of us. Please let me know when you are available to do so.

Thanks

A]

---

**From:** Jayakody, Ananda

**Sent:** Wednesday, December 01, 2010 9:04 AM

**To:** Batiuck, Jonathan

**Subject:** Re: Possible security hole

Hi Jon,

(b)(6)

[REDACTED] has been notified that two IP addresses had the access to Wikileaks site and downloaded some documents.

(b)(6)

One is a Philly workstation and the other one is [REDACTED] which is the Chicago subnet address. I need to discuss this with you and please give me a call because I would like to know how the Chicago subnet address was used.

Thanks

A]

**ananda jayakody**

**Clark, Roger**

---

**From:** Jayakody, Ananda [Ajayakody@eda.doc.gov]  
**Sent:** Wednesday, December 01, 2010 9:04 AM  
**To:** Batluck, Jonathan  
**Subject:** Re: Possible security hole

Hi Jon,

(b)(6)  
[REDACTED] has been notified that two IP addresses had the access to Wikileaks site and downloaded some documents.

(b)(6)  
One is a Philly workstation and the other one is [REDACTED] which is the Chicago subnet address. I need to discuss this with you and please give me a call because I would like to know how the Chicago subnet address was used.

Thanks

Aj


*ananda jayakody*

Clark, Roger

---

**From:** Jayakody, Ananda [Ajayakody@eda.doc.gov]  
**Sent:** Wednesday, December 01, 2010 11:06 AM  
**To:** Batluck, Jonathan  
**Subject:** FW: Re: Possible security hole

Hi Jon,

 wants to have a conference call between 3 of us. Please let me know when you are available to do so.


Thanks

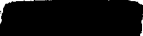
AJ

---

**From:** Jayakody, Ananda  
**Sent:** Wednesday, December 01, 2010 9:04 AM  
**To:** Batluck, Jonathan  
**Subject:** Re: Possible security hole

Hi Jon,

 has been notified that two IP addresses had the access to Wikileaks site and downloaded some documents.

One is a Philly workstation and the other one is  which is the Chicago subnet address. I need to discuss this with you and please give me a call because I would like to know how the Chicago subnet address was used.

Thanks

AJ

*ananda jayakody*





US DEPARTMENT OF COMMERCE

Computer Incident Response Team

DOC CIRT Evidence Custody Form

DOC CIRT Case Number: \_\_\_\_\_

Agency: EDA

Other Reference ID: W.K. Leaks

Item Number	Property Tag	Model Number	Serial Number
1E A54 643 0192814325			
Item Description			
UPS Package (unopened) containing hard drive from EDA (Ph. ludolphia)			

(b)(6) Chain of Custody

Date/Time		Released By			Received By		
Date	Time	Name	Agency	Signature	Name	Agency	Signature
12/1/10	1600	[Redacted]	EDA	[Redacted]	erClark	DOC/CS	Regis X Clark

For Official Use Only

**Clark, Roger**

---

**From:** smoses@eda.doc.gov  
**Sent:** Friday, December 10, 2010 1:41 PM  
**To:** Clark, Roger  
**Subject:** Custody Form for WikiLeaks

Roger,

Attached are the custody forms with my signature.

File(s) will be available for download until **09 January 2011**:

File: Custody Form HD WikiLeaks.pdf, 1,086.68 KB [Fingerprint: bf38a8b63c7ee57f4ce43b4843cc163e]

You have received attachment link(s) within this email sent via Proofpoint Secure File Transfer. To retrieve the attachment(s), please click on the link(s).

Accellion File Transfer



## US DEPARTMENT OF COMMERCE

Computer Incident Response Team

## DOC CIRT Evidence Custody Form

DOC CIRT Case Number: \_\_\_\_\_

Agency: EDAOther Reference ID: Wik. Leaks

Item Number	Property Tag	Model Number	Serial Number
12 A54 GHW 01 9447 5222			
Item Description			
UPS Package containing hard drive from EDA (Chicago)			

## Chain of Custody

Date/Time		Name	Released By		Received By		
Date	Time		Agency	Signature	Name	Agency	Signature
12/3/10	1640	[Redacted]	EDA	[Redacted]	Roger Clark	DDO/US	Roger X Clark

For Official Use Only

PW

(b)(6)

234  
45  
68

Requester CC

## Steve Needle

---

**From:** Alan Willard  
**Sent:** Wednesday, December 01, 2010 12:58 PM  
**To:** Bruce Borzino  
**Cc:** Steve Needle  
**Subject:** Wikileaks web

• Bruce;

This incident is over for now, below is a copy of the e-mail I sent downtown. OSY wants to read these people out – which is a relief that they are going to do it right – and that's it....we're done.

*DOC-CIRT, Roger Clark;*

*NTIS identified 3 PC workstations that accessed the wikileaks.org website on 11/29. After reviewing the firewall log files and interviewing the individuals and examining their workstations NTIS is certain that NO files were downloaded from wikileaks.org.*

*The names of the individuals (all contractors):*

[REDACTED]  
[REDACTED] (b)(6)  
[REDACTED]

*Please contact me if you need anything else.*

*Regards,  
Alan Willard*


## Steve Needle

---

**From:** Bob McClellan  
**Sent:** Wednesday, December 01, 2010 9:58 AM  
**To:** Alan Willard  
**Cc:** Keith Sinner  
**Subject:** RE: Wikileaks PC's  
**Attachments:** wikileaks.xlsx

See attached spreadsheet. Here are the PCs that accessed the wikileaks site since last Friday. All three accessed the site on 11/29:

172.16.66.55  
172.16.67.105  
172.16.70.166

 (b)(6)

Doesn't look like anyone downloaded any documents.

Bob

---

**From:** Alan Willard  
**Sent:** Wednesday, December 01, 2010 6:30 AM  
**To:** Bob McClellan  
**Cc:** Keith Sinner  
**Subject:** Wikileaks PC's

Bob;

Please determine which workstations accessed the wikileaks.org website, Keith and I need the names of the users.

Thanks,  
Alan

---

Alan R. Willard, CISSP, GSEC  
Chief IT Security Officer  
National Technical Information Service  
Department of Commerce

P 703-605-6440  
C 703-389-1553  
F 703-605-6686

[awillard@ntis.gov](mailto:awillard@ntis.gov)

**From:** Kenneth R Harrison  
**To:** William W Bradd  
**Cc:** Scott D Williams; Timothy P Ruland; Daren Gutschow  
**Subject:** Re: Wikileaks Site Block \*\*\*Situational Awareness\*\*\*  
**Date:** 12/01/2010 03:25 PM

---

Thanks! We are working on it now.

---

**From:** William W Bradd  
**Sent:** 12/01/2010 03:21 PM EST  
**To:** Kenneth Harrison  
**Cc:** Scott Williams; Timothy Ruland  
**Subject:** Fw: Wikileaks Site Block \*\*\*Situational Awareness\*\*\*

Kenney,

For the individuals below, here at the HQ, the ports can be enabled so LTSO can complete the replacement process.

--v/r--

-Security is a team sport.....  
Michael Hayden, Director, NSA

William W. Bradd  
Assistant IT Security Officer  
- for Technical Security  
US Census Bureau  
301-763-3518

----- Forwarded by William W Bradd/ITSO/HQ/BOC on 12/01/2010 03:19 PM -----

**From:** William W Bradd/ITSO/HQ/BOC  
**To:** "Patricia Musselman" <patricia.trainor.musselman@census.gov>, Jason B Schaufele/LTSO/HQ/BOC@BOC, Richard B Birdsong/LTSO/HQ/BOC@BOC, "Kenneth Harrison" <kenneth.r.harrison@census.gov>  
**Cc:** Timothy P Ruland/ITSO/HQ/BOC@BOC, Benjamin A Padilla/ITSO/HQ/BOC@BOC, Frederick W Fricker Jr/ITSO/HQ/BOC@BOC, BOC CIRT@BOC  
**Date:** 11/30/2010 01:32 PM  
**Subject:** Fw: Wikileaks Site Block \*\*\*Situational Awareness\*\*\*

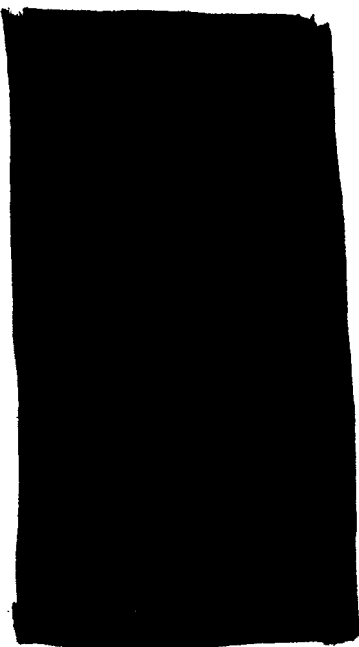
---

Tish/Jason

Do to the on going wikileak incident, we have been tasked to identify all users who accessed the site subsequent to the unauthorized release of classified US Government documents by the sites owners.

The users listed below, visited the site subsequent to the release (Nov 26th, 2010) of those documents and are assumed to have viewed and possibly saved classified documents, images, or data to their system.

The following systems need to be removed from the network immediately. Due to the concern that these systems may have classified information on them, no backups will be allowed.



(b)(6)

Also how difficult would it be to check user shares for potential classified data, if it comes to that.

=====

Kenney,

Need to have the port disabled on these systems until they have new systems.

--v/r--

-Security is a team sport.....  
Michael Hayden, Director, NSA

William W. Bradd  
Assistant IT Security Officer  
- for Technical Security  
US Census Bureau  
301-763-3518

----- Forwarded by William W Bradd/ITSO/HQ/BOC on 11/30/2010 01:16 PM -----

From: Timothy P Ruland/ITSO/HQ/BOC

To: Scott D Williams/TCO/HQ/BOC@BOC, Kenneth R. Harrison/TCO/HQ/BOC@BOC, Daren John Gutschow/TCO/HQ/BOC@BOC

Cc: William W Bradd/ITSO/HQ/BOC@BOC, BOC CIRT@BOC, Brian E McGrath/DIR/HQ/BOC@BOC

Date: 11/30/2010 12:25 PM

Subject: Fw: Wikileaks Site Block \*\*\*Situational Awareness\*\*\*



---

Bill has started a search on users access to Wikileaks per the request below. The concern is that someone visiting the site since 11/26 may have downloaded classified material and it is on their PC.

Timothy P. Ruland, CISM, CISSP, CFCP  
Chief, IT Security Officer  
US Census Bureau  
301-763-2869  
301-763-6805 (fax)

"Any man worth his salt will stick up for what he believes right, but  
it takes a slightly better man to acknowledge instantly and without reservation that he is in error" -  
Andrew Jackson

----- Forwarded by Timothy P Ruland/ITSO/HQ/BOC on 11/30/2010 12:23 PM -----

From: Timothy P Ruland/ITSO/HQ/BOC  
To: Scott D Williams/TCO/HQ/BOC@BOC, Kenneth R Harrison/TCO/HQ/BOC@BOC, Daren John Gutschow/TCO/HQ/BOC@BOC  
Cc: William W Bradd/ITSO/HQ/BOC@BOC, BOC CIRT@BOC, Brian E McGrath/DIR/HQ/BOC@BOC  
Date: 11/30/2010 12:09 PM  
Subject: Fw: Wikileaks Site Block \*\*\*Situational Awareness\*\*\*

---

FYI,

The Technical Security Staff is in a meeting. Please take the actions below to handle the Wikileaks.org website and let the BOC CIRT know when it is completed so we can inform the Department.

I will try and obtain clarification on the second item as we do not have classified material at Census.

Thanks

Timothy P. Ruland, CISM, CISSP, CFCP  
Chief, IT Security Officer  
US Census Bureau  
301-763-2869  
301-763-6805 (fax)

"Any man worth his salt will stick up for what he believes right, but  
it takes a slightly better man to acknowledge instantly and without reservation that he is in error" -  
Andrew Jackson

----- Forwarded by Timothy P Ruland/ITSO/HQ/BOC on 11/30/2010 12:06 PM -----

From: "Nguyen, Vu" <VNguyen@DOC.GOV>  
To: FEDCIRT@LIST.COMMERCE.GOV  
Date: 11/30/2010 11:57 AM  
Subject: Wikileaks Site Block \*\*\*Situational Awareness\*\*\*  
Sent by: members of the Federation of Department of Commerce CIRTs and CIRCs <FEDCIRT@LIST.COMMERCE.GOV>

---

Federation Team Members,

Due to recent reports of classified information residing on the Wikileaks.org website, all OU's are to immediately block access to the site via URL filter or DNS black-hole. Report completion of this task to DOC-CIRT by COB today.

In addition to the site-block, a report is required noting the number of PC's and a listing of users that have accessed the site since Friday, November 26, 2010. It is possible that these PC's could inadvertently contain classified information.

Thanks,

Vu T. Nguyen

Office of the Chief Information Officer

Advanced Cyber Threat and Forensic Analysis Team Lead

U.S. Department of Commerce

E-mail: [vnnguyen@doc.gov](mailto:vnnguyen@doc.gov)

SIPRNet: [vnnguyen@doc.sgov.gov](mailto:vnnguyen@doc.sgov.gov)

Phone: (202) 482-6401

Blackberry: (202) 834-9123

From: Patricia Trainor Musselman  
To: (b)(6)  
Cc: (b)(6) William W Bradd; timothy.p.ruland@census.gov  
Subject: Re: Data Recovery Following Wikileak Access  
Date: 12/02/2010 11:19 AM  
Attachments: 2010\_Acceptable\_Use\_Policy\_01\_Final.docx

---

(b)(6)  
This is the current version of the acceptable use policy.



2010\_Acceptable\_Use\_Policy\_01\_Final.docx

Tish Musselman

▼ Timothy P Ruland---12/01/2010 09:48:00 PM---Below is the guidance received from DOC. I bolded the specific reference to not copy files. I will a

(b)(6)  
From: Timothy P Ruland/ITSO/HQ/BOC  
To: (b)(6)  
Cc: (b)(6) Patricia Trainor Musselman/LTISO/HQ/BOC@BOC, William W Bradd/ITSO/HQ/BOC@BOC, (b)(6)  
Date: 12/01/2010 09:48 PM  
Subject: Re: Data Recovery Following Wikileak Access

---

Below is the guidance received from DOC. I bolded the specific reference to not copy files. I will ask LTISO to forward you a copy of the Census Bureau Acceptable Use Policy (AUP) as well. Employees were presented the AUP on log in earlier this week and had to specifically accept the conditions to connect. The policy states that users should not store files on the local (C: drive) as we will not try and restore or salvage them if the PC is involved in an incident.

Again, no one has indicated you have done anything wrong. However, since classified material was on the site you accessed we have to err on the side of caution that classified material may have been downloaded to your PC.

"The following action is to be taken on all PC's identified as accessing the WikiLeaks.org site since Friday, Nov 26<sup>th</sup> :

- 1) Immediately disconnect the PC from the network

- 2) Remove the hard drive and replace with a new hard drive.
- 3) **Do not copy user data from the removed drive to the new drive.**
- 4) Label the removed hard drive with the user name.
- 5) Label the removed hard drive as potentially having classified material.
- 6) The drive should be treated as containing Secret material.
- 7) Store the removed hard drive in a GSA approved safe until further guidance is provided or forward the hard drive (packaged in accordance with the DOC Security Manual for transporting Secret material) to:

Timothy P. Ruland, CISM, CISSP, CFCP  
Chief, IT Security Officer  
US Census Bureau  
301-763-2869  
301-763-6805 (fax)

"Any man worth his salt will stick up for what he believes right, but it takes a slightly better man to acknowledge instantly and without reservation that he is in error" - Andrew Jackson

(b)(6)

-----  
To: Timothy P Ruland/ITSO/HQ/BOC@BOC

From: (b)(6)

Date: 12/01/2010 04:21PM

cc:

(b)(6)

Patricia Trainor Musselman/LTSO/HQ/BOC@BOC, William W

Bradd/ITSO/HQ/BOC@BOC, (b)(6)

Subject: Re: Data Recovery Following Wikileaks Access

Mr. Ruland,

I appreciate the response, although I am at a loss as to why this decision is being made when I engaged in absolutely no illegal activity. The files on my desktop were accessible when the computer was confiscated. I understand the computer is Government property and there is no right to privacy, however, I felt it is within my right to make the request as instructed by management at the time.

Is it possible to have "the guidance from the Department" and "the Acceptable Use Policy " forwarded to me which you are referring to in your e-mail and any other policy I need to be aware of?

Thank you,

(b)(6)

[REDACTED]  
U.S. Census Bureau

-----Timothy P Ruland/ITSO/HQ/BOC wrote: -----

(b)(6)

To: [REDACTED]  
From: Timothy P Ruland/ITSO/HQ/BOC  
Date: 12/01/2010 04:01PM

(b)(6)

cc: [REDACTED]  
Patricia Trainor Musselman/LTISO/HQ/BOC@BOC, William W  
Bradd/ITSO/HQ/BOC@BOC  
Subject: Data Recovery Following Wikileaks Access

(b)(6)

[REDACTED]

I received a call from DOC on your request to them that we recover files from the PC that was picked up yesterday. DOC CIRT and the Critical Infrastructure Manager concur with our policy on data recovery from PCs picked up as part of security incidents. We do not recover files from PC hard drives under these circumstances.

While I understand your concerns, and I am sure you were not engaging in any malicious activity when you accessed this site, none-the-less, the guidance from the Department and in accordance with our Acceptable Use Policy we will not be able to recover files from your PC.

Timothy P. Ruland, CISM, CISSP, CFCP  
Chief, IT Security Officer  
US Census Bureau  
301-763-2869  
301-763-6805 (fax)

"Any man worth his salt will stick up for what he believes right, but it takes a slightly better man to acknowledge instantly and without reservation that he is in error" - Andrew Jackson

Acceptable Use Policy for  
U.S. Census Bureau Information Technology Systems  
Last Updated – November 8, 2010

This acceptable use policy (AUP) governs the conduct of all Census Bureau personnel—federal employees and contractors—with access to information technology (IT) systems, regardless of method of access or geographic location (i.e., local, or remote). This AUP communicates the role of Census Bureau personnel in protecting these resources and advises them of their obligations.

The Census Bureau's networks and IT systems assume no right of privacy for the personnel who use them; the Census Bureau is permitted to monitor any and all uses of these systems for compliance with this AUP and appropriate agency policy.

*Individual Accountability*

As representatives of the Census Bureau, all personnel—federal employees and contractors—will be held accountable for their actions and may be subject to administrative penalties, fines, termination, and/or imprisonment.

*Data Stewardship*

To fulfill its mission, the Census Bureau collects and processes information from many sources; this information includes responses of individuals and businesses to surveys and censuses, administrative records from other agencies, and personnel data. Federal laws such as Title 13, Title 26, and the Privacy Act protect the confidentiality of these data and the unauthorized use of confidential data by employees and contractors is prohibited.

*Security Practice*

Census Bureau personnel are responsible for securing their IT resources (i.e., computers, workstations, terminals, BlackBerry® wireless devices, etc.) to prohibit unauthorized access. Census Bureau personnel must:

- Log out of secure applications when the applications are no longer in use
- Lock their terminals, log out of the session, or use a password protected screen saver when leaving their computer
- Log out of their workstations at the end of each workday
- Not share workstation or device passwords with anyone except authorized Census Bureau personnel such as LAN staff. Once shared, passwords must be changed as soon as possible after the need has ended. If there is a chance a user's password has been compromised, it must be changed immediately
- Be careful while typing passwords so that the passwords are not observed
- Ensure mobile devices are not accessed by unauthorized persons

*Government Computer Use*

Use of government computers, personal digital assistants (PDA's), BlackBerry® wireless devices, wired or wireless communications systems, data, and other information is meant for only authorized purposes. Any unauthorized use of government equipment is prohibited.

U S C E N S U S B U R E A U

Census Bureau personnel are given access to Census Bureau systems based on the need to perform their job responsibilities. Census Bureau personnel are expected to work within the confinement of this access and are not to attempt to access systems or applications to which access has not been explicitly authorized.

Do not store sensitive work files on your computer's hard drive (the C:\ drive). Sensitive work files should be stored either on your network home directory (the H:\ drive) or network shared directory (the M:\ drive). Only the network directories are backed up. Your computer's hard drive is not backed up, thus there may be no recovery of work files stored on your computer such as when your computer is compromised by malware. It is your responsibility to move work files from your computer's hard drive to either your network home or shared directories.

#### *End-User Software Use*

Unauthorized software may not be installed on any official government computer. Software that has not gone through the SLIC approval process is considered unauthorized. Copyrighted software must be installed consistent with the respective licensing agreement and only after the installation has been approved by Census Bureau management.

#### *Portable Media Use*

The use of all portable media must be authorized by Census Bureau management and used in accordance with Census Bureau policy. Portable media include devices such as:

- Optical media (CD, DVD)
- Removable media (floppy, ZIP®, hard disk)
- Hard drives (portable, external)
- Flash drives (USB)
- Mobile devices in USB storage mode
- Laptops
- Paper printouts

For printing paper copies, use printers that print only with your personal identification number (called private or secure printing). For electronic copies, the sensitive data or the media/device on which the data is stored must be encrypted. Be sure to keep sensitive data separate, labeled properly, and stored securely. Immediately upon finishing with the data or the media/device, erase, shred, or, use burn bags to securely dispose of the data.

#### *Internet Use*

The Census Bureau provides Internet access and related computer resources to Census employees for authorized uses only. The Internet policy is located at  
<[http://www.census.gov/it/itso/docs/CensusInternetUsePolicy\\_v1.02009-02-17.doc](http://www.census.gov/it/itso/docs/CensusInternetUsePolicy_v1.02009-02-17.doc)>.

#### *Remote Access Use*

U S C E N S U S B U R E A U

Remote access to the Census Bureau network is available to Census Bureau personnel in the event of an emergency only and with prior Census Bureau management and Information Technology Security Office (ITSO) authorization.

#### *E-mail Use*

Census Bureau personnel should take into consideration the following when utilizing the e-mail system (either through workstation software or via remote access):

- Consider all messages sent over the Census Bureau computer and communications systems as Census Bureau property (there should be no expectation of privacy associated with information sent through Census Bureau systems)
- Do not send sensitive data of any kind in the text of e-mail (all sensitive data must be encrypted and sent as an attachment)
- Do not send illegal transmissions (e.g., respect copyright laws)
- Follow established retention (archiving) policies
- Consent to monitoring and review activities

#### *IT Security Incident Reporting*

If you are aware of an IT security incident you must contact the Bureau of the Census Computer Incident Response Team (BOC CIRT) immediately by e-mail ([BOC.CIRT@census.gov](mailto:BOC.CIRT@census.gov)) or phone 301-763-5141. Actual or suspected loss of sensitive data must be reported within one hour of discovery. A 24-hour, toll-free phone 877-343-2010 is available. Categories of IT security incidents are located at [<http://cwww.census.gov/it/itso/AV\\_categories\\_of\\_incidents.html>](http://cwww.census.gov/it/itso/AV_categories_of_incidents.html)



Katzman, Esther S.

---

**From:** nist-itso@nist.gov on behalf of remedy [remedy1@nist.gov]  
**Sent:** Thursday, December 02, 2010 7:01 PM  
**To:** Multiple recipients of list  
**Subject:** Case HD0000000372813, Severity 4 Priority, Low urgency, has been assigned to IT Security.

-----  
Requester Name: [REDACTED] (b)(6) Phone: [REDACTED]

Requester Email: [REDACTED]@nist.gov

Short Description: User contact by his supervisor who was contacted by his supervisor regarding a system that was used to look at Wikileaks.

Full Description: User contact by his supervisor who was contacted by his supervisor regarding a system that was used to look at Wikileaks. He does not know which system this may be and needs to know the next step. User did not access this site.

Priority: Severity 4

Request Urgency: Low  
-----

wiki sources (with contact)

**Subject:** wiki sources (with contact)

**From:** David Kustaborder <kusty@nist.gov>

**Date:** Wed, 1 Dec 2010 10:28:35 -0500

**To:** [REDACTED] <[REDACTED]@nist.gov>

**CC:** "Antonishek, John K." <john.antonishek@nist.gov>

<p>(b)(6)</p> <p>wiki_sources(with_users).xls</p>	<p><b>Content-Description:</b> wiki_sources(with_users).xls</p> <p><b>Content-Type:</b> application/vnd.ms-excel</p> <p><b>Content-Encoding:</b> base64</p>
---	---

**Loebach, Matthew T.**

---

**From:** Hurst V, Alfred Coulter  
**Sent:** Tuesday, December 28, 2010 2:46 PM  
**To:** Kustaborder, David P.  
**Cc:** Loebach, Matthew T.  
**Subject:** PC Sanitized

Dave,

(b)(6)

PC has been sanitized.

Al

**Clark, Roger**

---

**From:** Plummer, Christopher  
**Sent:** Friday, December 10, 2010 1:24 PM  
**To:** Clark, Roger  
**Subject:** FW: Incident 30241 - New Group Assignment Notification

Roger,

Another wikileaks hard drive request was put into ITSM for CIRT. I am passing it along to you. What do I need to do if anything?

V/R  
Chris Plummer

Advanced Cyber Threat and Forensic Analysis Team Office of the Secretary U.S. Department of Commerce

DOC-CIRT line (202) 482-4000  
Office: (202) 482-2580  
[cplummer@doc.gov](mailto:cplummer@doc.gov)

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

**From:** Sills, Taunya  
**Sent:** Friday, December 10, 2010 1:21 PM  
**To:** Plummer, Christopher  
**Cc:** Whiteside, Fred  
**Subject:** Fw: Incident 30241 - New Group Assignment Notification

Chris send Roger Clark an email regarding this user. This is one of the wiki leaks hard drive.

Remember to document in ITSM.

Thanks

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

**From:** [ITCSC@doc.gov](mailto:ITCSC@doc.gov) <[ITCSC@doc.gov](mailto:ITCSC@doc.gov)>  
**To:** OCIO-ITSM-CIRT  
**Sent:** Fri Dec 10 12:05:54 2010  
**Subject:** Incident 30241 - New Group Assignment Notification

CIRT,

A new assignment was created for your team on 12/10/2010 12:05 PM for incident number 30241.

The incident's information is as follows:

Summary: Employee Access

Customer Name: [REDACTED]  
Office: HCHB

(b)(6)

Category: Employee Access

Description: [REDACTED] hard drive was taken back but she needs to request files off of her machine. She is requesting files she has on my desktop with all my work in it."

Called "Shortcut to [REDACTED]"

Please review the assignment and follow up accordingly.

Thank you.

User Name

(b)(6)

[REDACTED]

Bureau

Other

Notes

OS

OS

OS

OS

BIS

BIS still reviewing logs to determine individual user

OIG

DOCFCU

EDA

Philadelphia

EDA

Chicago

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

NTIS

NTIS

NTIS

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

[illegible]

Jerusalem, Isreal

Islamabad, Pakistan

Passing addresses to line offices to match users  
Pending receipt of names

**Bold indicates updated names**  
**Updated as of 021630 Dec 10**

User Name

Bureau

Other

Notes

OS

OS

OS

OS

BIS

BIS still reviewing logs to determine individual user

OIG

DOCFCU

EDA

Philadelphia

EDA

Chicago

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

NTIS

NTIS

NTIS

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO



56

[REDACTED]

BEA  
BEA  
BEA  
BEA  
BEA  
BEA  
BEA  
BEA

Jerusalem, Isreal

Islamabad, Pakistan

**Bold indicates updated names**  
**Updated as of 021630 Dec 10**

## Clark, Roger

---

**From:** Plummer, Christopher  
**Sent:** Friday, December 10, 2010 1:25 PM  
**To:** Clark, Roger; Whiteside, Fred  
**Subject:** FW: Incident 30241 - New Group Assignment Notification

-----  
From: Clark, Roger  
Sent: Friday, December 10, 2010 1:25:20 PM  
To: Plummer, Christopher  
Subject: Re: Incident 30241 - New Group Assignment Notification Auto forwarded by a Rule

This is the same user.

----- Original Message -----  
From: Plummer, Christopher  
To: Clark, Roger  
Sent: Fri Dec 10 13:24:18 2010  
Subject: FW: Incident 30241 - New Group Assignment Notification

Roger,

Another wikileaks hard drive request was put into ITSM for CIRT. I am passing it along to you. What do I need to do if anything?

V/R  
Chris Plummer

Advanced Cyber Threat and Forensic Analysis Team Office of the Secretary U.S. Department of Commerce

DOC-CIRT line (202) 482-4000  
Office: (202) 482-2580  
[cplummer@doc.gov](mailto:cplummer@doc.gov)

-----Original Message-----  
From: Sills, Taunya  
Sent: Friday, December 10, 2010 1:21 PM  
To: Plummer, Christopher  
Cc: Whiteside, Fred  
Subject: Fw: Incident 30241 - New Group Assignment Notification

Chris send Roger Clark an email regarding this user. This is one of the wiki leaks hard drive.

Remember to document in ITSM.

Thanks

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

From: [ITCSC@doc.gov](mailto:ITCSC@doc.gov) <[ITCSC@doc.gov](mailto:ITCSC@doc.gov)>  
To: OCIO-ITSM-CIRT  
Sent: Fri Dec 10 12:05:54 2010  
Subject: Incident 30241 - New Group Assignment Notification

CIRT,

A new assignment was created for your team on 12/10/2010 12:05 PM for incident number 30241.

The incident's information is as follows:

Summary: Employee Access

Customer Name: [REDACTED]

Office: HCHB

Category: Employee Access

Description: [REDACTED] hard drive was taken back but she needs to request files off of her machine. She is requesting files she has on my desktop with all my work in it."

Called "Shortcut to [REDACTED]"

Please review the assignment and follow up accordingly.

Thank you.

**Incident: 31394****Status** Closed**Priority** 5**Customer Info****Notify Customer** ☒

**Network Login** (b)(6)@doc.gov  
**Full Name** (b)(6)  
**Email** (b)(6)@doc.gov  
**Phone/Ext** (202) 482 (b)(6)

**Operating Unit** OSEC  
**Office** OHRM  
**Sub-Office** OHRO  
**Room** 5206

**Department** ITCSC  
**Type** Request  
**Request Category** Network  
**Sub-Category** (None)  
**Item** (None)  
**Source** Web/Internet  
**Urgency** Low  
**Impact** Individual

**Summary**  
Security Incident - Wikileaks

**Description** (b)(6)  
(b)(6) his hard drive taken from his machine because he visited wikileaks. According to Amy when the hard drive was taken that it would be return back to the user within a week. It has been more than two weeks now since, but till this day the hard drive had not been returned. (b)(6) needs his hard drive back so that he can perform his duties.

**Created by:** emedeTPOC@doc.gov **On:** 12/20/2010 4:46 PM  
**Last Mod by:** tarth@doc.gov **On:** 1/4/2011 2:50 PM  
**Closed by:** tarth@doc.gov **On:** 1/4/2011 2:50 PM

## Journal

Type	Subject	Created On	Modified On
Journal Notes	new hard drive has been setup a wh	1/4/2011 2:50 PM	1/4/2011 2:50 PM
Journal Notes	Esteve created Incident # 32422 whi	1/4/2011 2:48 PM	1/4/2011 2:50 PM
Journal Notes	We asked Esteve a month ago to su	1/4/2011 11:27 AM	1/4/2011 11:28 AM
Journal Notes	We have let Esteve know to open an	1/4/2011 11:12 AM	1/4/2011 11:13 AM
Journal Notes	The client's	12/22/2010 1:25 PM	12/22/2010 1:34 PM
Journal Notes	I will contact Esteve and ask him for	12/21/2010 9:42 AM	12/21/2010 9:44 AM

## Audit History

Event Source	Field Name	Old Field Value	New Field Value	Created By	Created On
RecordAdd	Urgency		Low	emedetPOC@doc.gov	12/20/2010 4:49 PM
RecordAdd	Impact		Individual	emedetPOC@doc.gov	12/20/2010 4:49 PM
RecordAdd	ProfileFullName		Aftab Bukhari	emedetPOC@doc.gov	12/20/2010 4:49 PM

Created On
12/20/2010 4:49 PM
12/20/2010 4:49 PM
12/20/2010 4:49 PM

**Incident: 28883**

**VIP**

Status Active

Priority 3

Customer Info

Notify Customer ☒

Network Login [REDACTED]@doc.gov  
Full Name [REDACTED]  
Email [REDACTED]@doc.gov  
Phone/Ext 202-482-[REDACTED]

Operating Unit OSEC  
Office IO  
Sub-Office OPSP  
Room 5040

Department CIRT  
Type Request  
Request Category Security Incident  
Sub-Category  
Item


Summary  
Security Incident (Remove [REDACTED] Harddrive for  
Description  
The CIRT needs users drive as part of wiki leaks access

Source Phone  
Urgency Medium  
Impact Individual

Created by: JDarbre@doc.gov On: 12/1/2010 10:40 AM  
Last Mod by: JDarbre@doc.gov On: 12/1/2010 12:35 PM



## Attachment

Name	Created On	Modified On
 Cit Document.pdf	12/1/2010 10:47 AM	12/1/2010 10:53

**[REDACTED]**

Created On
12/1/2010 10:53 AM
12/1/2010 10:53 AM
12/1/2010 10:53 AM
12/1/2010 10:53 AM

**Incident: 28919**

Status Closed

Priority 4

## Customer Info

Notify Customer ☒

Network Login [REDACTED]@doc.gov  
Full Name [REDACTED]  
Email [REDACTED]@doc.gov  
Phone/Ext 202-487-[REDACTED]

Operating Unit OSEC  
Office OHRM  
Sub-Office HRITO  
Room 5204


Department CIRT  
Type Request  
Request Category Security Incident  
Sub-Category  
Item

Summary  
Security Incident (Remove [REDACTED] Harddrive for  
Description  
The CIRT needs users drive as part of wiki leaks access

Source Phone  
Urgency Medium  
Impact Individual

Created by: JDarbre@doc.gov On: 12/1/2010 12:06 PM  
Last Mod by: JDarbre@doc.gov On: 1/4/2011 11:04 AM  
Closed by: JDarbre@doc.gov On: 1/4/2011 11:04 AM

## Attachment

Name	Created On	Modified On
 Cirt Document.pdf	12/1/2010 12:14 PM	12/1/2010 12:14

**[REDACTED]**

Created On
12/1/2010 12:12 PM
12/1/2010 12:12 PM
12/1/2010 12:12 PM
1/4/2011 11:04 AM

# Incident: 28921

Status Active

Priority 4

## Customer Info

Notify Customer ☒

Network Login (b)(6) [redacted]@doc.gov  
Full Name (b)(6) [redacted]  
Email (b)(6) [redacted]@doc.gov  
Phone/Ext (202) 482- (b)(6)

Operating Unit OSEC  
Office OHRM  
Sub-Office OHRO  
Room 5206

Department CIRT  
Type Request  
Request Category Security Incident  
Sub-Category  
Item

Summary (b)(6)  
Security Incident (Remove (b)(6) Harddrive for  
Description  
The CIRT needs users drive as part of wiki leaks access

Source Phone  
Urgency Medium  
Impact Individual

Created by: JDarbre@doc.gov On: 12/1/2010 12:14 PM  
Last Mod by: fdecker@doc.gov On: 12/13/2010 2:31 PM

## Journal

Type	Subject	Created On	Modified On
Journal Notes	informed CIRT supervisor	12/13/2010 2:31 PM	12/13/2010 2:31 PM
Journal Notes	TPOC Esteve called for status	12/13/2010 12:33 PM	12/13/2010 12:36 PM

Created On
12/1/2010 12:16 PM
12/1/2010 12:16 PM
12/1/2010 12:16 PM



**Clark, Roger**

---

**From:** ITCSC@doc.gov  
**Sent:** Tuesday, December 21, 2010 8:29 AM  
**To:** OCIO-ITCSC  
**Subject:** Incident 31394 - New Group Assignment Notification

ITCSC,

A new assignment was created for your team on 12/21/2010 8:27 AM for incident number 31394.

The incident's information is as follows:

Summary: Security Incident - Wikileaks

Customer Name: [REDACTED]

Office: OHRM

Category: Network

Description: [REDACTED] had his hard drive taken from his machine because he visited wikileaks. According to Amy when the hard drive was taken that it would be return back to the user within a week. It has been more than two weeks now since, but till this day the hard drive had not been returned. [REDACTED] needs his hard drive back so that he can perform his duties.

Thank you,

Esteve

Please review the assignment and follow up accordingly.

Thank you.

**Clark, Roger**

---

**From:** ITCSC@doc.gov  
**Sent:** Wednesday, December 22, 2010 8:16 AM  
**To:** Arth, Terrence  
**Subject:** Incident 31394 - New Assignment Notification

tarth@doc.gov,

A new assignment was created for your you on 12/22/2010 8:14 AM for incident number 31394.

The incident's information is as follows:

Summary: Security Incident - Wikileaks

Customer Name: [REDACTED]  
Office: OHRM

Category: Network

Description: [REDACTED] had his hard drive taken from his machine because he visited wikileaks. According to Amy when the hard drive was taken that it would be return back to the user within a week. It has been more than two weeks now since, but till this day the hard drive had not been returned. [REDACTED] needs his hard drive back so that he can perform his duties.

Thank you,

Esteve

Please review the assignment and follow up accordingly.

Thank you.

**Clark, Roger**

---

**From:** Arth, Terrence  
**Sent:** Tuesday, January 04, 2011 2:47 PM  
**To:** Clark, Roger  
**Cc:** Arth, Terrence; Rogers, William; Arth, Robert  
**Subject:** Wikileaks -- Incident # 32422 -- Aftab Bukhari

Recent (b)(6) hard drive was pulled because of "Wikileaks". His TPOC, Esteve Mede, created Incident # 32422 which requests that we restore the following data and provide this to (b)(6). I have listed Esteve's e mail which lists what data Aftab requires from his old hard drive.

"the user got his hard drive taken because he went to WiliLeaks. The user needs the following folders back and applications re-install.

My Desktop  
My Documents  
Abukhari Folder"

Please let us know if you have any questions about this.

Thanks,

**Terrence Arth**  
**IT Customer Service Center**  
**Office of IT Services**  
**Office of the Chief Information Officer**  
**Office of the Secretary**  
**U.S. Department of Commerce**  
**Phone: (202)-482-5010**  
**Fax: (202)-501-6073**  
**itcsc@doc.gov**

**Clark, Roger**

---

**From:** Plummer, Christopher  
**Sent:** Wednesday, December 01, 2010 11:45 AM  
**To:** Clark, Roger  
**Cc:** Nguyen, Vu  
**Subject:** Wikileaks calls to CIRT

Roger,

Vu just told me to forward you everything I've gotten about Wikileaks today in case you wanted to follow up or provide more guidance:

- 1) [REDACTED] wanted to know why his drive was pulled yesterday. Robbie from helpdesk guessed it was in relation to Wikileaks (prior to DOC broadcast email this morning)
- 2) A gentleman from x21233 requested I pass along his comment that accessing Wikileaks does not represent a security incident (after broadcast email) I'm not really sure what to do with this one.
- 3) A third gentleman had comments about Wikileaks, but did not provide any info to me. His number was 571-272-3846

If you have any questions let me know.

v/r  
Chris Plummer

Computer Incident Response Team (CIRT)  
Office of the Secretary  
U.S. Department of Commerce

Office: (202) 482-2580  
[cplummer@doc.gov](mailto:cplummer@doc.gov)

## User Name

## Bureau

## Other

## Notes

OS

Drive secured in OCIO/NCSP

OS

Drive secured in OCIO/NCSP

OS

Drive secured in OCIO/NCSP

OS

Drive secured in OCIO/NCSP

BIS

BIS still reviewing logs to determine individual user

OIG

DOFCU

EDA

Philadelphia

Drive secured in OCIO/NCSP

EDA

Chicago

Drive secured in OCIO/NCSP

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

Census

NTIS

Confirmed no classified by NTIS IT Security Staff

NTIS

Confirmed no classified by NTIS IT Security Staff

NTIS

Confirmed no classified by NTIS IT Security Staff

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

USPTO

(b)(6)

(b)(6)

1076

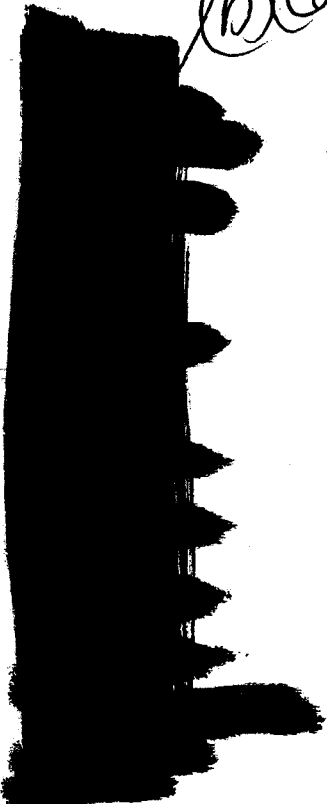
# NOBIA

17

# HOE11NOAA

10/10/10

**Remove misidentified per NIST**



(b)(6)

NIST	Div 610	
NIST	Div 191	
NIST	Div 688	
NIST	Div 682	
NIST	Div 183	
NIST	Div 775	
NIST	Div 732	
NIST	Div 653	
NIST	Div 181	
NIST	Div 730	
NIST	Div 688	
NIST	Div 488	
NIST	Div 687	
NIST	Div 730	
NIST	Div 610	
NIST	Div 773	
NIST	Div 470	
NIST	Div 620	
NIST	Div 697	
NIST	Div 181	
NIST	Div 774	
<b>NIST</b>	<b>Div 774</b>	Replaces GodII
NIST	Div 684	
NIST	Div 470	
NIST	Div 773	To be determined



Running Total Department-wide: 174

Bold indicates updated names  
Updated as of 060855 Dec 10  
Note: NTIA & MBDA 0 hits

**Clark, Roger**

---

**From:** Scalsky, Terry  
**Sent:** Wednesday, December 01, 2010 7:49 AM  
**To:** 'stan scalsky'  
**Subject:** RE: boa

OK - since we already have the account it won't impact our score.  
Here's the directions for wikilieaks. You won't believe them.

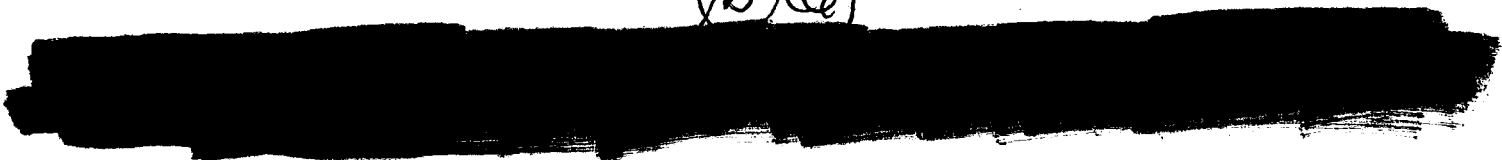
The following action is to be taken on all PC's identified as accessing the WikiLeaks.org site since Friday, Nov 26th:

- 1) Immediately disconnect the PC from the network
- 2) Remove the hard drive and replace with a new hard drive.
- 3) Do not copy user data from the removed drive to the new drive.
- 4) Label the removed hard drive with the user name.
- 5) Label the removed hard drive as potentially having classified material.
- 6) The drive should be treated as containing Secret material.
- 7) Store the removed hard drive in a GSA approved safe until further guidance is provided or forward the hard drive (packaged in accordance with the DOC Security Manual for transporting Secret material) to:

Terry Scalsky  
Security Operations Center Manager  
Office of Security, Infrastructure and Technology Office of the Chief Information Officer  
Department of Commerce  
202-482-3775 (o) 202-657-8331 (m)

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

**From:** stan scalsky [mailto: (b)(6)]  
**Sent:** Wednesday, December 01, 2010 7:15 AM  
**To:** Scalsky, Terry  
**Subject:** boa (b)(6)





**Clark, Roger**

---

**From:** ITCSC@doc.gov  
**Sent:** Wednesday, December 01, 2010 1:28 PM  
**To:** OCIO-ITSM-NOC  
**Subject:** Incident 28863 - New Group Assignment Notification

NOC,

A new assignment was created for your team on 12/1/2010 11:37 AM for incident number 28863.

The incident's information is as follows:

Summary: Network - Scan

Customer Name: [REDACTED] (b)(6)

Office: HCHB

Category: Network

Description: Attn: SOC/NOC: Our Internal network does not consist of the Web filtering/Firewall tools to perform the detail scan of Site access to Wikileaks.org for MBDA Desktop computers. Since MBDA Internet access is filtered and secured via the Web Security infrastructure implemented at the SOC/NOC could you perform a scan for MBDA IP address segment listed below?

[REDACTED] (b)(2)

Could you please provide a report of the results for the scan to us via electronic (Email, Text Document, Excel, etc...) or Media (CD, DVD). This will be so that we can cross reference the IP Address to Hostname assigned in the event any MBDA Desktop/Machines are identified. If there are any questions or to contact me, I can be reached at:

Direct Line: 202 482-6279

Blackberry: 202 422-2419

Email: [khill@mbda.gov](mailto:khill@mbda.gov)

Please review the assignment and follow up accordingly.

Thank you.

## Clark, Roger

---

**From:** Sills, Taunya  
**Sent:** Friday, December 10, 2010 1:35 PM  
**To:** Plummer, Christopher  
**Subject:** Re: Incident 30241 - New Group Assignment Notification

There is an existing ticket for this user.

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

**From:** Plummer, Christopher  
**To:** Clark, Roger  
**Cc:** DOC-CIRT  
**Sent:** Fri Dec 10 13:30:35 2010  
**Subject:** RE: Incident 30241 - New Group Assignment Notification

Same user as who? I just got the ticket notification, and according to ITSM it was created about an hour ago.

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

**From:** Clark, Roger  
**Sent:** Friday, December 10, 2010 1:25 PM  
**To:** Plummer, Christopher  
**Subject:** Re: Incident 30241 - New Group Assignment Notification

This is the same user.

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

**From:** Plummer, Christopher  
**To:** Clark, Roger  
**Sent:** Fri Dec 10 13:24:18 2010  
**Subject:** FW: Incident 30241 - New Group Assignment Notification

Roger,

Another wikileaks hard drive request was put into ITSM for CIRT. I am passing it along to you. What do I need to do if anything?

V/R  
Chris Plummer

Advanced Cyber Threat and Forensic Analysis Team Office of the Secretary U.S. Department of Commerce

DOC-CIRT line (202) 482-4000  
Office: (202) 482-2580  
[cplummer@doc.gov](mailto:cplummer@doc.gov)

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

**From:** Sills, Taunya  
**Sent:** Friday, December 10, 2010 1:21 PM  
**To:** Plummer, Christopher  
**Cc:** Whiteside, Fred

Subject: Fw: Incident 30241 - New Group Assignment Notification

Chris send Roger Clark an email regarding this user. This is one of the wiki leaks hard drive.

Remember to document in ITSM.

Thanks

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

From: [ITCSC@doc.gov](mailto:ITCSC@doc.gov) <[ITCSC@doc.gov](mailto:ITCSC@doc.gov)>

To: OCIO-ITSM-CIRT

Sent: Fri Dec 10 12:05:54 2010

Subject: Incident 30241 - New Group Assignment Notification

CIRT,

A new assignment was created for your team on 12/10/2010 12:05 PM for incident number 30241.

The incident's information is as follows:

Summary: Employee Access

Customer Name: [REDACTED]

Office: HCHB

(b)(6)

Category: Employee Access

Description: [REDACTED] hard drive was taken back but she needs to request files off of her machine. She is requesting files she has on my desktop with all my work in it."

Called "Shortcut to [REDACTED]"

(b)(6)

Please review the assignment and follow up accordingly.

Thank you.

**Clark, Roger**

---

**From:** Decker, Fred  
**Sent:** Monday, December 13, 2010 2:32 PM  
**To:** Clark, Roger  
**Cc:** Rogers, William; Darbre, Jack  
**Subject:** Incident 28921...

Roger,

Just a heads up on a user who had his drive taken due to the Wikileaks episode and is now providing information to the CIRT on what folders he would like to be made available to him since the drive can not be given back to him! All items within the "My Documents" folder, all items within a folder called [REDACTED] all "Desktop" items and all "Favorites" folder items for Internet Explorer.

I will input this information in the journal of this incident since the CIRT is already assigned.

Thank Roger

FRED

*Frederick A. Decker*

Frederick A. Decker

IT Customer Service Center

HCHB Room 6071

[ITCSC@doc.gov](mailto:ITCSC@doc.gov)

202-482-5010

**Clark, Roger**

---

**From:** Slebodnik, Alisha  
**Sent:** Friday, December 17, 2010 10:00 AM  
**To:** Nguyen, Vu  
**Cc:** Plummer, Christopher  
**Subject:** RE: Meeting

Vu,

Chris and I have had a couple of phone calls about users asking when they are getting their hard drives back. The users in question are (b)(6), who has is taken because of wikileaks and the other is (b)(6) whose hard drive was also taken because of wikileaks. We wanted to give them a time frame of when they will receive them because they have information on their needed for their work.

Thanks.

r/

Alisha Slebodnik  
Advanced Cyber Threat and Forensic Analysis Team U.S. Department of Commerce Office of the Secretary  
DOC-CIRTL: 202.482.4000  
Office: 202.482.1508  
[aslebodnik@doc.gov](mailto:aslebodnik@doc.gov)

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

**From:** Nguyen, Vu  
**Sent:** Friday, December 17, 2010 9:41 AM  
**To:** DOC-CIRT  
**Subject:** Meeting

Team,

Our meeting for this morning is cancel.

Thanks,  
Vu

Clark, Roger

---

**From:** Arth, Robert  
**Sent:** Wednesday, December 01, 2010 11:41 AM  
**To:** Rogers, William  
**Cc:** Johnson, Dale  
**Subject:** Incident 28879

Bill:

As directed, I stopped down to [REDACTED] office (OPA, Rm. 5040) at 10:40am this morning to re-image his machine with a new drive – his was one of the drives that were pulled yesterday due to the WikiLeaks issue. We had been advised to have the users contact the CIRT for further information. When ITCSC arrived at [REDACTED] office, I let him know I was there to re-image his machine and that if he wanted further information he would have to call CIRT at x24000. While I was re-imaging the machine with a new drive, [REDACTED] called CIRT. Chris Plummer (CIRT) answered and after [REDACTED] explained why he was calling, he was told that CIRT did not have his old drive and also were not sure why his drive had been pulled. CIRT then asked to talk to me about this – I got on the line with CIRT and let them know that Amy Hintz had informed us of the issue yesterday afternoon and that we had been directed to have the users affected by this incident to call CIRT. Chris Plummer then asked me, "Who is Amy? Does she work at the Help Desk?" I informed him that Amy worked for Wayne Blackwood, but not at the ITCSC. Chris Plummer then reiterated that he did not know about any drives that had been pulled for or by CIRT – he then said he had heard about four new PCs for Ken Ford and asked if this is what we were calling about. I told him that was not it. He then mentioned WikiLeaks and I said that [REDACTED] drive was related to that. He then asked to be put back on with [REDACTED]. After [REDACTED] finished talking to CIRT, he let me know he had been told that the CIRT did not know about his drive, had not pulled his drive and that he should "maybe call Roger Clark about it." [REDACTED] then asked me who Roger Clark was since CIRT did not elaborate on this information for him. Shortly after this, I finished re-imaging the user's computer with a new drive, so he is up and running at this time, but he did want to know who had his old hard drive and who he could talk to about it – I let him know I would pass his concerns along to my management.

Regards,

Robby Arth  
IT Customer Service Center  
Office of IT Services  
Office of the Chief Information Officer  
Office of the Secretary  
U.S. Department of Commerce  
Phone: 202-482-5010  
Fax: 202-501-6073  
[itcsc@doc.gov](mailto:itcsc@doc.gov)

**Clark, Roger**

---

**From:** Harper, Pam  
**Sent:** Wednesday, December 01, 2010 11:59 AM  
**To:** Rogers, William  
**Cc:** Blackwood, Wayne  
**Subject:** RE: Incident 28879

Thanks Bill. I am addressing this with Wayne.

Pam

**From:** Rogers, William  
**Sent:** Wednesday, December 01, 2010 11:44 AM  
**To:** Harper, Pam  
**Cc:** Blackwood, Wayne  
**Subject:** FW: Incident 28879  
**Importance:** High

FYI

We have had another incident with the CIRT. When we pulled the drives yesterday afternoon Amy instructed us to point the users to the CIRT for further info. Below is a synopsis of a conversation this morning between a user and the CIRT about their drive/data.

**Bill Rogers**  
IT Customer Service Center  
Office of IT Services  
Office of the Chief Information Officer  
Office of the Secretary  
U.S. Department of Commerce  
Phone: (202)-482-5010  
Fax: (202)-501-6073  
[itcsc@doc.gov](mailto:itcsc@doc.gov)

**From:** Arth, Robert  
**Sent:** Wednesday, December 01, 2010 11:41 AM  
**To:** Rogers, William  
**Cc:** Johnson, Dale  
**Subject:** Incident 28879

Bill:

(b)(6)

As directed, I stopped down to [REDACTED] office (OPA, Rm. 5040) at 10:40am this morning to re-image his machine with a new drive – his was one of the drives that were pulled yesterday due to the WikiLeaks issue. We had been advised to have the users contact the CIRT for further information. When ITCSC arrived at [REDACTED] office, I let him know I was there to re-image his machine and that if he wanted further information he would have to call CIRT at 240000. While I was re-imaging the machine with a new drive, [REDACTED] called CIRT. Chris Plummer (CIRT) answered and after [REDACTED] explained why he was calling, he was told that CIRT did not have his old drive and also were not sure why his drive had been pulled. CIRT then asked to talk to me about this – I got on the line with CIRT and let them know that Amy Hintz had informed us of the issue yesterday afternoon and that we had been directed to have the users affected by this incident to call CIRT. Chris Plummer then asked me, "Who is Amy? Does she work at the Help Desk?" I informed him that Amy worked for Wayne Blackwood, but not at the ITCSC. Chris Plummer then reiterated that he did not know about any drives that had been pulled for or by CIRT – he then said he had heard about four new PCs for Ken

(b)(6)

(b)(6) (b)(6)

Ford and asked if this is what we were calling about. I told him that was not it. He then mentioned WikiLeaks and I said that [REDACTED] drive was related to that. He then asked to be put back on with [REDACTED]. After [REDACTED] finished talking to CIRT, he let me know he had been told that the CIRT did not know about his drive, had not pulled his drive and that he should "maybe call Roger Clark about it." [REDACTED] then asked me who Roger Clark was since CIRT did not elaborate on this information for him. Shortly after this, I finished re-imaging the user's computer with a new drive, so he is up and running at this time, but he did want to know who had his old hard drive and who he could talk to about it – I let him know I would pass his concerns along to my management.

Regards,

Robby Arth  
IT Customer Service Center  
Office of IT Services  
Office of the Chief Information Officer  
Office of the Secretary  
U.S. Department of Commerce  
Phone: 202-482-5010  
Fax: 202-501-6073  
[itcsc@doc.gov](mailto:itcsc@doc.gov)



**Clark, Roger**

---

**From:** Rogers, William  
**Sent:** Wednesday, December 01, 2010 11:44 AM  
**To:** Harper, Pam  
**Cc:** Blackwood, Wayne  
**Subject:** FW: Incident 28879

**Importance:** High

FYI

We have had another incident with the CIRT. When we pulled the drives yesterday afternoon Amy instructed us to point the users to the CIRT for further info. Below is a synopsis of a conversation this morning between a user and the CIRT about their drive/data.

**Bill Rogers**  
**IT Customer Service Center**  
**Office of IT Services**  
**Office of the Chief Information Officer**  
**Office of the Secretary**  
**U.S. Department of Commerce**  
**Phone: (202)-482-5010**  
**Fax: (202)-501-6073**  
**itcsc@doc.gov**

---

**From:** Arth, Robert  
**Sent:** Wednesday, December 01, 2010 11:41 AM  
**To:** Rogers, William  
**Cc:** Johnson, Dale  
**Subject:** Incident 28879

Bill:

As directed, I stopped down to [REDACTED] office (OPA, Rm. 5040) at 10:40am this morning to re-image his machine with a new drive – his was one of the drives that were pulled yesterday due to the WikiLeaks issue. We had been advised to have the users contact the CIRT for further information. When ITCSC arrived at [REDACTED] office, I let him know I was there to re-image his machine and that if he wanted further information he would have to call CIRT at x24000. While I was re-imaging the machine with a new drive, [REDACTED] called CIRT. Chris Plummer (CIRT) answered and after [REDACTED] explained why he was calling, he was told that CIRT did not have his old drive and also were not sure why his drive had been pulled. CIRT then asked to talk to me about this – I got on the line with CIRT and let them know that Amy Hintz had informed us of the issue yesterday afternoon and that we had been directed to have the users affected by this incident to call CIRT. Chris Plummer then asked me, "Who is Amy? Does she work at the Help Desk?" I informed him that Amy worked for Wayne Blackwood, but not at the ITCSC. Chris Plummer then reiterated that he did not know about any drives that had been pulled for or by CIRT – he then said he had heard about four new PCs for Ken Ford and asked if this is what we were calling about. I told him that was not it. He then mentioned WikiLeaks and I said that [REDACTED] drive was related to that. He then asked to be put back on with [REDACTED]. After [REDACTED] finished talking to CIRT, he let me know he had been told that the CIRT did not know about his drive, had not pulled his drive and that he should "maybe call Roger Clark about it." Mr. [REDACTED] then asked me who Roger Clark was since CIRT did not elaborate on this information for him. Shortly after this, I finished re-imaging the user's computer with a new drive, so he is up and running at this time, but he did want to know who had his old hard drive and who he could talk to about it – I let him know I would pass his concerns along to my management.

Regards,

Robby Arth  
IT Customer Service Center  
Office of IT Services  
Office of the Chief Information Officer  
Office of the Secretary  
U.S. Department of Commerce  
Phone: 202-482-5010  
Fax: 202-501-6073  
[itcsc@doc.gov](mailto:itcsc@doc.gov)

## Clark, Roger

---

**From:** Blackwood, Wayne  
**Sent:** Wednesday, December 01, 2010 1:24 PM  
**To:** Harper, Pam  
**Subject:** RE: Incident 28879

Got it.

Wayne S. Blackwood  
Director  
Office of IT Services  
Office of the Chief Information Officer  
Office of the Secretary  
U.S. Department of Commerce  
Phone 202-482-3175  
Cell 202-957-6342  
Fax 202-219-2444  
[wblackwood@doc.gov](mailto:wblackwood@doc.gov)

**From:** Harper, Pam  
**Sent:** Wednesday, December 01, 2010 11:59 AM  
**To:** Blackwood, Wayne  
**Subject:** FW: Incident 28879  
**Importance:** High

Can you address this with Earl? I think that this is giving the ITCSC a bad name. Obviously there is little communication within Earl's teams.

**From:** Rogers, William  
**Sent:** Wednesday, December 01, 2010 11:44 AM  
**To:** Harper, Pam  
**Cc:** Blackwood, Wayne  
**Subject:** FW: Incident 28879  
**Importance:** High

FYI

We have had another incident with the CIRT. When we pulled the drives yesterday afternoon Amy instructed us to point the users to the CIRT for further info. Below is a synopsis of a conversation this morning between a user and the CIRT about their drive/data.

Bill Rogers  
IT Customer Service Center  
Office of IT Services  
Office of the Chief Information Officer  
Office of the Secretary  
U.S. Department of Commerce  
Phone: (202)-482-5010  
Fax: (202)-501-6073  
[itcsc@doc.gov](mailto:itcsc@doc.gov)

**From:** Arth, Robert  
**Sent:** Wednesday, December 01, 2010 11:41 AM  
**To:** Rogers, William

**Clark, Roger**

---

**From:** Plummer, Christopher  
**Sent:** Friday, December 10, 2010 1:31 PM  
**To:** Clark, Roger  
**Cc:** DOC-CIRT  
**Subject:** RE: Incident 30241 - New Group Assignment Notification

Same user as who? I just got the ticket notification, and according to ITSM it was created about an hour ago.

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

**From:** Clark, Roger  
**Sent:** Friday, December 10, 2010 1:25 PM  
**To:** Plummer, Christopher  
**Subject:** Re: Incident 30241 - New Group Assignment Notification

This is the same user.

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

**From:** Plummer, Christopher  
**To:** Clark, Roger  
**Sent:** Fri Dec 10 13:24:18 2010  
**Subject:** FW: Incident 30241 - New Group Assignment Notification

Roger,

Another wikileaks hard drive request was put into ITSM for CIRT. I am passing it along to you. What do I need to do if anything?

V/R  
Chris Plummer

Advanced Cyber Threat and Forensic Analysis Team Office of the Secretary U.S. Department of Commerce

DOC-CIRT line (202) 482-4000  
Office: (202) 482-2580  
[cplummer@doc.gov](mailto:cplummer@doc.gov)

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

**From:** Sills, Taunya  
**Sent:** Friday, December 10, 2010 1:21 PM  
**To:** Plummer, Christopher  
**Cc:** Whiteside, Fred  
**Subject:** Fw: Incident 30241 - New Group Assignment Notification

Chris send Roger Clark an email regarding this user. This is one of the wiki leaks hard drive.

Remember to document in ITSM.

Thanks

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

From: ITCSC@doc.gov <ITCSC@doc.gov>

To: OCIO-ITSM-CIRT

Sent: Fri Dec 10 12:05:54 2010

Subject: Incident 30241 - New Group Assignment Notification

CIRT,

A new assignment was created for your team on 12/10/2010 12:05 PM for incident number 30241.

The incident's information is as follows:

Summary: Employee Access

Customer Name: [REDACTED]

Office: HCHB

Category: Employee Access

Description: [REDACTED] hard drive was taken back but she needs to request files off of her machine. She is requesting files she has on my desktop with all my work in it."

Called "Shortcut to [REDACTED]"

Please review the assignment and follow up accordingly.

Thank you.

Clark, Roger

---

From: Clark, Roger  
Sent: Friday, December 10, 2010 1:25 PM  
To: Plummer, Christopher  
Subject: Re: Incident 30241 - New Group Assignment Notification

This is the same user.

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

From: Plummer, Christopher  
To: Clark, Roger  
Sent: Fri Dec 10 13:24:18 2010  
Subject: FW: Incident 30241 - New Group Assignment Notification

Roger,

Another wikileaks hard drive request was put into ITSM for CIRT. I am passing it along to you. What do I need to do if anything?

V/R  
Chris Plummer

Advanced Cyber Threat and Forensic Analysis Team Office of the Secretary U.S. Department of Commerce

DOC-CIRT line (202) 482-4000  
Office: (202) 482-2580  
[cplummer@doc.gov](mailto:cplummer@doc.gov)

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

From: Sills, Taunya  
Sent: Friday, December 10, 2010 1:21 PM  
To: Plummer, Christopher  
Cc: Whiteside, Fred  
Subject: Fw: Incident 30241 - New Group Assignment Notification

Chris send Roger Clark an email regarding this user. This is one of the wiki leaks hard drive.

Remember to document in ITSM.

Thanks

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

From: [ITCSC@doc.gov](mailto:ITCSC@doc.gov) <[ITCSC@doc.gov](mailto:ITCSC@doc.gov)>  
To: OCIO-ITSM-CIRT  
Sent: Fri Dec 10 12:05:54 2010  
Subject: Incident 30241 - New Group Assignment Notification

CIRT,

A new assignment was created for your team on 12/10/2010 12:05 PM for incident number 30241.

The incident's information is as follows:

Summary: Employee Access

Customer Name: [REDACTED] (b)(6)  
Office: HCHB

Category: Employee Access

Description: [REDACTED] hard drive was taken back but she needs to request files off of her machine. She is requesting files she has on my desktop with all my work in it."

Called "Shortcut to [REDACTED] (b)(6)

Please review the assignment and follow up accordingly.

Thank you.

**Subject:** IMPORTANT - RE: Guidance regarding WikiLeaks

**From:** "Glenn, K. Robert" <robert.glenn@nist.gov>

**Date:** Mon, 6 Dec 2010 11:30:01 -0500

**To:** "[REDACTED]" <[REDACTED]@nist.gov>

**CC:** "Glenn, K. Robert" <robert.glenn@nist.gov>

Dear [REDACTED] (b)(6)

I am the NIST IT Security Officer and I have been asked to contact all NIST staff who may have had a computer that connected to WikiLeaks prior to the guidance issued by DoC.

~~Please be assured, that due to the nature of this issue, while this deals with access to~~  
potential classified information and we are required by DoC to respond to this incident, no one at NIST who went to the site prior to the guidance issued by DoC is going to get into any trouble. In fact, several NIST staff computers connected to the site prior to the issuance of the DoC guidance.

DOC has confirmed that WikiLeaks was accessed from a computer registered to you, which may mean classified information was unknowingly accessed. Because access occurred prior to receiving guidance from DOC (see below), this is viewed as an unintentional incident. However, NIST is required to treat the computer as though there is classified data resident (i.e., classified information spillage) and, the computer must be appropriately sanitized to ensure that any classified information is removed.

**The NIST Office of Information Systems Management (formerly OCIO) incident response team (John Antonishek, Jeff McIntyre, David Kustaborder, Al Hurst, or Matt Loebach) will contact you to schedule sanitization of the computer.** Please do not access, read, forward, or otherwise move any WikiLeaks documents that may have been downloaded. Also, please do not attempt to remove any such documents on your own. Sanitization will include removal of the information in your browser cache/history, temporary files, backups that may contain WikiLeaks documentation, etc., and verification that the information was not forwarded via other methods such as email, instant messaging, etc. Every effort will be made to preserve all other user data on the computer (i.e. ***this is a routine process and user data should not be affected***). Given the number of incidents within NIST, we ask for your patience in scheduling sanitization. Since classified information is involved, **the DOC Office of Security (OSY) will likely follow up and send you an inadvertent disclosure briefing which includes a reminder to not disclose any sensitive information you may have seen when going to the WikiLeaks site.**

As a reminder, please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents.

Please do not hesitate to contact me personally if you have any questions or concerns.

Regards,

Rob Glenn  
IT Security Officer, NIST



rob.glenn@nist.gov  
301-975-3667

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

From: allstaff@nist.gov [mailto:allstaff@nist.gov] On Behalf Of NIST IT Assistance Center  
Sent: Wednesday, December 01, 2010 2:45 PM  
To: Multiple recipients of list  
Subject: RE: Guidance regarding WikiLeaks

Attention NIST Staff:

---

To clarify the guidance that the Department of Commerce issued earlier today we ask that you not use the Commerce contact information provided in that email. Instead, direct any questions or notifications of access to WikiLeaks documents to the NIST IT Assistance Center (iTAC).

iTAC  
IT Assistance Center  
itac@nist.gov

303-497-5375 (Boulder)  
301-975-5375 (Gaithersburg)

Hours of Operation:

Boulder: 7:30am - 5:30pm (Mountain Time) Monday - Friday  
Gaithersburg: 7:30am - 5:30pm (Eastern Time) Monday - Friday

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

From: allstaff@nist.gov [mailto:allstaff@nist.gov] On Behalf Of Broadcast, DOC  
Sent: Wednesday, December 01, 2010 11:11 AM  
To: Multiple recipients of list  
Subject: Guidance regarding WikiLeaks

To: All Commerce Employees and Contractors

Recent reports indicate that a number of government documents have been posted on the WikiLeaks website. These documents may or may not contain information that is considered National Security Information (classified information) and as such, the information is NOT authorized for downloading, viewing, printing, processing, copying, or transmitting via non-classified Government-issued computers, laptops, blackberries, or other communication devices and is not an authorized use of DOC IT equipment. Doing so would introduce potentially classified information onto our unclassified networks and represent a potential security incident.

There has been a rumor that the information is no longer classified since it resides in the public domain. This is NOT true. Executive Order 13526, Section 1.1(4)(2) states "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information." The information was neither properly nor improperly "declassified" by the appropriate authority and requires continued classification or reclassification.

Please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents because these documents may contain classified information. Accessing the WikiLeaks documents will lead to sanitization of your PC to remove any potentially

IMPORTANT - RE: Guidance regarding WikiLeaks

classified information from the system and result in possible data loss.

If you have questions regarding this broadcast or have accessed the WikiLeaks documents, please contact the DOC Computer Incident Response Team at email [doc-cirt@doc.gov](mailto:doc-cirt@doc.gov) or call (202) 482-4000.

---

This message was authorized by the Office of Secretary OSY/OCIO.

Please do not reply to this message. The broadcast email account is not monitored for incoming mail.

---

**Subject:** IMPORTANT - RE: Guidance regarding WikiLeaks

**From:** "Glenn, K. Robert" <robert.glenn@nist.gov>

**Date:** Mon, 6 Dec 2010 11:34:24 -0500

**To:** "[REDACTED]@nist.gov"

**CC:** "Glenn, K. Robert" <robert.glenn@nist.gov>

Dear [REDACTED],

I am the NIST IT Security Officer and I have been asked to contact all NIST staff who may have had a computer that connected to WikiLeaks prior to the guidance issued by DoC. Please be assured, that due to the nature of this issue, while this deals with access to potential classified information and we are required by DoC to respond to this incident, no one at NIST who went to the site prior to the guidance issued by DoC is going to get into any trouble. In fact, several NIST staff computers connected to the site prior to the issuance of the DoC guidance.

DOC has confirmed that WikiLeaks was accessed from a computer registered to you, which may mean classified information was unknowingly accessed. Because access occurred prior to receiving guidance from DOC (see below), this is viewed as an unintentional incident. However, NIST is required to treat the computer as though there is classified data resident (i.e., classified information spillage) and, the computer must be appropriately sanitized to ensure that any classified information is removed.

**The NIST Office of Information Systems Management (formerly OCIO) incident response team (John Antonishek, Jeff McIntyre, David Kustaborder, Al Hurst, or Matt Loebach) will contact you to schedule sanitization of the computer.** Please do not access, read, forward, or otherwise move any WikiLeaks documents that may have been downloaded. Also, please do not attempt to remove any such documents on your own. Sanitization will include removal of the information in your browser cache/history, temporary files, backups that may contain WikiLeaks documentation, etc., and verification that the information was not forwarded via other methods such as email, instant messaging, etc. Every effort will be made to preserve all other user data on the computer (i.e. **this is a routine process and user data should not be affected**). Given the number of incidents within NIST, we ask for your patience in scheduling sanitization. Since classified information is involved, **the DOC Office of Security (OSY) will likely follow up and send you an inadvertent disclosure briefing which includes a reminder to not disclose any sensitive information you may have seen when going to the WikiLeaks site.**

As a reminder, please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents.

Please do not hesitate to contact me personally if you have any questions or concerns.

Regards,

Rob Glenn  
IT Security Officer, NIST

rob.glenn@nist.gov  
301-975-3667

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

From: allstaff@nist.gov [mailto:allstaff@nist.gov] On Behalf Of NIST IT Assistance Center  
Sent: Wednesday, December 01, 2010 2:45 PM  
To: Multiple recipients of list  
Subject: RE: Guidance regarding WikiLeaks

Attention NIST Staff:

---

To clarify the guidance that the Department of Commerce issued earlier today we ask that you not use the Commerce contact information provided in that email. Instead, direct any questions or notifications of access to WikiLeaks documents to the NIST IT Assistance Center (ITAC).

ITAC  
IT Assistance Center  
itac@nist.gov

303-497-5375 (Boulder)  
301-975-5375 (Gaithersburg)

Hours of Operation:

Boulder: 7:30am - 5:30pm (Mountain Time) Monday - Friday  
Gaithersburg: 7:30am - 5:30pm (Eastern Time) Monday - Friday

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

From: allstaff@nist.gov [mailto:allstaff@nist.gov] On Behalf Of Broadcast, DOC  
Sent: Wednesday, December 01, 2010 11:11 AM  
To: Multiple recipients of list  
Subject: Guidance regarding WikiLeaks

To: All Commerce Employees and Contractors

Recent reports indicate that a number of government documents have been posted on the WikiLeaks website. These documents may or may not contain information that is considered National Security Information (classified information) and as such, the information is NOT authorized for downloading, viewing, printing, processing, copying, or transmitting via non-classified Government-issued computers, laptops, blackberries, or other communication devices and is not an authorized use of DOC IT equipment. Doing so would introduce potentially classified information onto our unclassified networks and represent a potential security incident.

There has been a rumor that the information is no longer classified since it resides in the public domain. This is NOT true. Executive Order 13526, Section 1.1(4)(2) states "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information." The information was neither properly nor improperly "declassified" by the appropriate authority and requires continued classification or reclassification.

Please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents because these documents may contain classified information. Accessing the WikiLeaks documents will lead to sanitization of your PC to remove any potentially

classified information from the system and result in possible data loss.

If you have questions regarding this broadcast or have accessed the WikiLeaks documents, please contact the DOC Computer Incident Response Team at email [doc-cirt@doc.gov](mailto:doc-cirt@doc.gov) or call (202) 482-4000.

---

This message was authorized by the Office of Secretary OSY/OCIO.

Please do not reply to this message. The broadcast email account is not monitored for incoming mail.

---

**Subject:** RE: IMPORTANT - RE: Guidance regarding WikiLeaks

**From:** "Glenn, K. Robert" <robert.glenn@nist.gov>

**Date:** Mon, 6 Dec 2010 11:36:44 -0500

**To:** "[REDACTED] <[REDACTED]@nist.gov>

**CC:** "Glenn, K. Robert" <robert.glenn@nist.gov>

Dear [REDACTED] (b)(6)

I am the NIST IT Security Officer and I have been asked to contact all NIST staff who may have had a computer that connected to WikiLeaks prior to the guidance issued by DoC.

~~Please be assured, that due to the nature of this issue, while this deals with access to~~  
potential classified information and we are required by DoC to respond to this incident, no one at NIST who went to the site prior to the guidance issued by DoC is going to get into any trouble. In fact, several NIST staff computers connected to the site prior to the issuance of the DoC guidance.

DOC has confirmed that WikiLeaks was accessed from a computer registered to you, which may mean classified information was unknowingly accessed. Because access occurred prior to receiving guidance from DOC (see below), this is viewed as an unintentional incident. However, NIST is required to treat the computer as though there is classified data resident (i.e., classified information spillage) and, the computer must be appropriately sanitized to ensure that any classified information is removed.

**The NIST Office of Information Systems Management (formerly OCIO) incident response team (John Antonishek, Jeff McIntyre, David Kustaborder, Al Hurst, or Matt Loebach) will contact you to schedule sanitization of the computer.** Please do not access, read, forward, or otherwise move any WikiLeaks documents that may have been downloaded. Also, please do not attempt to remove any such documents on your own. Sanitization will include removal of the information in your browser cache/history, temporary files, backups that may contain WikiLeaks documentation, etc., and verification that the information was not forwarded via other methods such as email, instant messaging, etc. Every effort will be made to preserve all other user data on the computer (i.e. **this is a routine process and user data should not be affected**). Given the number of incidents within NIST, we ask for your patience in scheduling sanitization. Since classified information is involved, **the DOC Office of Security (OSY) will likely follow up and send you an inadvertent disclosure briefing which includes a reminder to not disclose any sensitive information you may have seen when going to the WikiLeaks site.**

As a reminder, please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents.

Please do not hesitate to contact me personally if you have any questions or concerns.

Regards,

Rob Glenn  
IT Security Officer, NIST

rob.glenn@nist.gov  
301-975-3667

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

From: allstaff@nist.gov [mailto:allstaff@nist.gov] On Behalf Of NIST IT Assistance Center  
Sent: Wednesday, December 01, 2010 2:45 PM  
To: Multiple recipients of list  
Subject: RE: Guidance regarding WikiLeaks

Attention NIST Staff:

~~To clarify the guidance that the Department of Commerce issued earlier today we ask that you not use the Commerce contact information provided in that email. Instead, direct any questions or notifications of access to WikiLeaks documents to the NIST IT Assistance Center (ITAC).~~

ITAC  
IT Assistance Center  
itac@nist.gov

303-497-5375 (Boulder)  
301-975-5375 (Gaithersburg)

Hours of Operation:

Boulder: 7:30am - 5:30pm (Mountain Time) Monday - Friday  
Gaithersburg: 7:30am - 5:30pm (Eastern Time) Monday - Friday

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

From: allstaff@nist.gov [mailto:allstaff@nist.gov] On Behalf Of Broadcast, DOC  
Sent: Wednesday, December 01, 2010 11:11 AM  
To: Multiple recipients of list  
Subject: Guidance regarding WikiLeaks

To: All Commerce Employees and Contractors

Recent reports indicate that a number of government documents have been posted on the WikiLeaks website. These documents may or may not contain information that is considered National Security Information (classified information) and as such, the information is NOT authorized for downloading, viewing, printing, processing, copying, or transmitting via non-classified Government-issued computers, laptops, blackberries, or other communication devices and is not an authorized use of DOC IT equipment. Doing so would introduce potentially classified information onto our unclassified networks and represent a potential security incident.

There has been a rumor that the information is no longer classified since it resides in the public domain. This is NOT true. Executive Order 13526, Section 1.1(4)(2) states "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information." The information was neither properly nor improperly "declassified" by the appropriate authority and requires continued classification or reclassification.

Please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents because these documents may contain classified information. Accessing the WikiLeaks documents will lead to sanitization of your PC to remove any potentially

classified information from the system and result in possible data loss.

If you have questions regarding this broadcast or have accessed the WikiLeaks documents, please contact the DOC Computer Incident Response Team at email [doc-cirt@doc.gov](mailto:doc-cirt@doc.gov) or call (202) 482-4000.

---

This message was authorized by the Office of Secretary OSY/OCIO.

Please do not reply to this message. The broadcast email account is not monitored for incoming mail.

---



**Subject:** IMPORTANT - RE: Guidance regarding WikiLeaks

**From:** "Glenn, K. Robert" <robert.glenn@nist.gov>

**Date:** Mon, 6 Dec 2010 11:47:38 -0500

**To:** "[REDACTED]@nist.gov"

**CC:** "Glenn, K. Robert" <robert.glenn@nist.gov>

Dear [REDACTED] (b)(6)

I am the NIST IT Security Officer and I have been asked to contact all NIST staff who may have had a computer that connected to WikiLeaks prior to the guidance issued by DoC. Please be assured, that due to the nature of this issue, while this deals with access to potential classified information and we are required by DoC to respond to this incident, no one at NIST who went to the site prior to the guidance issued by DoC is going to get into any trouble. In fact, several NIST staff computers connected to the site prior to the issuance of the DoC guidance.

DOC has confirmed that WikiLeaks was accessed from a computer registered to you, which may mean classified information was unknowingly accessed. Because access occurred prior to receiving guidance from DOC (see below), this is viewed as an unintentional incident. However, NIST is required to treat the computer as though there is classified data resident (i.e., classified information spillage) and, the computer must be appropriately sanitized to ensure that any classified information is removed.

**The NIST Office of Information Systems Management (formerly OCIO) incident response team (Robert Sorensen or John Beltz) will contact you to schedule sanitization of the computer.** Please do not access, read, forward, or otherwise move any WikiLeaks documents that may have been downloaded. Also, please do not attempt to remove any such documents on your own. Sanitization will include removal of the information in your browser cache/history, temporary files, backups that may contain WikiLeaks documentation, etc., and verification that the information was not forwarded via other methods such as email, instant messaging, etc. Every effort will be made to preserve all other user data on the computer (i.e. **this is a routine process and user data should not be affected**). Given the number of incidents within NIST, we ask for your patience in scheduling sanitization. Since classified information is involved, **the DOC Office of Security (OSY) will likely follow up and send you an inadvertent disclosure briefing which includes a reminder to not disclose any sensitive information you may have seen when going to the WikiLeaks site.**

As a reminder, please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents.

Please do not hesitate to contact me personally if you have any questions or concerns.

Regards,

Rob Glenn  
IT Security Officer, NIST

[rob.glenn@nist.gov](mailto:rob.glenn@nist.gov)

URGENT - RE: Guidance regarding WikiLeaks

301-975-3667

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

From: allstaff@nist.gov [mailto:allstaff@nist.gov] On Behalf Of NIST IT Assistance Center  
Sent: Wednesday, December 01, 2010 2:45 PM  
To: Multiple recipients of list  
Subject: RE: Guidance regarding WikiLeaks

Attention NIST Staff:

To clarify the guidance that the Department of Commerce issued earlier today we ask that you not use the Commerce contact information provided in that email. Instead, direct any questions or notifications of access to WikiLeaks documents to the NIST IT Assistance Center (iTAC).

iTAC  
IT Assistance Center  
itac@nist.gov

303-497-5375 (Boulder)  
301-975-5375 (Gaithersburg)

Hours of Operation:  
Boulder: 7:30am - 5:30pm (Mountain Time) Monday - Friday  
Gaithersburg: 7:30am - 5:30pm (Eastern Time) Monday - Friday

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

From: allstaff@nist.gov [mailto:allstaff@nist.gov] On Behalf Of Broadcast, DOC  
Sent: Wednesday, December 01, 2010 11:11 AM  
To: Multiple recipients of list  
Subject: Guidance regarding WikiLeaks

To: All Commerce Employees and Contractors

Recent reports indicate that a number of government documents have been posted on the WikiLeaks website. These documents may or may not contain information that is considered National Security Information (classified information) and as such, the information is NOT authorized for downloading, viewing, printing, processing, copying, or transmitting via non-classified Government-issued computers, laptops, blackberries, or other communication devices and is not an authorized use of DOC IT equipment. Doing so would introduce potentially classified information onto our unclassified networks and represent a potential security incident.

There has been a rumor that the information is no longer classified since it resides in the public domain. This is NOT true. Executive Order 13526, Section 1.1(4)(2) states "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information." The information was neither properly nor improperly "declassified" by the appropriate authority and requires continued classification or reclassification.

Please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents because these documents may contain classified information. Accessing the WikiLeaks documents will lead to sanitization of your PC to remove any potentially classified information from the system and result in possible data loss.

IMPORTANT - RE: Guidance regarding WikiLeaks

If you have questions regarding this broadcast or have accessed the WikiLeaks documents, please contact the DOC Computer Incident Response Team at email [doc-cirt@doc.gov](mailto:doc-cirt@doc.gov) or call (202) 482-4000.

---

This message was authorized by the Office of Secretary OSY/OCIO.

Please do not reply to this message. The broadcast email account is not monitored for incoming mail.

---

**Subject:** RE: IMPORTANT - RE: Guidance regarding WikiLeaks

**From:** "Glenn, K. Robert" <robert.glenn@nist.gov>

**Date:** Mon, 6 Dec 2010 11:48:58 -0500 (b)(6)

**To:** [REDACTED] (b)(6)

**CC:** "Glenn, K. Robert" <robert.glenn@nist.gov>

Dear [REDACTED] (b)(6),

I am the NIST IT Security Officer and I have been asked to contact all NIST staff who may have had a computer that connected to WikiLeaks prior to the guidance issued by DoC. Please be assured, that due to the nature of this issue, while this deals with access to potential classified information and we are required by DoC to respond to this incident, no one at NIST who went to the site prior to the guidance issued by DoC is going to get into any trouble. In fact, several NIST staff computers connected to the site prior to the issuance of the DoC guidance.

DOC has confirmed that WikiLeaks was accessed from a computer registered to you, which may mean classified information was unknowingly accessed. Because access occurred prior to receiving guidance from DOC (see below), this is viewed as an unintentional incident. However, NIST is required to treat the computer as though there is classified data resident (i.e., classified information spillage) and, the computer must be appropriately sanitized to ensure that any classified information is removed.

**The NIST Office of Information Systems Management (formerly OCIO) incident response team (Robert Sorensen or John Beltz) will contact you to schedule sanitization of the computer.** Please do not access, read, forward, or otherwise move any WikiLeaks documents that may have been downloaded. Also, please do not attempt to remove any such documents on your own. Sanitization will include removal of the information in your browser cache/history, temporary files, backups that may contain WikiLeaks documentation, etc., and verification that the information was not forwarded via other methods such as email, instant messaging, etc. Every effort will be made to preserve all other user data on the computer (i.e. **this is a routine process and user data should not be affected**). Given the number of incidents within NIST, we ask for your patience in scheduling sanitization. Since classified information is involved, **the DOC Office of Security (OSY) will likely follow up and send you an inadvertent disclosure briefing which includes a reminder to not disclose any sensitive information you may have seen when going to the WikiLeaks site.**

As a reminder, please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents.

Please do not hesitate to contact me personally if you have any questions or concerns.

Regards,

Rob Glenn  
IT Security Officer, NIST

rob.glenn@nist.gov

301-975-3667

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

From: allstaff@nist.gov [mailto:allstaff@nist.gov] On Behalf Of NIST IT Assistance Center  
Sent: Wednesday, December 01, 2010 2:45 PM  
To: Multiple recipients of list  
Subject: RE: Guidance regarding WikiLeaks

Attention NIST Staff:

To clarify the guidance that the Department of Commerce issued earlier today we ask that you not use the Commerce contact information provided in that email. Instead, direct any questions or notifications of access to WikiLeaks documents to the NIST IT Assistance Center (ITAC).

ITAC  
IT Assistance Center  
itac@nist.gov

303-497-5375 (Boulder)  
301-975-5375 (Gaithersburg)

Hours of Operation:

Boulder: 7:30am - 5:30pm (Mountain Time) Monday - Friday  
Gaithersburg: 7:30am - 5:30pm (Eastern Time) Monday - Friday

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

From: allstaff@nist.gov [mailto:allstaff@nist.gov] On Behalf Of Broadcast, DOC  
Sent: Wednesday, December 01, 2010 11:11 AM  
To: Multiple recipients of list  
Subject: Guidance regarding WikiLeaks

To: All Commerce Employees and Contractors

Recent reports indicate that a number of government documents have been posted on the WikiLeaks website. These documents may or may not contain information that is considered National Security Information (classified information) and as such, the information is NOT authorized for downloading, viewing, printing, processing, copying, or transmitting via non-classified Government-issued computers, laptops, blackberries, or other communication devices and is not an authorized use of DOC IT equipment. Doing so would introduce potentially classified information onto our unclassified networks and represent a potential security incident.

There has been a rumor that the information is no longer classified since it resides in the public domain. This is NOT true. Executive Order 13526, Section 1.1(4)(2) states "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information." The information was neither properly nor improperly "declassified" by the appropriate authority and requires continued classification or reclassification.

Please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents because these documents may contain classified information. Accessing the WikiLeaks documents will lead to sanitization of your PC to remove any potentially classified information from the system and result in possible data loss.

E: IMPORTANT - RE: Guidance regarding WikiLeaks

If you have questions regarding this broadcast or have accessed the WikiLeaks documents, please contact the DOC Computer Incident Response Team at email [doc-cirt@doc.gov](mailto:doc-cirt@doc.gov) or call (202) 482-4000.

---

This message was authorized by the Office of Secretary OSY/OCIO.

Please do not reply to this message. The broadcast email account is not monitored for incoming mail.

---

**Subject:** IMPORTANT - RE: Guidance regarding WikiLeaks

**From:** "Glenn, K. Robert" <robert.glenn@nist.gov>

**Date:** Mon, 6 Dec 2010 11:50:45 -0500

**To:** [REDACTED] (b)(6)

**CC:** "Glenn, K. Robert" <robert.glenn@nist.gov>

Dear [REDACTED] (b)(6)

I am the NIST IT Security Officer and I have been asked to contact all NIST staff who may have had a computer that connected to WikiLeaks prior to the guidance issued by DoC. Please be assured, that due to the nature of this issue, while this deals with access to potential classified information and we are required by DoC to respond to this incident, no one at NIST who went to the site prior to the guidance issued by DoC is going to get into any trouble. In fact, several NIST staff computers connected to the site prior to the issuance of the DoC guidance.

DOC has confirmed that WikiLeaks was accessed from a computer registered to you, which may mean classified information was unknowingly accessed. Because access occurred prior to receiving guidance from DOC (see below), this is viewed as an unintentional incident. However, NIST is required to treat the computer as though there is classified data resident (i.e., classified information spillage) and, the computer must be appropriately sanitized to ensure that any classified information is removed.

**The NIST Office of Information Systems Management (formerly OCIO) incident response team (Robert Sorensen or John Beltz) will contact you to schedule sanitization of the computer.** Please do not access, read, forward, or otherwise move any WikiLeaks documents that may have been downloaded. Also, please do not attempt to remove any such documents on your own. Sanitization will include removal of the information in your browser cache/history, temporary files, backups that may contain WikiLeaks documentation, etc., and verification that the information was not forwarded via other methods such as email, instant messaging, etc. Every effort will be made to preserve all other user data on the computer (i.e. **this is a routine process and user data should not be affected**). Given the number of incidents within NIST, we ask for your patience in scheduling sanitization. Since classified information is involved, **the DOC Office of Security (OSY) will likely follow up and send you an inadvertent disclosure briefing which includes a reminder to not disclose any sensitive information you may have seen when going to the WikiLeaks site.**

As a reminder, please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents.

Please do not hesitate to contact me personally if you have any questions or concerns.

Regards,

Rob Glenn  
IT Security Officer, NIST

rob.glenn@nist.gov

301-975-3667

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

From: allstaff@nist.gov [mailto:allstaff@nist.gov] On Behalf Of NIST IT Assistance Center  
Sent: Wednesday, December 01, 2010 2:45 PM  
To: Multiple recipients of list  
Subject: RE: Guidance regarding WikiLeaks

Attention NIST Staff:

To clarify the guidance that the Department of Commerce issued earlier today we ask that you not use the Commerce contact information provided in that email. Instead, direct any questions or notifications of access to WikiLeaks documents to the NIST IT Assistance Center (ITAC).

ITAC  
IT Assistance Center  
itac@nist.gov

303-497-5375 (Boulder)  
301-975-5375 (Gaithersburg)

Hours of Operation:

Boulder: 7:30am - 5:30pm (Mountain Time) Monday - Friday  
Gaithersburg: 7:30am - 5:30pm (Eastern Time) Monday - Friday

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

From: allstaff@nist.gov [mailto:allstaff@nist.gov] On Behalf Of Broadcast, DOC  
Sent: Wednesday, December 01, 2010 11:11 AM  
To: Multiple recipients of list  
Subject: Guidance regarding WikiLeaks

To: All Commerce Employees and Contractors

Recent reports indicate that a number of government documents have been posted on the WikiLeaks website. These documents may or may not contain information that is considered National Security Information (classified information) and as such, the information is NOT authorized for downloading, viewing, printing, processing, copying, or transmitting via non-classified Government-issued computers, laptops, blackberries, or other communication devices and is not an authorized use of DOC IT equipment. Doing so would introduce potentially classified information onto our unclassified networks and represent a potential security incident.

There has been a rumor that the information is no longer classified since it resides in the public domain. This is NOT true. Executive Order 13526, Section 1.1(4)(2) states "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information." The information was neither properly nor improperly "declassified" by the appropriate authority and requires continued classification or reclassification.

Please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents because these documents may contain classified information. Accessing the WikiLeaks documents will lead to sanitization of your PC to remove any potentially classified information from the system and result in possible data loss.



IMPORTANT - RE: Guidance regarding WikiLeaks

If you have questions regarding this broadcast or have accessed the WikiLeaks documents, please contact the DOC Computer Incident Response Team at email [doc-cirt@doc.gov](mailto:doc-cirt@doc.gov) or call (202) 482-4000.

---

This message was authorized by the Office of Secretary OSY/OCIO.

Please do not reply to this message. The broadcast email account is not monitored for incoming mail.

---

**Subject:** IMPORTANT - RE: Guidance regarding WikiLeaks

**From:** "Glenn, K. Robert" <robert.glenn@nist.gov>

**Date:** Mon, 6 Dec 2010 11:52:09 -0500

**To:** [REDACTED] (b)(6)

**CC:** "Glenn, K. Robert" <robert.glenn@nist.gov>

Dear [REDACTED] (b)(6)

I am the NIST IT Security Officer and I have been asked to contact all NIST staff who may have had a computer that connected to WikiLeaks prior to the guidance issued by DoC. Please be assured, that due to the nature of this issue, while this deals with access to potential classified information and we are required by DoC to respond to this incident, no one at NIST who went to the site prior to the guidance issued by DoC is going to get into any trouble. In fact, several NIST staff computers connected to the site prior to the issuance of the DoC guidance.

DOC has confirmed that WikiLeaks was accessed from a computer registered to you, which may mean classified information was unknowingly accessed. Because access occurred prior to receiving guidance from DOC (see below), this is viewed as an unintentional incident. However, NIST is required to treat the computer as though there is classified data resident (i.e., classified information spillage) and, the computer must be appropriately sanitized to ensure that any classified information is removed.

**The NIST Office of Information Systems Management (formerly OCIO) incident response team (John Antonishek, Jeff McIntyre, David Kustaborder, Al Hurst, or Matt Loebach) will contact you to schedule sanitization of the computer.** Please do not access, read, forward, or otherwise move any WikiLeaks documents that may have been downloaded. Also, please do not attempt to remove any such documents on your own. Sanitization will include removal of the information in your browser cache/history, temporary files, backups that may contain WikiLeaks documentation, etc., and verification that the information was not forwarded via other methods such as email, instant messaging, etc. Every effort will be made to preserve all other user data on the computer (i.e. **this is a routine process and user data should not be affected**). Given the number of incidents within NIST, we ask for your patience in scheduling sanitization. Since classified information is involved, **the DOC Office of Security (OSY) will likely follow up and send you an inadvertent disclosure briefing which includes a reminder to not disclose any sensitive information you may have seen when going to the WikiLeaks site.**

As a reminder, please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents.

Please do not hesitate to contact me personally if you have any questions or concerns.

Regards,

Rob Glenn  
IT Security Officer, NIST

rob.glenn@nist.gov  
301-975-3667

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

From: allstaff@nist.gov [mailto:allstaff@nist.gov] On Behalf Of NIST IT Assistance Center  
Sent: Wednesday, December 01, 2010 2:45 PM  
To: Multiple recipients of list  
Subject: RE: Guidance regarding WikiLeaks

Attention NIST Staff:

~~To clarify the guidance that the Department of Commerce issued earlier today we ask that you not use the Commerce contact information provided in that email. Instead, direct any questions or notifications of access to WikiLeaks documents to the NIST IT Assistance Center (ITAC).~~

ITAC  
IT Assistance Center  
itac@nist.gov

303-497-5375 (Boulder)  
301-975-5375 (Gaithersburg)

Hours of Operation:

Boulder: 7:30am - 5:30pm (Mountain Time) Monday - Friday  
Gaithersburg: 7:30am - 5:30pm (Eastern Time) Monday - Friday

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

From: allstaff@nist.gov [mailto:allstaff@nist.gov] On Behalf Of Broadcast, DOC  
Sent: Wednesday, December 01, 2010 11:11 AM  
To: Multiple recipients of list  
Subject: Guidance regarding WikiLeaks

To: All Commerce Employees and Contractors

Recent reports indicate that a number of government documents have been posted on the WikiLeaks website. These documents may or may not contain information that is considered National Security Information (classified information) and as such, the information is NOT authorized for downloading, viewing, printing, processing, copying, or transmitting via non-classified Government-issued computers, laptops, blackberries, or other communication devices and is not an authorized use of DOC IT equipment. Doing so would introduce potentially classified information onto our unclassified networks and represent a potential security incident.

There has been a rumor that the information is no longer classified since it resides in the public domain. This is NOT true. Executive Order 13526, Section 1.1(4)(2) states "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information." The information was neither properly nor improperly "declassified" by the appropriate authority and requires continued classification or reclassification.

Please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents because these documents may contain classified information. Accessing the WikiLeaks documents will lead to sanitization of your PC to remove any potentially

IMPORTANT - RE: Guidance regarding WikiLeaks

classified information from the system and result in possible data loss.

If you have questions regarding this broadcast or have accessed the WikiLeaks documents, please contact the DOC Computer Incident Response Team at email [doc-cirt@doc.gov](mailto:doc-cirt@doc.gov) or call (202) 482-4000.

---

This message was authorized by the Office of Secretary OSY/OCIO.

Please do not reply to this message. The broadcast email account is not monitored for incoming mail.

---

refer to  
Dept

From: Hynek, Diana [dHynek@doc.gov]  
 Sent: Friday, December 17, 2010 4:09 PM  
 To: Adeseun, Janine; Annan, Joyce; Bender, Avi; Bergersen, Benjamin; Bingham, Joselyn; Borzino, Bruce; Brabson, Sarah; McGrath, Brian E; Brockett, Del; Brooks, Donna; Callahan, Brian; Census Listserv; Clark, Roger; Clark, Tammy L; Clift, Douglas; RCONRAD@BIS.DOC.GOV; Crawley, Allen; Ahrnsbrak, Darice; Daley, Maureen; Donnell, Duane; Donnell, Eddie; Douglas, Frances; Frazier, Mary B; Glenn, Robert K; Gordon, Judith; Herbst, Ellen; Holland, Robbin; Janssen, Jerry; Jones, Gwendolyn; Jones, Kathy; Kelsner, Renee; Kessler-Smith, Debi; Klimavicz, Joseph; ksinner@ntis.fedworld.gov; Leidich, John; Levitas, Howard; Macklin, Renee; Martin, John; McCoy, Wendy; McKenney, Crystal; McMahon, Keith; Meerholz, Thomas; Miller, Darryl; Morgan, Dennis; Murphy, Terryne F; Owens II, John; Praner, Karen; Raville, Michele; Redmond, Rosalie; Reed, Lawrence; Reed, Michelle; Rod.Smart@mail.doc.gov; Rodgers, Karen; Rodriguez, Gladys; Rosen, Bruce K; Ruggieri, Rand; Ruland, Timothy; Schiller, Susannah B; Secor, Jeffrey A; Dean, Shirley; Shukran, Lisa; Slaughter, Ronald; Soto, Linel; Stowe, Kathy; Swisher, Robert; Szykman, Simon; Taylor, Tom; Thompson, Gwendolyn; Turk, Rod; Villemarette, John; Watkins, Dianne; Weldon, Mary; Whitley, Yolanda; Williams, Scott; Zinser, Todd  
 Cc: Blackwood, Wayne; Broadwater, Patricia; Byrd, Teresa; Davitt, Robin; Dickerson-Womack, Bernadette; Dornell, Izella; Fitzgerald, Erin; Frink, Jackie; Grant, Charlene; Harper, Jerry; Harper, Pam; Hurr, Tim; Kauinui, Kelli; Ky, Wes; Maraya, Mike; Neal, Earl; Pennington, Thomas; Rooney, Dan; Simon, Stuart; Sutch, Dennis; Ware, Terri; Westerback, Lisa  
 Subject: DATA CALL: Inventory of Classified Systems and Devices DUE January 7, 2011  
 Attachments: Inventory Data Call.xlsx

As a result of the recent WikiLeaks incident, OMB issued Memorandum M-11-06 directing each department or agency that handles classified information to establish a security assessment team to review the agency's implementation of procedures for safeguarding classified information against improper disclosures. Specifically, such review should include (without limitation) evaluation of the agency's configuration of classified government systems to ensure users do not have broader access than is necessary to do their jobs effectively, as well as implementation of usage of, and removable media capabilities from, classified government computer networks. This security review will be conducted jointly by counter-intelligence, security, and information assurance experts.

In order to conduct a full assessment of all departmental classified information systems, an updated system and device inventory is required. Please note that the device listing is considered classified when data is filled into the sheet. Contact Roger Clark for information regarding delivery of the classified portion of the data call.

Type of Call	Data
Name	Inventory of Classified Systems and Devices
Due Date	January 7, 2011
Originator	OMB
OCIO Office	OCIO/OITSCI
Purpose	Establish an inventory of all DOC classified information systems and associated devices.
Use	Respond to OMB, ISSO, and ODNI
Category	OMB Memorandum
Voluntary/Mandatory (Negative Response Required)	Mandatory
Recurring/Non-Recurring	Non-Recurring
POC	Roger Clark, RClark@doc.gov, 202-482-0121

Diana Hynek

refer to  
Dept | Office of the CIO  
[dhrynek@doc.gov](mailto:dhrynek@doc.gov)  
202-482-0266

[REDACTED]

---

Subject: DATA CALL: Inventory of Classified Systems and Devices DUE January 7, 2011  
Location: 7725

Start: Wed 1/5/2011 12:00 PM  
End: Wed 1/5/2011 12:30 PM  
Show Time As: Tentative

Recurrence: (none)

Meeting Status: Not yet responded

Organizer: [REDACTED]  
Required Attendees: [REDACTED] [REDACTED]

refer to -----  
Dept

From: Hynek, Diana [dHynek@doc.gov]  
Sent: Friday, December 17, 2010 4:09 PM  
To: Adeseun, Janine; Annan, Joyce; Bender, Avi; Bergersen, Benjamin; Bingham, Joselyn; Borzino, Bruce; Brabson, Sarah; McGrath, Brian E; Brockett, Del; Brooks, Donna; Callahan, Brian; Census Listserv; Clark, Roger; Clark, Tammy L; Clift, Douglas; [RCONRAD@BIS.DOC.GOV](mailto:RCONRAD@BIS.DOC.GOV); Crawley, Allen; Ahrnsbrak, Darice; Daley, Maureen; Donnell, Duane; Donnell, Eddie; Douglas, Frances; Frazier, Mary B; Glenn, Robert K; Gordon, Judith; Herbst, Ellen; Holland, Robbin; Janssen, Jerry; Jones, Gwendolyn; Jones, Kathy; Kelser, Renee; Kessler-Smith, Debi; Klimavicz, Joseph; [ksinner@ntis.fedworld.gov](mailto:ksinner@ntis.fedworld.gov); Leidich, John; Levitas, Howard; Macklin, Renee; Martin, John; McCoy, Wendy; McKenney, Crystal; McMahon, Keith; Meerholz, Thomas; Miller, Darryl; Morgan, Dennis; Murphy, Terryne F; Owens II, John; Praner, Karen; Raville, Michele; Redmond, Rosalie; Reed, Lawrence; Reed, Michelle; [Rod.Smart@mail.doc.gov](mailto:Rod.Smart@mail.doc.gov); Rodgers, Karen; Rodriguez, Gladys; Rosen, Bruce K; Ruggieri, Rand; Ruland, Timothy; Schiller, Susannah B; Secor, Jeffrey A; Dean, Shirley; Shukran, Lisa; Slaughter, Ronald; Soto, Linel; Stowe, Kathy; Swisher, Robert; Szykman, Simon; Taylor, Tom; Thompson, Gwendolyn; Turk, Rod; Villemarette, John; Watkins, Dianne; Weldon, Mary; Whitley, Yolanda; Williams, Scott; Zinser, Todd

Cc: Blackwood, Wayne; Broadwater, Patricia; Byrd, Teresa; Davitt, Robin; Dickerson-Womack, Bernadette; Dornell, Izella; Fitzgerald, Erin; Frink, Jackie; Grant, Charlene; Harper, Jerry; Harper, Pam; Hurr, Tim; Kauinui, Kelli; Ky, Wes; Maraya, Mike; Neal, Earl; Pennington, Thomas; Rooney, Dan; Simon, Stuart; Sutch, Dennis; Ware, Terri; Westerback, Lisa

Subject: DATA CALL: Inventory of Classified Systems and Devices DUE January 7, 2011  
Attachments: Inventory Data Call.xlsx

As a result of the recent WikiLeaks incident, OMB issued Memorandum M-11-06 directing each department or agency that handles classified information to establish a security assessment team to review the agency's implementation of procedures for safeguarding classified information against improper disclosures. Specifically, such review should include (without limitation) evaluation of the agency's configuration of classified government systems to ensure users do not have broader access than is necessary to do their jobs effectively, as well as implementation of usage of, and removable media capabilities from, classified government computer networks. This security review will be conducted jointly by counter-intelligence, security, and information assurance experts.

In order to conduct a full assessment of all departmental classified information systems, an updated system and device inventory is required. Please note that the device listing is considered classified

refer to  
Dept

when data is filled into the sheet. Contact Roger Clark for information regarding delivery of the classified portion of the data call.

Type of Call

Data

Name

*Inventory of Classified Systems and Devices*

Due Date

January 7, 2011

Originator

OMB

OCIO Office

OCIO/OTSCI

Purpose

Establish an inventory of all DOC classified information systems and associated devices.

Use

Respond to OMB, ISSO, and ODNI

Category

OMB Memorandum

Voluntary/Mandatory (Negative Response Required)

Mandatory

Recurring/Non-Recurring

Non-Recurring

POC

Roger Clark, [RClark@doc.gov](mailto:RClark@doc.gov), 202-482-0121

Diana Hynek



refer to  
Dept

Office of the CIO

[dhynnek@doc.gov](mailto:dhynnek@doc.gov)

202-482-0266

[REDACTED]  
From: [REDACTED]  
Sent: Tuesday, December 21, 2010 11:25 AM  
To: [REDACTED]  
Subject: FW: DATA CALL: Inventory of Classified Systems and Devices DUE January 7, 2011  
Attachments: Inventory Data Call.xlsx

H [REDACTED] and [REDACTED] this data call is due in two weeks.

[REDACTED]  
General Dynamics Information Technology  
Office of the Chief Information Officer  
Office of the Inspector General  
U.S. Department of Commerce  
[REDACTED]@oig.doc.gov  
(202) 482-[REDACTED]

refer to From: Hynek, Diana [mailto:dHynek@doc.gov]

Dept Sent: Friday, December 17, 2010 4:09 PM

To: Adeseun, Janine; Annan, Joyce; Bender, Avi; Bergersen, Benjamin; Bingham, Joselyn; Borzino, Bruce; Brabson, Sarah; McGrath, Brian E; Brockett, Del; Brooks, Donna; Callahan, Brian; Census Listserv; Clark, Roger; Clark, Tammy L; Clift, Douglas; RCONRAD@BIS.DOC.GOV; Crawley, Allen; Ahrnsbrak, Darice; Daley, Maureen; Donnell, Duane; Donnell, Eddie; Douglas, Frances; Frazier, Mary B; Glenn, Robert K; Gordon, Judith; Herbst, Ellen; Holland, Robbin; Janssen, Jerry; Jones, Gwendolyn; Jones, Kathy; Kelser, Renee; Kessler-Smith, Debi; Klimavicz, Joseph; ksinner@ntis.fedworld.gov; Leidich, John; Levitas, Howard; Macklin, Renee; Martin, John; McCoy, Wendy; McKenney, Crystal; McMahon, Keith; Meerholz, Thomas; Miller, Darryl; Morgan, Dennis; Murphy, Terryne F; Owens II, John; Praner, Karen; Raville, Michele; Redmond, Rosalie; Reed, Lawrence; Reed, Michelle; Rod.Smart@mail.doc.gov; Rodgers, Karen; Rodriguez, Gladys; Rosen, Bruce K; Ruggieri, Rand; Ruland, Timothy; Schiller, Susannah B; Secor, Jeffrey A; Dean, Shirley; Shukran, Lisa; Slaughter, Ronald; Soto, Linel; Stowe, Kathy; Swisher, Robert; Szykman, Simon; Taylor, Tom; Thompson, Gwendolyn; Turk, Rod; Villemarette, John; Watkins, Dianne; Weldon, Mary; Whitley, Yolanda; Williams, Scott; Zinser, Todd  
Cc: Blackwood, Wayne; Broadwater, Patricia; Byrd, Teresa; Davitt, Robin; Dickerson-Womack, Bernadette; Dornell, Izella; Fitzgerald, Erin; Frink, Jackie; Grant, Charlene; Harper, Jerry; Harper, Pam; Hurr, Tim; Kauinui, Kelli; Ky, Wes; Maraya, Mike; Neal, Earl; Pennington, Thomas; Rooney, Dan; Simon, Stuart; Sutch, Dennis; Ware, Terri; Westerback, Lisa  
Subject: DATA CALL: Inventory of Classified Systems and Devices DUE January 7, 2011

As a result of the recent WikiLeaks incident, OMB issued Memorandum M-11-06 directing each department or agency that handles classified information to establish a security assessment team to review the agency's implementation of procedures for safeguarding classified information against improper disclosures. Specifically, such review should include (without limitation) evaluation of the agency's configuration of classified government systems to ensure users do not have broader access than is necessary to do their jobs effectively, as well as implementation of usage of, and removable media capabilities from, classified government computer networks. This security review will be conducted jointly by counter-intelligence, security, and information assurance experts.

In order to conduct a full assessment of all departmental classified information systems, an updated system and device inventory is required. Please note that the device listing is considered classified when data is filled into the sheet. Contact Roger Clark for information regarding delivery of the classified portion of the data call.

refer to  
Dept

Type of Call	Data
Name	Inventory of Classified Systems and Devices
Due Date	January 7, 2011
Originator	OMB
OCIO Office	OCIO/OITSCI
Purpose	Establish an inventory of all DOC classified information systems and associated devices.
Use	Respond to OMB, ISSO, and ODNI
Category	OMB Memorandum
Voluntary/Mandatory (Negative Response Required)	Mandatory
Recurring/Non-Recurring	Non-Recurring
POC	Roger Clark, <a href="mailto:RClark@doc.gov">RClark@doc.gov</a> , 202-482-0121

Diana Hynek  
Office of the CIO  
[dhynek@doc.gov](mailto:dhynek@doc.gov)  
202-482-0266

[REDACTED]

---

From: [REDACTED]  
Sent: Tuesday, December 21, 2010 2:37 PM  
To: [REDACTED]  
Cc: [REDACTED]  
Subject: RE: DATA CALL: Inventory of Classified Systems and Devices DUE January 7, 2011  
Importance: High

[REDACTED] and [REDACTED]

OIG does not have any classified systems or devices. Please submit our response as such.

[REDACTED]

Office of the Chief Information Officer  
Office of Inspector General  
U.S. Department of Commerce  
(202) 482-[REDACTED] office  
(202) 680-[REDACTED] cell  
(202) 501-[REDACTED] or (202) 482-[REDACTED] fax  
[REDACTED]@oig.doc.gov

From: [REDACTED]  
Sent: Tuesday, December 21, 2010 11:25 AM  
To: [REDACTED]  
Subject: FW: DATA CALL: Inventory of Classified Systems and Devices DUE January 7, 2011

Hi [REDACTED] and [REDACTED], this data call is due in two weeks.

[REDACTED]

General Dynamics Information Technology  
Office of the Chief Information Officer  
Office of the Inspector General  
U.S. Department of Commerce  
[REDACTED]@oig.doc.gov  
(202) 482-[REDACTED]

refer to  
Dept

From: Hynek, Diana [mailto:dHynek@doc.gov]  
Sent: Friday, December 17, 2010 4:09 PM  
To: Adeseun, Janine; Annan, Joyce; Bender, Avi; Bergersen, Benjamin; Bingham, Joselyn; Borzino, Bruce; Brabson, Sarah; McGrath, Brian E; Brockett, Del; Brooks, Donna; Callahan, Brian; Census Listserv; Clark, Roger; Clark, Tammy L; Clift, Douglas; RCONRAD@BIS.DOC.GOV; Crawley, Allen; Ahrensbrak, Darice; Daley, Maureen; Donnell, Duane; Donnell,

all redactions (b)(6)

[REDACTED]  
From: [REDACTED]  
Sent: Tuesday, December 21, 2010 3:07 PM  
To: [REDACTED]  
Subject: RE: DATA CALL: Inventory of Classified Systems and Devices DUE January 7, 2011

I will take care of the response, thank you [REDACTED]

[REDACTED]  
General Dynamics Information Technology  
Office of the Chief Information Officer  
Office of the Inspector General  
U.S. Department of Commerce  
[REDACTED]@oig.doc.gov  
(202) 482-[REDACTED]

From: [REDACTED]  
Sent: Tuesday, December 21, 2010 2:37 PM  
To: [REDACTED]; [REDACTED]  
Cc: [REDACTED]  
Subject: RE: DATA CALL: Inventory of Classified Systems and Devices DUE January 7, 2011  
Importance: High

[REDACTED] and [REDACTED],

OIG does not have any classified systems or devices. Please submit our response as such.

[REDACTED]  
Office of the Chief Information Officer  
Office of Inspector General  
U.S. Department of Commerce  
(202) 482-[REDACTED] office  
(202) 680-[REDACTED] cell  
(202) 501-[REDACTED] or (202) 482-[REDACTED] fax  
[REDACTED]@oig.doc.gov

From: [REDACTED]  
Sent: Tuesday, December 21, 2010 11:25 AM  
To: [REDACTED]  
Subject: FW: DATA CALL: Inventory of Classified Systems and Devices DUE January 7, 2011

Hi [REDACTED] and [REDACTED], this data call is due in two weeks.

[REDACTED]  
 General Dynamics Information Technology  
 Office of the Chief Information Officer  
 Office of the Inspector General  
 U.S. Department of Commerce  
 [REDACTED]@oig.doc.gov  
 (202) 482-[REDACTED]

refer to  
 Dept

**From:** Hynek, Diana [mailto:dHynek@doc.gov]  
**Sent:** Friday, December 17, 2010 4:09 PM  
**To:** Adeseun, Janine; Annan, Joyce; Bender, Avi; Bergersen, Benjamin; Bingham, Joselyn; Borzino, Bruce; Brabson, Sarah; McGrath, Brian E; Brockett, Del; Brooks, Donna; Callahan, Brian; Census Listserv; Clark, Roger; Clark, Tammy L; Clift, Douglas; RCONRAD@BIS.DOC.GOV; Crawley, Allen; Ahrnsbrak, Darice; Daley, Maureen; Donnell, Duane; Donnell, Eddie; Douglas, Frances; Frazier, Mary B; Glenn, Robert K; Gordon, Judith; Herbst, Ellen; Holland, Robbin; Janssen, Jerry; Jones, Gwendolyn; Jones, Kathy; Kelser, Renee; Kessler-Smith, Debi; Klimavicz, Joseph; ksinner@ntis.fedworld.gov; Leidich, John; Levitas, Howard; Macklin, Renee; Martin, John; McCoy, Wendy; Mckenney, Crystal; McMahon, Keith; Meerholz, Thomas; Miller, Darryl; Morgan, Dennis; Murphy, Terryne F; Owens II, John; Praner, Karen; Raville, Michele; Redmond, Rosalie; Reed, Lawrence; Reed, Michelle; Rod.Smart@mail.doc.gov; Rodgers, Karen; Rodriguez, Gladys; Rosen, Bruce K; Ruggieri, Rand; Ruland, Timothy; Schiller, Susannah B; Secor, Jeffrey A; Dean, Shirley; Shukran, Lisa; Slaughter, Ronald; Soto, Linel; Stowe, Kathy; Swisher, Robert; Szykman, Simon; Taylor, Tom; Thompson, Gwendolyn; Turk, Rod; Villemairette, John; Watkins, Dianne; Weldon, Mary; Whitley, Yolanda; Williams, Scott; Zinser, Todd  
**Cc:** Blackwood, Wayne; Broadwater, Patricia; Byrd, Teresa; Davitt, Robin; Dickerson-Womack, Bernadette; Dornell, Izella; Fitzgerald, Erin; Frink, Jackie; Grant, Charlene; Harper, Jerry; Harper, Pam; Hurr, Tim; Kauinui, Kelli; Ky, Wes; Maraya, Mike; Neal, Earl; Pennington, Thomas; Rooney, Dan; Simon, Stuart; Sutth, Dennis; Ware, Terri; Westerback, Lisa  
**Subject:** DATA CALL: Inventory of Classified Systems and Devices DUE January 7, 2011

As a result of the recent WikiLeaks incident, OMB issued Memorandum M-11-06 directing each department or agency that handles classified information to establish a security assessment team to review the agency's implementation of procedures for safeguarding classified information against improper disclosures. Specifically, such review should include (without limitation) evaluation of the agency's configuration of classified government systems to ensure users do not have broader access than is necessary to do their jobs effectively, as well as implementation of usage of, and removable media capabilities from, classified government computer networks. This security review will be conducted jointly by counter-intelligence, security, and information assurance experts.

In order to conduct a full assessment of all departmental classified information systems, an updated system and device inventory is required. Please note that the device listing is considered classified when data is filled into the sheet. Contact Roger Clark for information regarding delivery of the classified portion of the data call.

Type of Call	Data
Name	Inventory of Classified Systems and Devices
Due Date	January 7, 2011
Originator	OMB
OCIO Office	OCIO/OITSCI
Purpose	Establish an inventory of all DOC classified information systems and associated devices.
Use	Respond to OMB, ISSO, and ODNI

refer to  
Dept

Category	OMB Memorandum
Voluntary/Mandatory (Negative Response Required)	Mandatory
Recurring/Non-Recurring	Non-Recurring
POC	Roger Clark, <a href="mailto:RClark@doc.gov">RClark@doc.gov</a> , 202-482-0121

Diana Hynek  
Office of the CIO  
[dhynek@doc.gov](mailto:dhynek@doc.gov)  
202-482-0266

[REDACTED]

---

From: [REDACTED]  
Sent: Tuesday, December 21, 2010 3:07 PM  
To: Thompson, Gwendolyn; Slaughter, Ronald  
Subject: RE: DATA CALL: Inventory of Classified Systems and Devices DUE January 7, 2011

I will take care of the response, thank you [REDACTED]

[REDACTED]  
General Dynamics Information Technology  
Office of the Chief Information Officer  
Office of the Inspector General  
U.S. Department of Commerce  
[REDACTED]@oig.doc.gov  
(202) 482-1238

From: [REDACTED]  
Sent: Tuesday, December 21, 2010 2:37 PM  
To: [REDACTED]  
Cc: [REDACTED]  
Subject: RE: DATA CALL: Inventory of Classified Systems and Devices DUE January 7, 2011  
Importance: High

[REDACTED] and [REDACTED]

OIG does not have any classified systems or devices. Please submit our response as such.

[REDACTED]

Office of the Chief Information Officer  
Office of Inspector General  
U.S. Department of Commerce  
(202) 482-[REDACTED] office  
(202) 680-[REDACTED] cell  
(202) 501-[REDACTED] or (202) 482-[REDACTED] fax  
[REDACTED]@oig.doc.gov

From: [REDACTED]  
Sent: Tuesday, December 21, 2010 11:25 AM  
To: [REDACTED]  
Subject: FW: DATA CALL: Inventory of Classified Systems and Devices DUE January 7, 2011



Hi [REDACTED] and [REDACTED] this data call is due in two weeks.

[REDACTED]  
General Dynamics Information Technology  
Office of the Chief Information Officer  
Office of the Inspector General  
U.S. Department of Commerce  
[REDACTED]@oig.doc.gov  
(202) 482-[REDACTED]

refer  
to  
Dept

**From:** Hynek, Diana [mailto:dHynek@doc.gov]  
**Sent:** Friday, December 17, 2010 4:09 PM  
**To:** Adeseun, Janine; Annan, Joyce; Bender, Avi; Bergersen, Benjamin; Bingham, Joselyn; Borzino, Bruce; Brabson, Sarah; McGrath, Brian E; Brockett, Del; Brooks, Donna; Callahan, Brian; Census Listserv; Clark, Roger; Clark, Tammy L; Clift, Douglas; RCONRAD@BIS.DOC.GOV; Crawley, Allen; Ahrnsbrak, Darice; Daley, Maureen; Donnell, Duane; Donnell, Eddie; Douglas, Frances; Frazier, Mary B; Glenn, Robert K; Gordon, Judith; Herbst, Ellen; Holland, Robbin; Janssen, Jerry; Jones, Gwendolyn; Jones, Kathy; Kelsner, Renee; Kessler-Smith, Debi; Klimavicz, Joseph; ksinner@ntis.fedworld.gov; Leidich, John; Levitas, Howard; Macklin, Renee; Martin, John; McCoy, Wendy; McKenney, Crystal; McMahon, Keith; Meerholz, Thomas; Miller, Darryl; Morgan, Dennis; Murphy, Terryne F; Owens II, John; Prater, Karen; Raville, Michele; Redmond, Rosalie; Reed, Lawrence; Reed, Michelle; Rod.Smart@mail.doc.gov; Rodgers, Karen; Rodriguez, Gladys; Rosen, Bruce K; Ruggieri, Rand; Ruland, Timothy; Schiller, Susannah B; Secor, Jeffrey A; Dean, Shirley; Shukran, Lisa; Slaughter, Ronald; Soto, Linel; Stowe, Kathy; Swisher, Robert; Szykman, Simon; Taylor, Tom; Thompson, Gwendolyn; Turk, Rod; Villemarette, John; Watkins, Dianne; Weldon, Mary; Whitley, Yolanda; Williams, Scott; Zinser, Todd  
**Cc:** Blackwood, Wayne; Broadwater, Patricia; Byrd, Teresa; Davitt, Robin; Dickerson-Womack, Bernadette; Dornell, Izella; Fitzgerald, Erin; Frink, Jackie; Grant, Charlene; Harper, Jerry; Harper, Pam; Hurr, Tim; Kauinui, Kelli; Ky, Wes; Maraya, Mike; Neal, Earl; Pennington, Thomas; Rooney, Dan; Simon, Stuart; Sutch, Dennis; Ware, Terri; Westerback, Lisa  
**Subject:** DATA CALL: Inventory of Classified Systems and Devices DUE January 7, 2011

As a result of the recent Wikileaks incident, OMB issued Memorandum M-11-06 directing each department or agency that handles classified information to establish a security assessment team to review the agency's implementation of procedures for safeguarding classified information against improper disclosures. Specifically, such review should include (without limitation) evaluation of the agency's configuration of classified government systems to ensure users do not have broader access than is necessary to do their jobs effectively, as well as implementation of usage of, and removable media capabilities from, classified government computer networks. This security review will be conducted jointly by counter-intelligence, security, and information assurance experts.

In order to conduct a full assessment of all departmental classified information systems, an updated system and device inventory is required. Please note that the device listing is considered classified when data is filled into the sheet. Contact Roger Clark for information regarding delivery of the classified portion of the data call.

Type of Call	Data
Name	Inventory of Classified Systems and Devices
Due Date	January 7, 2011
Originator	OMB
OCIO Office	OCIO/OITSCI
Purpose	Establish an inventory of all DOC classified information systems and associated devices.
Use	Respond to OMB, ISSO, and ODNI

refer to  
Dept

Category	OMB Memorandum
Voluntary/Mandatory (Negative Response Required)	Mandatory
Recurring/Non-Recurring	Non-Recurring
POC	Roger Clark, <a href="mailto:RClark@doc.gov">RClark@doc.gov</a> , 202-482-0121

Diana Hynek  
Office of the CIO  
[dhynek@doc.gov](mailto:dhynek@doc.gov)  
202-482-0266

[REDACTED]  
From: [REDACTED]  
Sent: Tuesday, December 21, 2010 3:07 PM  
To: [REDACTED]  
Subject: RE: DATA CALL: Inventory of Classified Systems and Devices DUE January 7, 2011

Follow Up Flag: Follow up  
Flag Status: Completed

I will take care of the response, thank you [REDACTED]

[REDACTED]  
General Dynamics Information Technology  
Office of the Chief Information Officer  
Office of the Inspector General  
U.S. Department of Commerce  
[REDACTED]@oig.doc.gov  
(202) 482-[REDACTED]

From: [REDACTED]  
Sent: Tuesday, December 21, 2010 2:37 PM  
To: [REDACTED]  
Cc: [REDACTED]  
Subject: RE: DATA CALL: Inventory of Classified Systems and Devices DUE January 7, 2011  
Importance: High

[REDACTED] and [REDACTED]

OIG does not have any classified systems or devices. Please submit our response as such.

[REDACTED]  
Office of the Chief Information Officer  
Office of Inspector General  
U.S. Department of Commerce  
(202) 482-[REDACTED] office  
(202) 680-[REDACTED] cell  
(202) 501-[REDACTED] or (202) 482-[REDACTED] fax  
[REDACTED]@oig.doc.gov

From: [REDACTED]  
Sent: Tuesday, December 21, 2010 11:25 AM

all redactions (b)(6)

To: [REDACTED]  
Subject: FW: DATA CALL: Inventory of Classified Systems and Devices DUE January 7, 2011

Hi [REDACTED] and [REDACTED] this data call is due in two weeks.

[REDACTED]  
General Dynamics Information Technology  
Office of the Chief Information Officer  
Office of the Inspector General  
U.S. Department of Commerce  
[REDACTED]@oig.doc.gov  
(202) 482-[REDACTED]

refer to  
Dept

From: Hynek, Diana [mailto:dHynek@doc.gov]  
Sent: Friday, December 17, 2010 4:09 PM  
To: Adeseun, Janine; Annan, Joyce; Bender, Avi; Bergersen, Benjamin; Bingham, Joselyn; Borzino, Bruce; Brabson, Sarah; McGrath, Brian E; Brockett, Del; Brooks, Donna; Callahan, Brian; Census Listserv; Clark, Roger; Clark, Tammy L; Clift, Douglas; RCONRAD@BIS.DOC.GOV; Crawley, Allen; Ahrnsbrak, Darice; Daley, Maureen; Donnell, Duane; Donnell, Eddie; Douglas, Frances; Frazier, Mary B; Glenn, Robert K; Gordon, Judith; Herbst, Ellen; Holland, Robbin; Janssen, Jerry; Jones, Gwendolyn; Jones, Kathy; Kelser, Renee; Kessler-Smith, Debi; Klimavicz, Joseph; ksinner@ntis.fedworld.gov; Leidich, John; Levitas, Howard; Macklin, Renee; Martin, John; McCoy, Wendy; McKenney, Crystal; McMahon, Keith; Meerholz, Thomas; Miller, Darryl; Morgan, Dennis; Murphy, Terryne F; Owens II, John; Praner, Karen; Raville, Michele; Redmond, Rosalie; Reed, Lawrence; Reed, Michelle; Rod.Smart@mail.doc.gov; Rodgers, Karen; Rodriguez, Gladys; Rosen, Bruce K; Ruggieri, Rand; Ruland, Timothy; Schiller, Susannah B; Secor, Jeffrey A; Dean, Shirley; Shukran, Lisa; Slaughter, Ronald; Soto, Linel; Stowe, Kathy; Swisher, Robert; Szykman, Simon; Taylor, Tom; Thompson, Gwendolyn; Turk, Rod; Villemarette, John; Watkins, Dianne; Weldon, Mary; Whitley, Yolanda; Williams, Scott; Zinser, Todd  
Cc: Blackwood, Wayne; Broadwater, Patricia; Byrd, Teresa; Davitt, Robin; Dickerson-Womack, Bernadette; Dornell, Izella; Fitzgerald, Erin; Frink, Jackie; Grant, Charlene; Harper, Jerry; Harper, Pam; Hurr, Tim; Kauinui, Kelli; Ky, Wes; Maraya, Mike; Neal, Earl; Pennington, Thomas; Rooney, Dan; Simon, Stuart; Sutch, Dennis; Ware, Terri; Westerback, Lisa  
Subject: DATA CALL: Inventory of Classified Systems and Devices DUE January 7, 2011

As a result of the recent WikiLeaks incident, OMB issued Memorandum M-11-06 directing each department or agency that handles classified information to establish a security assessment team to review the agency's implementation of procedures for safeguarding classified information against improper disclosures. Specifically, such review should include (without limitation) evaluation of the agency's configuration of classified government systems to ensure users do not have broader access than is necessary to do their jobs effectively, as well as implementation of usage of, and removable media capabilities from, classified government computer networks. This security review will be conducted jointly by counter-intelligence, security, and information assurance experts.

In order to conduct a full assessment of all departmental classified information systems, an updated system and device inventory is required. Please note that the device listing is considered classified when data is filled into the sheet. Contact Roger Clark for information regarding delivery of the classified portion of the data call.

Type of Call	Data
Name	Inventory of Classified Systems and Devices
Due Date	January 7, 2011
Originator	OMB
OCIO Office	OCIO/OITSCI

refer to  
Dept

Purpose	Establish an inventory of all DOC classified information systems and associated devices.
Use	Respond to OMB, ISSO, and ODNI
Category	OMB Memorandum
Voluntary/Mandatory (Negative Response Required)	Mandatory
Recurring/Non-Recurring	Non-Recurring
POC	Roger Clark, <a href="mailto:RClark@doc.gov">RClark@doc.gov</a> , 202-482-0121

Diana Hynek  
Office of the CIO  
[dhynek@doc.gov](mailto:dhynek@doc.gov)  
202-482-0266

[REDACTED]  
[REDACTED]  
From: [REDACTED]  
Sent: Wednesday, December 22, 2010 4:27 PM  
To: [REDACTED]  
Cc: [REDACTED]  
Subject: FW: DATA CALL: Inventory of Classified Systems and Devices DUE January 7, 2011  
Attachments: 2010-090 Inventory of Classified Systems and Devices Memo.docx

Hi [REDACTED], attached is our initial draft in response to the data call. Please refer to link to see the topic subfolder.

S:\Data Call\2010 Data Call\2010-090 Inventory of Classified Systems and Devices

[REDACTED]  
General Dynamics Information Technology  
Office of the Chief Information Officer  
Office of the Inspector General  
U.S. Department of Commerce  
[REDACTED]@oig.doc.gov  
(202) 482-[REDACTED]

refer to  
Dept

From: Hynek, Diana [mailto:dHynek@doc.gov]  
Sent: Friday, December 17, 2010 4:09 PM  
To: Adeseun, Janine; Annan, Joyce; Bender, Avi; Bergersen, Benjamin; Bingham, Joselyn; Borzino, Bruce; Brabson, Sarah; McGrath, Brian E; Brockett, Del; Brooks, Donna; Callahan, Brian; Census Listserv; Clark, Roger; Clark, Tammy L; Clift, Douglas; RCONRAD@BIS.DOC.GOV; Crawley, Allen; Ahrnsbrak, Darice; Daley, Maureen; Donnell, Duane; Donnell, Eddie; Douglas, Frances; Frazier, Mary B; Glenn, Robert K; Gordon, Judith; Herbst, Ellen; Holland, Robbin; Janssen, Jerry; Jones, Gwendolyn; Jones, Kathy; Kelser, Renee; Kessler-Smith, Debi; Klimavicz, Joseph; ksinner@ntis.fedworld.gov; Leidich, John; Levitas, Howard; Macklin, Renee; Martin, John; McCoy, Wendy; McKenney, Crystal; McMahon, Keith; Meerholz, Thomas; Miller, Darryl; Morgan, Dennis; Murphy, Terryne F; Owens II, John; Praner, Karen; Raville, Michele; Redmond, Rosalie; Reed, Lawrence; Reed, Michelle; Rod.Smart@mail.doc.gov; Rodgers, Karen; Rodriguez, Gladys; Rosen, Bruce K; Ruggieri, Rand; Ruland, Timothy; Schiller, Susannah B; Secor, Jeffrey A; Dean, Shirley; Shukran, Lisa; Slaughter, Ronald; Soto, Linel; Stowe, Kathy; Swisher, Robert; Szykman, Simon; Taylor, Tom; Thompson, Gwendolyn; Turk, Rod; Villemarette, John; Watkins, Dianne; Weldon, Mary; Whitley, Yolanda; Williams, Scott; Zinser, Todd  
Cc: Blackwood, Wayne; Broadwater, Patricia; Byrd, Teresa; Davitt, Robin; Dickerson-Womack, Bernadette; Dornell, Izella; Fitzgerald, Erin; Frink, Jackie; Grant, Charlene; Harper, Jerry; Harper, Pam; Hurr, Tim; Kauinui, Kelli; Ky, Wes; Maraya, Mike; Neal, Earl; Pennington, Thomas; Rooney, Dan; Simon, Stuart; Sutch, Dennis; Ware, Terri; Westerback, Lisa  
Subject: DATA CALL: Inventory of Classified Systems and Devices DUE January 7, 2011

As a result of the recent WikiLeaks incident, OMB issued Memorandum M-11-06 directing each department or agency that handles classified information to establish a security assessment team to review the agency's implementation of procedures for safeguarding classified information against improper disclosures. Specifically, such review should include (without limitation) evaluation of the agency's configuration of classified government systems to ensure users do not have broader access than is necessary to do their jobs effectively, as well as implementation of usage of, and removable media capabilities from, classified government computer networks. This security review will be conducted jointly by counter-intelligence, security, and information assurance experts.

refer  
to  
Dept

In order to conduct a full assessment of all departmental classified information systems, an updated system and device inventory is required. Please note that the device listing is considered classified when data is filled into the sheet. Contact Roger Clark for information regarding delivery of the classified portion of the data call.

Type of Call	Data
Name	Inventory of Classified Systems and Devices
Due Date	January 7, 2011
Originator	OMB
OCIO Office	OCIO/OITSCI
Purpose	Establish an inventory of all DOC classified information systems and associated devices.
Use	Respond to OMB, ISSO, and ODNI
Category	OMB Memorandum
Voluntary/Mandatory (Negative Response Required)	Mandatory
Recurring/Non-Recurring	Non-Recurring
POC	Roger Clark, <a href="mailto:RClark@doc.gov">RClark@doc.gov</a> , 202-482-0121

Diana Hynek  
Office of the CIO  
[dhynek@doc.gov](mailto:dhynek@doc.gov)  
202-482-0266

[REDACTED]

---

**From:** [REDACTED]  
**Sent:** Wednesday, December 22, 2010 4:27 PM  
**To:** [REDACTED]  
**Cc:** [REDACTED]  
**Subject:** FW: DATA CALL: Inventory of Classified Systems and Devices DUE January 7, 2011  
**Attachments:** 2010-090 Inventory of Classified Systems and Devices Memo.docx

Hi [REDACTED] attached is our initial draft in response to the data call. Please refer to link to see the topic subfolder.

S:\Data Call\2010 Data Call\2010-090 Inventory of Classified Systems and Devices

[REDACTED]  
General Dynamics Information Technology  
Office of the Chief Information Officer  
Office of the Inspector General  
U.S. Department of Commerce  
[REDACTED]

(202) 482 [REDACTED]

refer to  
Dept

**From:** Hynek, Diana [mailto:dHynek@doc.gov]  
**Sent:** Friday, December 17, 2010 4:09 PM  
**To:** Adeseun, Janine; Annan, Joyce; Bender, Avi; Bergersen, Benjamin; Bingham, Joselyn; Borzino, Bruce; Brabson, Sarah; McGrath, Brian E; Brockett, Del; Brooks, Donna; Callahan, Brian; Census Listserv; Clark, Roger; Clark, Tammy L; Clift, Douglas; RCONRAD@BIS.DOC.GOV; Crawley, Allen; Ahrnsbrak, Darice; Daley, Maureen; Donnell, Duane; Donnell, Eddie; Douglas, Frances; Frazier, Mary B; Glenn, Robert K; Gordon, Judith; Herbst, Ellen; Holland, Robbin; Janssen, Jerry; Jones, Gwendolyn; Jones, Kathy; Kelser, Renee; Kessler-Smith, Debi; Klimavicz, Joseph; ksinner@ntis.fedworld.gov; Leidich, John; Levitas, Howard; Macklin, Renee; Martin, John; McCoy, Wendy; McKenney, Crystal; McMahon, Keith; Meerholz, Thomas; Miller, Darryl; Morgan, Dennis; Murphy, Terryne F; Owens II, John; Praner, Karen; Raville, Michele; Redmond, Rosalie; Reed, Lawrence; Reed, Michelle; Rod.Smart@mail.doc.gov; Rodgers, Karen; Rodriguez, Gladys; Rosen, Bruce K; Ruggieri, Rand; Ruland, Timothy; Schiller, Susannah B; Secor, Jeffrey A; Dean, Shirley; Shukran, Lisa; Slaughter, Ronald; Soto, Linel; Stowe, Kathy; Swisher, Robert; Szykman, Simon; Taylor, Tom; Thompson, Gwendolyn; Turk, Rod; Villemarette, John; Watkins, Dianne; Weldon, Mary; Whitley, Yolanda; Williams, Scott; Zinser, Todd  
**Cc:** Blackwood, Wayne; Broadwater, Patricia; Byrd, Teresa; Davitt, Robin; Dickerson-Womack, Bernadette; Dornell, Izella; Fitzgerald, Erin; Frink, Jackie; Grant, Charlene; Harper, Jerry; Harper, Pam; Hurr, Tim; Kauinui, Kelli; Ky, Wes; Maraya, Mike; Neal, Earl; Pennington, Thomas; Rooney, Dan; Simon, Stuart; Sutch, Dennis; Ware, Terri; Westerback, Lisa  
**Subject:** DATA CALL: Inventory of Classified Systems and Devices DUE January 7, 2011

As a result of the recent WikiLeaks incident, OMB issued Memorandum M-11-06 directing each department or agency that handles classified information to establish a security assessment team to review the agency's implementation of procedures for safeguarding classified information against improper disclosures. Specifically, such review should include (without limitation) evaluation of the agency's configuration of classified government systems to ensure users do not have broader access than is necessary to do their jobs effectively, as well as implementation of usage of, and removable media capabilities from, classified government computer networks. This security review will be conducted jointly by counter-intelligence, security, and information assurance experts.



refer to  
Dept

In order to conduct a full assessment of all departmental classified information systems, an updated system and device inventory is required. Please note that the device listing is considered classified when data is filled into the sheet. Contact Roger Clark for information regarding delivery of the classified portion of the data call.

Type of Call	Data
Name	Inventory of Classified Systems and Devices
Due Date	January 7, 2011
Originator	OMB
OCIO Office	OCIO/OITSCI
Purpose	Establish an inventory of all DOC classified information systems and associated devices.
Use	Respond to OMB, ISSO, and ODNI
Category	OMB Memorandum
Voluntary/Mandatory (Negative Response Required)	Mandatory
Recurring/Non-Recurring	Non-Recurring
POC	Roger Clark, <a href="mailto:RClark@doc.gov">RClark@doc.gov</a> , 202-482-0121

Diana Hynek  
Office of the CIO  
[dhynek@doc.gov](mailto:dhynek@doc.gov)  
202-482-0266

pw

(b)(2); d

(b)(6)

Requester cc

FORM CD-76 (REV. 1-07) (PRESCR. BY DAO-207-2)		U.S. DEPARTMENT OF COMMERCE		Receipt Number: OIG-2010-30-11-0001	
CLASSIFIED MATERIAL RECEIPT				Classification of Document: Secret	
Sent By: (Name, Unit, Address) [REDACTED], OIG [REDACTED] (b)(6)					Date of Document: 11/30/2010
Description of Document: Two hard drives (master and slave) from a [REDACTED] (b)(2) [REDACTED] (b)(2) [REDACTED] (b)(6)					
Date Transmitted	To: (Name and address)		Received by: (Signature)		Date Received
11/30/2010	OIG Computer Forensics & Technical Services HCHB, Room [REDACTED] (b)(6) and (b)(7)(C) [REDACTED] (b)(2)		[REDACTED]		12/1/10
	[REDACTED] (b)(2) [REDACTED] (b)(6)		[REDACTED] (b)(6) and (b)(7)(C)		

**Loebach, Matthew T.**

---

**From:** David Kustaborder [kusty@nist.gov]  
**Sent:** Thursday, December 02, 2010 1:36 PM  
**To:** Loebach, Matthew T.  
**Subject:** Fwd: FW: Wikileaks Site Block \*\*\*Situational Awareness\*\*\*  
**Attachments:** wiki\_sources.csv

fyi

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

**Subject:**FW: Wikileaks Site Block \*\*\*Situational Awareness\*\*\*

**Date:**Tue, 30 Nov 2010 14:28:05 -0500

**From:** [REDACTED] <[REDACTED]@nist.gov>

**To:**Kustaborder, David P. <david.kustaborder@nist.gov>

**CC:**Antonishek, John K. <john.antonishek@nist.gov> [REDACTED] <[REDACTED]@nist.gov>

(b)(6)  
David – per our conversation...

Rob G.

---

**From:** Chambers, William  
**Sent:** Tuesday, November 30, 2010 1:49 PM  
**To:** Richter, Gale C.  
**Cc:** Antonishek, John K. [REDACTED] (b)(6)  
**Subject:** RE: Wikileaks Site Block \*\*\*Situational Awareness\*\*\*

Firewall report is attached since 00:01 Friday. 36 sources were seen in firewall logs total using any destination associated with the domain in logs. This includes those taken from the dig of the wikileaks.org DNS servers below (184.72.37.90 and 46.51.171.90), plus observed traffic to sub-domains which revealed 204.236.131.131, 91.194.60.112, 91.194.60.32 and 91.194.60.90. These last addresses might seem strange, but I know the site moved to Amazon Web Services and possibly other places after they were DDoS attacked yesterday.

Answer records

wikileaks.org SOA

server: [REDACTED] (b)(6)

email: [hostmaster@wikileaks.org](mailto:hostmaster@wikileaks.org)

serial: 1291137007

refresh: 3600

retry: 900

expire: 1209600

minimum ttl: 3600

360s

wikileaks.org	NS	[REDACTED]	86400s
wikileaks.org	NS	[REDACTED]	86400s
wikileaks.org	NS	[REDACTED]	(b)(6) 86400s
wikileaks.org	NS	[REDACTED]	86400s
wikileaks.org	A	[REDACTED]	3600s
wikileaks.org	A	[REDACTED]	3600s

(b)(6)

wikileaks.org  
wikileaks.org

A  
A

3600s  
3600s



---

**From:** Richter, Gale C.  
**Sent:** Tuesday, November 30, 2010 12:48 PM  
**To:** Chambers, William  
**Cc:** Antonishek, John K.; Glenn, K. Robert  
**Subject:** RE: Wikileaks Site Block \*\*\*Situational Awareness\*\*\*

I'd do both given the immediacy of this requirement. I also just read the second paragraph. Can you generate a SPLUNK report with the list of IPs and send it to John who can try to match the user to the IP?

---

**From:** Chambers, William  
**Sent:** Tuesday, November 30, 2010 12:41 PM  
**To:** Richter, Gale C.  
**Subject:** RE: Wikileaks Site Block \*\*\*Situational Awareness\*\*\*

Gale:

Should I do this via the usual mailing lists or talk to the DNS admins individually?

---

**From:** Richter, Gale C.  
**Sent:** Tuesday, November 30, 2010 12:37 PM  
**To:** Chambers, William  
**Cc:** Antonishek, John K.; Glenn, K. Robert  
**Subject:** FW: Wikileaks Site Block \*\*\*Situational Awareness\*\*\*  
**Importance:** High

Bill - See e-mail below. Please have DNS black-hole blocks put in for the **Wikileaks.org** website and have each DNS admin notify everyone on this e-mail when the blocks are in place.

John - will you take care of notifying DOC when this is completed?

Thanks.  
Gale

---


**From:** members of the Federation of Department of Commerce CIRTs and CIRCs  
[mailto:FEDCIRT@LIST.COMMERCE.GOV] **On Behalf Of** Nguyen, Vu  
**Sent:** Tuesday, November 30, 2010 11:57 AM  
**To:** FEDCIRT@LIST.COMMERCE.GOV  
**Subject:** Wikileaks Site Block \*\*\*Situational Awareness\*\*\*  
**Importance:** High

Federation Team Members,

Due to recent reports of classified information residing on the Wikileaks.org website, all OU's are to immediately block access to the site via URL filter or DNS black-hole. Report completion of this task to DOC-CIRT by COB today.

In addition to the site-block, a report is required noting the number of PC's and a listing of users that have accessed the site since Friday, November 26, 2010. It is possible that these PC's could inadvertently contain classified information.

Thanks,  
Vu T. Nguyen  
Office of the Chief Information Officer  
Advanced Cyber Threat and Forensic Analysis Team Lead  
U.S. Department of Commerce  
E-mail: [vnnguyen@doc.gov](mailto:vnnguyen@doc.gov)  
SIPRNet: [vnnguyen@doc.sgov.gov](mailto:vnnguyen@doc.sgov.gov)  
Phone: (202) 482-6401  
Blackberry: (202) 834-9123

src	count	percent
	29	10.32029
	26	9.252669
	18	6.405694
	17	6.049822
	16	5.69395
	14	4.982206
	10	3.558719
	10	3.558719
	10	3.558719
	10	3.558719
	9	3.202847
	9	3.202847
	9	3.202847
	8	2.846975
	6	2.135231
	6	2.135231
	6	2.135231
	6	2.135231
	6	2.135231
	5	1.779359
	5	1.779359
	4	1.423488
	4	1.423488
	4	1.423488
	4	1.423488
	4	1.423488
	3	1.067616
	3	1.067616
	3	1.067616
	3	1.067616
	3	1.067616
3	1.067616	
3	1.067616	
2	0.711744	
2	0.711744	
1	0.355872	

(b)(2)

Run Date: 01/03/2011

Rpt Name: RMDYHD

**HelpDesk Record**

HD0000000372813

Severity 4

**HelpDesk Request****HelpDesk Request Information**

Case ID: HD0000000372813  
 Status: Closed  
 Pending Code:  
 Group: IT Security  
 Individual: Glenn, K. Robert  
 CTI: Security | Other | Other  
 Priority: Severity 4  
 Case Type: Question  
 Source: Phone  
 Submitter: Eldrige, Lisa A.  
 Billable Parts?: No

**Requester Information**

Requester Name: [REDACTED] (b)(6)  
 VIP: No (b)(6)  
 Email: [REDACTED]@nist.gov (b)(6)  
 Phone: [REDACTED] (b)(6)  
 OU: MML  
 Site: Boulder  
 Division: 638 (b)(2)  
 Office Location: [REDACTED]  
 NIST System#:

**Time Information**

Arrival Time: 12/02/2010 18:47:24  
 Create Time: 12/02/2010 18:46:56  
 Assigned Time: 12/06/2010 12:38:52  
 Resolved Time: 12/07/2010 14:02:09

Days Outstanding: 2  
 Total Time Spent(min): 36  
 ReOpen:

**Summary**

User contact by his supervisor who was contacted by his supervisor regarding a system that was used to look at WikiLeaks.

**Description**

User contact by his supervisor who was contacted by his supervisor regarding a system that was used to look at WikiLeaks. He does not know which system this may be and needs to know the next step. User did not access this site.

**Solution Summary**

Robert Sorensen and/or John Beltz will follow-up

**Solution Description**



Robert or John will follow-up for the initial sanitization; but additional follow-up with the student is likely.

### Work Log

12/06/2010 12:38:52 glenn

Waiting for reply with name of student.

From: Glenn, K. Robert

Sent: Monday, December 06, 2010 12:02 PM

To: [REDACTED] (b)(6)

Cc: Glenn, K. Robert

Subject: RE: IMPORTANT - RE: Guidance regarding WikiLeaks

(b)(2) Tom, The address is

[REDACTED] property # 930364. Please send the name of the student, so OSY can send them the inadvertent disclosure briefing.

Thanks,

Rob G.

(b)(6)  
From: [REDACTED] [mailto:[REDACTED]@boulder.nist.gov]

Sent: Monday, December 06, 2010 11:59 AM

To:

Glenn, K. Robert

Subject: Re: IMPORTANT - RE: Guidance regarding WikiLeaks

Rob:

Apparently this was done by a student. I have already spoken to the individual. Can you give me the IP address of the computer?

(b)(6)  
[REDACTED]

[REDACTED], Group

Leader

Experimental Properties of Fluids

Thermophysical Properties Division

National Institute of Standards and Technology

325 Broadway, MS 638.00

Boulder, CO 80305

303-497-[REDACTED] (office)

303-497-[REDACTED] (lab)

303-497-[REDACTED] (fax) (b)(6)

On 12/6/2010 9:32 AM,

Glenn, K. Robert wrote:

Dear [REDACTED]

I am the NIST IT Security Officer and I have been asked to contact all NIST staff who may have had a computer that connected to WikiLeaks prior to the guidance issued by DoC. Please be assured, that due to the nature of this issue, while this deals with access to potential classified information and we are required by DoC to respond to this incident, no one at NIST who went to the site prior to the guidance issued by DoC is going to get into any trouble. In fact, several NIST staff computers connected to the site prior to the issuance of the DoC guidance.

DOC has confirmed that WikiLeaks was accessed from a computer registered to you, which may mean classified information was unknowingly accessed. Because access occurred prior to receiving guidance from DOC (see below), this is viewed as an unintentional incident. However, NIST is required to treat the computer as though there is classified data resident (i.e., classified information spillage) and, the computer must be appropriately sanitized to ensure that any classified information is removed.

The NIST Office of Information Systems Management (formerly OCIO) incident response team (Robert Sorensen or John Beltz) will contact you to schedule sanitization of the computer. Please do not access, read, forward, or otherwise move any WikiLeaks documents that may have been downloaded. Also, please do not attempt to remove any such documents on your own. Sanitization will include removal of the information in your browser cache/history, temporary files, backups that may contain WikiLeaks documentation, etc., and verification that the information was not forwarded via other methods such as email, instant messaging, etc. Every effort will be made to preserve all other user data on the computer (i.e. this is a routine process and user data should not be affected). Given the number of incidents within NIST, we ask for your patience in scheduling sanitization. Since classified information is involved, the DOC Office of Security (OSY) will likely follow up and send you an inadvertent disclosure briefing which includes a reminder to not disclose any sensitive information you may have seen when going to the WikiLeaks site.

As a reminder, please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents.

Please do not hesitate to contact me personally if you have any questions or concerns.

Regards,

Rob Glenn  
IT Security Officer, NIST

rob.glenn@nist.gov  
301-975-3667

—Original Message—

From: allstaff@nist.gov [mailto:allstaff@nist.gov] On Behalf Of NIST IT Assistance Center  
Sent: Wednesday, December 01, 2010 2:45 PM  
To: Multiple recipients of list  
Subject: RE: Guidance regarding WikiLeaks

Attention NIST Staff:

To clarify the guidance that the Department of Commerce issued earlier today we ask that you not use the Commerce contact information provided in that email. Instead, direct any questions or notifications of access to WikiLeaks documents to the NIST IT Assistance Center (ITAC).

ITAC  
IT Assistance Center  
itac@nist.gov

303-497-5375  
(Boulder)  
301-975-5375 (Gaithersburg)

Hours of Operation:  
Boulder: 7:30am - 5:30pm (Mountain Time) Monday - Friday  
Gaithersburg: 7:30am - 5:30pm (Eastern Time) Monday - Friday

—Original Message—

From: allstaff@nist.gov  
[mailto:allstaff@nist.gov] On Behalf Of Broadcast, DOC  
Sent: Wednesday, December 01, 2010 11:11 AM  
To: Multiple recipients of list  
Subject: Guidance regarding WikiLeaks

To: All Commerce Employees and Contractors

Recent reports indicate that a number of government documents have been posted on the WikiLeaks website. These documents may or may not contain information that is considered National Security Information (classified information) and as such, the information is NOT authorized for downloading, viewing, printing, processing, copying, or transmitting via non-classified Government-issued computers, laptops, blackberries, or other communication devices and is not an authorized use of DOC IT equipment. Doing so would introduce potentially classified information onto our unclassified networks and represent a potential security incident.

There has been a rumor that the information is no longer classified since it resides in the public domain. This is NOT true. Executive Order 13526, Section 1.1(4)(2) states "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information." The information was neither properly nor improperly "declassified" by the appropriate authority and requires continued classification or reclassification.

Please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents because these documents may contain classified information. Accessing the WikiLeaks documents will lead to sanitization of your PC to remove any potentially classified information from the system and result in possible data loss.

If you have questions regarding this broadcast or have accessed the WikiLeaks documents, please contact the DOC Computer Incident Response Team at email doc-cirt@doc.gov or call (202) 482-4000.

---

This message was  
authorized by the Office of Secretary OSY/OCIO.

Please do not reply to this message. The broadcast email account is not monitored for incoming mail.  
12/07/2010 14:02:09 glenn

From: Glenn, K. Robert  
Sent: Tuesday, December 07, 2010 1:34 PM  
To: [REDACTED] (b)(6)

Cc: Glenn, K. Robert  
Subject RE: IMPORTANT - RE: Guidance regarding WikiLeaks

(b)(6), I'll have my staff follow-up with you to perform an initial sanitization, but they are likely to have questions that only your student can answer. They will need to follow up at a later date and ask if they did any more than just browse the site, and if they downloaded any documentation, where they would have put that documentation.

Regards,

Rob G.

From: [REDACTED] (b)(6)  
[mailto:[REDACTED]@boulder.nist.gov]  
Sent: Tuesday, December 07, 2010 9:06 AM  
To: Glenn, K. Robert  
Subject Re: IMPORTANT - RE: Guidance regarding WikiLeaks

Rob:

Follow up with me, not him. He has finals this week and then will be on break for some time.

Tom (b)(6)  
J. Bruno, Group Leader  
Experimental Properties of Fluids  
Thermophysical Properties Division  
National Institute of Standards and Technology  
325 Broadway, MS 638.00  
Boulder, CO 80305  
303-497-5158 (office)  
303-497-5978  
(lab)  
303-497-5044 (fax)

On 12/7/2010 6:33 AM, Glenn, K. Robert wrote:

(b)(6)  
We don't know the format or much else about the specific classified documents; I suspect given the quantity of material leaked from the site, that few know what is and

is not classified. DoC has required that we remove all traces of access to the wikileaks websites as well as any files that may have been downloaded.

I'll have my staff follow up with Evgenii to have the computer cleaned. After removing any relevant files, clearing browser history and temporary files, etc., they install software that will permanently erase any/all deleted files. This is a routine process for removing these types of files from computers and should not affect any other user data stored on the computer.

Regards,

Rob G.

From: [REDACTED] (b)(6) [mailto:[REDACTED]@boulder.nist.gov]  
Sent: Monday, December 06, 2010 4:01 PM  
To: Glenn, K. Robert  
Subject: Re: IMPORTANT - RE: Guidance regarding WikiLeaks

Is this a ppt?

His name is [REDACTED] (b)(6)

Dr. Thomas J. Bruno, Group Leader  
Experimental Properties of Fluids  
Thermophysical Properties Division  
National Institute of Standards and Technology  
325 Broadway, MS 638.00  
Boulder, CO 80305  
303-497-[REDACTED] (office)

303-497-[REDACTED] (lab) (b)(6)

303-497-[REDACTED] (fax)

12/14/2010 14:08:55 AR\_ESCALATOR

Case HD0000000372813 was automatically closed on 12/14/10 14:08:55.

The solution used is Robert Sorensen and/or John Beltz will follow-up

### Audit Trail

12/02/2010 18:47:24 eldrige

This ticket was submitted by eldrige on 12/02/10 18:47:24 with the Status of Assigned.

Status of Requester [REDACTED] (b)(6) AU Form =Y Employee =Y Locked =N Data Updated on 12/01/10 Term Date is

12/06/2010 12:38:52 glenn

Assigned

to Individual changed from to Glenn, K. Robert

The Status field has changed from Assigned to Pending

1/3/2011 3:13 PM

Pending field has changed from to Requester Information.

Status of Requester [REDACTED]: A/U Form =Y Employee =Y Locked =N Data  
Updated on 12/06/10 Term Date is (b)(6)

12/07/2010 14:02:10 glenn

The Status field has changed from Pending to Resolved

Pending field has changed from Requester Information to .

Status of Requester [REDACTED] (b)(6) A/U Form =Y Employee =Y Locked =N Data  
Updated on 12/07/10 Term Date is

12/14/2010 14:08:55 AR\_ESCALATOR

The Status field has changed from Resolved to Closed

Re Wikileak status and files (Updated) 12-23-11 130pm.txt  
From: Robert Sorensen [rsoren@boulder.nist.gov]  
Sent: Thursday, December 23, 2010 1:34 PM  
To: Beltz, John  
Cc: Sorensen, Robert; Kustaborder, David P.  
Subject: Re: Wikileak status and files (Updated)

John,

Here is an update of what I got completed.

Finished [REDACTED]. Also got [REDACTED] system at [REDACTED]. Left paperwork for both in your mail slot. Been trying to get hold of the system at [REDACTED] with no success. Left some info on the user in your box as well.

See you after the new year!

-Robert

> Scheduled:

> [REDACTED] (Windows) XXX [REDACTED] 191

> X [REDACTED] Left a message on voicemail. Scheduled for 10am on 12/14.

> Contacted, trying to set a time:

> [REDACTED] (Windows) 933751 [REDACTED] 697

> X [REDACTED] Left a message on voicemail. Dan called and left John a message at 3pm on 12/9/10. Called dan back on 12/14, left vmail.

> Have left vmails, no return:

> [REDACTED] (Windows) 931061 [REDACTED] 688

(email) [REDACTED]  
> X [REDACTED] Left a message on voicemail on 12/8/10. Another vmail on 12/14. Left email as well on 12/14.

> [REDACTED] (Windows) 933199 [REDACTED] 687

(email) [REDACTED]  
> X [REDACTED] No answer? No voicemail available. Left email on NIST account and gmail account on 12/14.

> Non-Windows

> [REDACTED] Box)

> Waiting for Instructions.

> [REDACTED] (Mac).

> Waiting for instructions.

> Completed:

> [REDACTED] (Windows) 940819 [REDACTED] 194

(email) [REDACTED]  
> X4579 Spoke with Nathan, anytime tomorrow, just call him before. Started Eraser on 12/9/10. Check back for completion. Completed by Robert on 12/10.

> [REDACTED] (Windows) 930364 [REDACTED]

(Student - POC: Dr. Thomas Bruno) 638

> X [REDACTED] Set a meeting for tomorrow at 9am. Started Eraser on 12/9/10. Check back for completion. Also need to follow up with the student when they return. Completed by Robert on 12/10.

> [REDACTED] (Windows) 851068 [REDACTED] 653

> X [REDACTED] Said anytime tomorrow ok. Just call him. Complete!

**Steve Needle**

---

**From:** Bob McClellan  
**Sent:** Tuesday, June 07, 2011 4:55 PM  
**To:** Steve Needle  
**Subject:** FW: Wikileaks PC's  
**Attachments:** wikileaks.xlsx

**From:** Bob McClellan  
**Sent:** Wednesday, December 01, 2010 9:58 AM  
**To:** Alan Willard  
**Cc:** Keith Sinner  
**Subject:** RE: Wikileaks PC's

See attached spreadsheet. Here are the PCs that accessed the wikileaks site since last Friday. All three accessed the site on 11/29:

(b)(2) (b)(6)  
[Redacted]  
[Redacted]

Doesn't look like anyone downloaded any documents.

Bob

**From:** Alan Willard  
**Sent:** Wednesday, December 01, 2010 6:30 AM  
**To:** Bob McClellan  
**Cc:** Keith Sinner  
**Subject:** Wikileaks PC's

Bob;

Please determine which workstations accessed the wikileaks.org website, Keith and I need the names of the users.

Thanks,  
Alan

---

Alan R. Willard, CISSP, GSEC  
Chief IT Security Officer  
National Technical Information Service  
Department of Commerce

P 703-605-6440  
C 703-389-1553  
F 703-605-6686

[awillard@ntis.gov](mailto:awillard@ntis.gov)



**McIntyre, Jeffrey J.**

---

**From:** David Kustaborder [kusty@nist.gov]  
**Sent:** Tuesday, December 21, 2010 3:38 PM  
**To:** Glenn, K. Robert  
**Cc:** siirt  
**Subject:** Wiki Status  
**Attachments:** wiki-contact.xls

---

Property Number		src	User	Sheet1	Division	Phone	Associate
634024		(b)(2)	(b)(2)		184		
631634					774		Y
629071					774		
931061					688		
624503					775		
934346					181		
631753					732		
634008					772		
851531					731		
940819					194		
850752					183		
612740					730		
933199					687		
851068					653		
					191		
623254					683		
629074					773		
621855					488		
940569					697		
624101					610		
631298					775		
617030					683		N
633663					470		E
633683					470		E
612061					682		N
930364					638		E
933751					688		N
634222					181		E
635896					771		E
851511					698		E
634111					684		E
635565					610		E
850223					620		E
634570					730		E

(b)(2)  
[REDACTED]

(b)(6)  
[REDACTED]

Sheet1

Sheet1

Sanitized

Complete

Complete

Complete

Complete

Complete

Complete

Complete

Complete

Complete

Complete

Complete

Complete

Complete

Complete

Complete

Complete

Complete

Complete

Complete

Complete

Complete

Complete

Complete

Complete

Scheduled for next Tuesday user is working 1<sup>st</sup> shift

Complete

Complete

Mac Safari

Linux Firefox

Mac

Windows Firefox

Linux Chrome

Windows IE

Students machine.  (b)(2)

CentOS firefox

NetBSD mozilla

Windows IE

Sheet1

Complete

Page 4

# Wikileaks Permitted Access (11/26/2010 - 11/30/2010)

Count of Hits	OU	User	Username	Day	Total
cablegate.wikileaks.org	BCE	[REDACTED]	lcanceko	2010-11-30	1
	BCE Total				1
	BIS	[REDACTED]		2010-11-29	1
	BIS Total				1
	DOCFCU	[REDACTED]		2010-11-30	1
	DOCFCU Total				1
	OIG	[REDACTED]		2010-11-29	1
	OIG Total				1
	OS	[REDACTED]	sstamps	2010-11-29	6
		[REDACTED]	wharris	2010-11-29	7
	OS Total				13
cablegate.wikileaks.org Total					17
wikileaks.org	EDA (Philadelphia)	[REDACTED]		2010-11-29	2
	EDA (Philadelphia) Total				2
	OIG	[REDACTED]		2010-11-29	1
	OIG Total				1
	OS	[REDACTED]	abukhari	2010-11-30	1
	OS Total				1
wikileaks.org Total					4
www.wikileaks.org	EDA (Chicago)	[REDACTED]		11/30/2010	2
	EDA (Chicago) Total				2
www.wikileaks.org Total					2
(blank)					
Grand Total					23

\* Username information was pulled from ePO. This is OS ONLY.

[2010-11-26-2010-11-30]

(b)(2)

User	OU	Username	Day	URL Hostname	Category	Hits	
	BIS	Citrix Svr	2010-11-29	cablegate.wikileaks.org	Advocacy Groups	1	Notified Jack Ward
	OIG		2010-11-29	cablegate.wikileaks.org	Advocacy Groups	1	Notified Gwen Thompson (Randall)
	BCE		2010-11-30	cablegate.wikileaks.org	Advocacy Groups	2	
	OS		2010-11-29	cablegate.wikileaks.org	Advocacy Groups	1	
	OS		2010-11-29	cablegate.wikileaks.org	Advocacy Groups	2	
	OS		2010-11-29	cablegate.wikileaks.org	Advocacy Groups	2	
	OS		2010-11-29	cablegate.wikileaks.org	Advocacy Groups	3	
	OS		2010-11-29	cablegate.wikileaks.org	Advocacy Groups	3	
	OS		2010-11-29	cablegate.wikileaks.org	Advocacy Groups	4	
	OS		2010-11-29	cablegate.wikileaks.org	Advocacy Groups	1	
	OS		2010-11-29	cablegate.wikileaks.org	Advocacy Groups	1	
	OS		2010-11-29	cablegate.wikileaks.org	Advocacy Groups	1	
	OS		2010-11-29	cablegate.wikileaks.org	Advocacy Groups	1	
	OS		2010-11-29	cablegate.wikileaks.org	Advocacy Groups	2	
	OS		2010-11-29	cablegate.wikileaks.org	Advocacy Groups	2	
	OS		2010-11-29	cablegate.wikileaks.org	Advocacy Groups	9	
	DOCFCU		2010-11-30	cablegate.wikileaks.org	Advocacy Groups	1	
	OIG		2010-11-29	wikileaks.org	Advocacy Groups	1	Notified Gwen Thompson (Randall)
	OS		2010-11-30	wikileaks.org	Advocacy Groups	5	
	EDA (Philadelphia)		2010-11-29	wikileaks.org	Advocacy Groups	1	Notified Sandra Moses (Edward)
	EDA (Philadelphia)		2010-11-29	wikileaks.org	Advocacy Groups	2	Notified Sandra Moses (Edward)
	EDA (Chicago)		11/30/2010	www.wikileaks.org	Advocacy Groups	3	Notified Sandra Moses
	EDA (Chicago)		11/30/2010	www.wikileaks.org	Advocacy Groups	9	Notified Sandra Moses
						58	

(b)(6)

Bureau	# Users	Comments
OS	4	
BIS	1	
EDA	2	
OIG	1	
DOCFCU	1	
Census	19	
USPTO	29	
NTIS	3	Confirmed no classified - per Alan Willard
BEA	9	
NIST	15	
NOAA	80	
ITA	24	Some hits where from OCONUS
	188	

#s are preliminary

As of 011245, only 3 people have called to confess



Sheet1

Property Number	src	count	percent	NNIS Primary User	Property User
634024	[REDACTED]	29	10.320285	[REDACTED]	[REDACTED] (b)(6)
631634	[REDACTED]	26	9.252669	[REDACTED]	[REDACTED]
	[REDACTED]	18	6.405694	[REDACTED]	[REDACTED]
629071	[REDACTED]	17	6.049822	[REDACTED]	[REDACTED]
931061	[REDACTED]	16	5.693950	[REDACTED]	[REDACTED]
624503	[REDACTED]	14	4.982206	[REDACTED]	[REDACTED]
934346	[REDACTED]	10	3.558719	[REDACTED]	[REDACTED]
631753	[REDACTED]	10	3.558719	[REDACTED]	[REDACTED] (b)(6)
634008	[REDACTED]	10	3.558719	[REDACTED]	[REDACTED]
851531	[REDACTED]	10	3.558719	[REDACTED]	[REDACTED]
940819	[REDACTED]	9	3.202847	[REDACTED]	[REDACTED]
850752	[REDACTED]	9	3.202847	[REDACTED]	[REDACTED]
612740	[REDACTED]	9	3.202847	[REDACTED]	[REDACTED]
933199	[REDACTED]	8	2.846975	[REDACTED]	[REDACTED]
851068	[REDACTED]	6	2.135231	[REDACTED]	[REDACTED]
Prop filled in as XXX	[REDACTED]	6	2.135231	[REDACTED]	[REDACTED]
623254	[REDACTED]	6	2.135231	[REDACTED]	[REDACTED]
629074	[REDACTED]	6	2.135231	[REDACTED]	[REDACTED]
621855	[REDACTED]	6	2.135231	[REDACTED]	[REDACTED]
940569	[REDACTED]	5	1.779359	[REDACTED]	[REDACTED]
624101	[REDACTED]	5	1.779359	[REDACTED]	[REDACTED]
631298	[REDACTED]	4	1.423488	[REDACTED]	[REDACTED]
617030	[REDACTED]	4	1.423488	[REDACTED]	[REDACTED] (b)(6)
633663	[REDACTED]	4	1.423488	[REDACTED]	[REDACTED]
633683	[REDACTED]	4	1.423488	[REDACTED]	[REDACTED]
612061	[REDACTED]	4	1.423488	[REDACTED]	[REDACTED]
930364	[REDACTED]	3	1.067616	[REDACTED]	[REDACTED]
933751	[REDACTED]	3	1.067616	[REDACTED]	[REDACTED]
634222	[REDACTED]	3	1.067616	[REDACTED]	[REDACTED]
635896	[REDACTED]	3	1.067616	[REDACTED]	[REDACTED]
851511	[REDACTED]	3	1.067616	[REDACTED]	[REDACTED]
634111	[REDACTED]	3	1.067616	[REDACTED]	[REDACTED]
635565	[REDACTED]	3	1.067616	[REDACTED]	[REDACTED]
850223	[REDACTED]	2	0.711744	[REDACTED]	[REDACTED]
634570	[REDACTED]	2	0.711744	[REDACTED]	[REDACTED]
	[REDACTED]	1	0.355872	[REDACTED]	[REDACTED]

(b)(2)

774  
184  
774  
688  
775  
181  
732  
772  
731  
194  
183  
730  
687  
653  
191  
683  
773  
488  
697  
610  
775  
683  
470  
470  
682  
638  
688  
181  
771  
836  
840  
610  
620  
730

[REDACTED] (b)(6)

[REDACTED] { (b)(6) }

[REDACTED] (b)(6)

MISC Info

[REDACTED]  
(b)(6)

Was [REDACTED] Desktop computer, now [REDACTED] has it

(b)(6)

**Loebach, Matthew T.**

---

**From:** David Kustaborder [kusty@nist.gov]  
**Sent:** Thursday, December 02, 2010 1:33 PM  
**To:** Loebach, Matthew T.; Hurst V, Alfred Coulter  
**Subject:** wiki  
**Attachments:** wiki\_sources(with\_users).xls

Sheet1

Property Number	src	count	percent	NNIS Primary User	Property User
634024	[REDACTED]	29	10.320285	[REDACTED]	[REDACTED]
631634	[REDACTED]	26	9.252669	[REDACTED]	[REDACTED]
	[REDACTED]	18	6.405694	[REDACTED]	[REDACTED]
629071	[REDACTED]	17	6.049822	[REDACTED]	[REDACTED]
931061	[REDACTED]	16	5.693950	[REDACTED]	[REDACTED]
624503	[REDACTED]	14	4.982206	[REDACTED]	[REDACTED]
934346	[REDACTED]	10	3.558719	[REDACTED]	[REDACTED]
631753	[REDACTED]	10	3.558719	[REDACTED]	[REDACTED]
634008	[REDACTED]	10	3.558719	[REDACTED]	[REDACTED]
851531	[REDACTED]	10	3.558719	[REDACTED]	[REDACTED]
940819	[REDACTED]	9	3.202847	[REDACTED]	[REDACTED]
850752	[REDACTED]	9	3.202847	[REDACTED]	[REDACTED]
612740	[REDACTED]	9	3.202847	[REDACTED]	[REDACTED]
933199	[REDACTED]	8	2.846975	[REDACTED]	[REDACTED]
851068	[REDACTED]	6	2.135231	[REDACTED]	[REDACTED]
Prop filled in as XXX	[REDACTED]	6	2.135231	[REDACTED]	[REDACTED]
623254	[REDACTED]	6	2.135231	[REDACTED]	[REDACTED]
629074	[REDACTED]	6	2.135231	[REDACTED]	[REDACTED]
621855	[REDACTED]	6	2.135231	[REDACTED]	[REDACTED]
940569	[REDACTED]	5	1.779359	[REDACTED]	[REDACTED]
624101	[REDACTED]	5	1.779359	[REDACTED]	[REDACTED]
631298	[REDACTED]	4	1.423488	[REDACTED]	[REDACTED]
617030	[REDACTED]	4	1.423488	[REDACTED]	[REDACTED]
633663	[REDACTED]	4	1.423488	[REDACTED]	[REDACTED]
633683	[REDACTED]	4	1.423488	[REDACTED]	[REDACTED]
612061	[REDACTED]	4	1.423488	[REDACTED]	[REDACTED]
930364	[REDACTED]	3	1.067616	[REDACTED]	[REDACTED]
933751	[REDACTED]	3	1.067616	[REDACTED]	[REDACTED]
634222	[REDACTED]	3	1.067616	[REDACTED]	[REDACTED]
635896	[REDACTED]	3	1.067616	[REDACTED]	[REDACTED]
851511	[REDACTED]	3	1.067616	[REDACTED]	[REDACTED]
634111	[REDACTED]	3	1.067616	[REDACTED]	[REDACTED]
635565	[REDACTED]	3	1.067616	[REDACTED]	[REDACTED]
850223	[REDACTED]	2	0.711744	[REDACTED]	[REDACTED]
634570	[REDACTED]	2	0.711744	[REDACTED]	[REDACTED]
	[REDACTED]	1	0.355872	[REDACTED]	[REDACTED]

(b)(2)

(b)(6)

LANDesk User    Division

Data not filled in

774  
184

774  
688  
775  
181  
732  
772  
731  
194  
183  
730  
687  
653  
191  
683  
773  
488  
697  
610  
775  
683  
470  
470  
682  
638  
688  
181  
771  
836  
840  
610  
620  
730

(b)(6)

(b)(6)

(b)(6)

MISC Info

[REDACTED] (b)(6)

Was [REDACTED] Desktop computer, now [REDACTED] has it  
(b)(6)

[REDACTED] (b)(6)

RE: Guidance regarding WikiLeaks

**Subject:** RE: Guidance regarding WikiLeaks  
**From:** "Glenn, K. Robert" <robert.glenn@nist.gov>  
**Date:** Fri, 3 Dec 2010 10:57:38 -0500  
**To:** "Wilkinson, R. Allen" <r.allen.wilkinson@nist.gov>  
**CC:** siirt <siirt@nist.gov>, "Glenn, K. Robert" <robert.glenn@nist.gov>

Allen, I've now reached both of your users. Here is the additional information.

633663 (b)(6)  
633683 (b)(6)

It is important that this issue be treated delicately and that this information not spread nor used to embarrass the users and they should continue to be reassured that they will not be getting into any trouble over this as long as they continue to refrain from accessing wikileaks documentation.

SIIRT will be following up to schedule desanitization. OSY will be following up to give them an inadvertent disclosure briefing.

Rob G.

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

From: Wilkinson, R. Allen  
Sent: Friday, December 03, 2010 8:30 AM  
To: Glenn, K. Robert  
Subject: RE: Guidance regarding WikiLeaks

Rob,

That is fine. Just did not want the backups overlooked 🙄

Let us know how else we can help,

Allen

R. Allen Wilkinson, CISSP  
IT Security Officer  
Technology Innovation Program  
National Institute of Standards & Technology  
[r.allen.wilkinson@nist.gov](mailto:r.allen.wilkinson@nist.gov)  
301-975-3383

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

From: Glenn, K. Robert  
Sent: Friday, December 03, 2010 8:28 AM  
To: Wilkinson, R. Allen  
Cc: siirt; Glenn, K. Robert  
Subject: RE: Guidance regarding WikiLeaks

Allen,

SIIRT will have to determine what needs to be done in those cases.

Rob G.

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

From: Wilkinson, R. Allen  
Sent: Friday, December 03, 2010 8:23 AM



To: Glenn, K. Robert  
Subject: RE: Guidance regarding WikiLeaks

Rob,

This sounds good. Since it has been a week since Nov 26 I am quite sure that TIP's 2 machines have been backed up. What should be done with the backups?

Allen

R. Allen Wilkinson, CISSP  
IT Security Officer  
Technology Innovation Program  
National Institute of Standards & Technology  
[r.allen.wilkinson@nist.gov](mailto:r.allen.wilkinson@nist.gov)  
301-975-3383

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

From: [ou\\_secur@nist.gov](mailto:ou_secur@nist.gov) [[mailto:ou\\_secur@nist.gov](mailto:ou_secur@nist.gov)] On Behalf Of Glenn, K. Robert  
Sent: Friday, December 03, 2010 8:09 AM  
To: Multiple recipients of list  
Subject: RE: Guidance regarding WikiLeaks

OU ITSOs,

In close consultation with the NIST Director's Office and DoC, we now have a plan to move forward for NIST computers that connected to wikileaks before blocks were implemented. I've included some details and highlights of the plan below; the technical work will be performed by SIIRT (and given that there are 36 computers involved, this could impact other priorities).

1) Notify users verbally that their computer has been identified as having accessed Wikileaks documentation and as a result, may have unknowingly accessed classified information. Users are re-assured that they are not in trouble over this as the access was done prior to DoC guidance being issued. The notification will also explain that over the next several days NIST OISM incident response staff will work with them to properly sanitize their computer. Until the sanitization is complete, users may continue using their computer, but they are not to access, read, or move any Wikileaks documentation downloaded to their computer. Users are also not to try to sanitize their own computers. Users will also be notified that DoC OSY will follow-up with them to provide a inadvertent disclosure briefing. Those with clearances may be asked (by OSY) to take refresher training.

> Status: Susannah and I started contacting users late yesterday afternoon and will try to complete this today.

2) Notify OU Directors and OU ITSOs that have affected computers in their OUs;

> Status: Del started contacting OU Directors late yesterday afternoon. This email is your initial notification. Once all users in your OU have been contacted, I will then send the relevant OU ITSO the list of their affected users/computers.

3) SIIRT to complete detailed analysis of network logs to prioritize the order for which computers will be sanitized. Computers that have accessed the site the most or downloaded the most documentation will be sanitized first.

4) For each computer to be sanitized SIIRT will schedule time with each user (in prioritized order) to:

a) Identify the browser used; for each browser, clear cache, history, temporary files, etc.

b) Verify if the user stored any downloaded files elsewhere (e.g., thumb drives, CDs, DVDs, backups, etc.). Verify that nothing was forwarded to other people via other methods such as email, IM, etc.

RE: Guidance regarding WikiLeaks

- c) Delete all other files and completely erase all unused data sectors on all relevant media and hard disks.
  - d) Sanitize or destroy any mobile media or backup storage used to store Wikileaks documentation.
  - e) Document all steps performed, responses from the user to questions, and any errors that may arise during the procedure.
- 5) Notify DoC OCIO that clean up has been completed and that specific details are available as needed.

=====

Note, that while the technical steps follow standard operating procedures for classified spillage clean-up, some aspects of the overall procedures (e.g. allowing users to continue using the computer) are only being done due to the massively public nature of the spillage. For more typically spillage incidents, the computer would be immediately removed from the network and sanitization would be immediate. For larger spillages, the hard drive would be removed, labeled, and stored in an approved container until the sanitization could be completed. The plan above was reviewed and approved by the Director's Office.

# of users/computers per OU (for OUs is not listed, there were no computers identified at this time):

OISM: 4 (1 in Boulder)  
OFPM: 2 (both in Boulder)  
TIP: 2  
MEP: 1  
NCNR: 2  
CNST: 1  
MML: 2 (both in Boulder)  
PML: 9 (4 in Boulder)  
EL: 4  
ITL: 9

Rob G.

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

From: [allstaff@nist.gov](mailto:allstaff@nist.gov) [<mailto:allstaff@nist.gov>] On Behalf Of NIST IT Assistance Center  
Sent: Wednesday, December 01, 2010 2:45 PM  
To: Multiple recipients of list  
Subject: RE: Guidance regarding WikiLeaks

Attention NIST Staff:

To clarify the guidance that the Department of Commerce issued earlier today we ask that you not use the Commerce contact information provided in that email. Instead, direct any questions or notifications of access to WikiLeaks documents to the NIST IT Assistance Center (iTAC).

iTAC  
IT Assistance Center  
[itac@nist.gov](mailto:itac@nist.gov)

303-497-5375 (Boulder)  
301-975-5375 (Gaithersburg)

Hours of Operation:  
Boulder: 7:30am - 5:30pm (Mountain Time) Monday - Friday  
Gaithersburg: 7:30am - 5:30pm (Eastern Time) Monday - Friday

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

E: Guidance regarding WikiLeaks

From: [allstaff@nist.gov](mailto:allstaff@nist.gov) [<mailto:allstaff@nist.gov>] On Behalf Of Broadcast, DOC  
Sent: Wednesday, December 01, 2010 11:11 AM  
To: Multiple recipients of list  
Subject: Guidance regarding WikiLeaks

To: All Commerce Employees and Contractors

Recent reports indicate that a number of government documents have been posted on the WikiLeaks website. These documents may or may not contain information that is considered National Security Information (classified information) and as such, the information is NOT authorized for downloading, viewing, printing, processing, copying, or transmitting via non-classified Government-issued computers, laptops, blackberries, or other communication devices and is not an authorized use of DOC IT equipment. Doing so would introduce potentially classified information onto our unclassified networks and represent a potential security incident.

There has been a rumor that the information is no longer classified since it resides in the public domain. This is NOT true. Executive Order 13526, Section I.1(4)(2) states "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information." The information was neither properly nor improperly "declassified" by the appropriate authority and requires continued classification or reclassification.

Please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents because these documents may contain classified information. Accessing the WikiLeaks documents will lead to sanitization of your PC to remove any potentially classified information from the system and result in possible data loss.

If you have questions regarding this broadcast or have accessed the WikiLeaks documents, please contact the DOC Computer Incident Response Team at email [doc-cirt@doc.gov](mailto:doc-cirt@doc.gov) or call (202) 482-4000.

---

This message was authorized by the Office of Secretary OSY/OCIO.

Please do not reply to this message. The broadcast email account is not monitored for incoming mail.

**Loebach, Matthew T.**

---

**From:** David Kustaborder [kusty@nist.gov]  
**Sent:** Thursday, December 02, 2010 3:38 PM  
**To:** Glenn, K. Robert; siirt  
**Subject:** Contacts.  
**Attachments:** wiki-contact.xls

Property Number	src	User
634024	[REDACTED]	[REDACTED]
631634	[REDACTED]	[REDACTED]
629071	[REDACTED]	[REDACTED]
931061	[REDACTED]	[REDACTED]
624503	[REDACTED]	[REDACTED]
934346	[REDACTED]	[REDACTED]
631753	[REDACTED]	[REDACTED]
634008	[REDACTED]	[REDACTED]
851531	[REDACTED]	[REDACTED]
940819	[REDACTED]	[REDACTED]
850752	[REDACTED]	[REDACTED]
612740	[REDACTED]	[REDACTED]
933199	[REDACTED]	[REDACTED]
851068	[REDACTED]	[REDACTED]
Prop filled in as XXX		
623254	[REDACTED]	[REDACTED]
629074	[REDACTED]	[REDACTED]
621855	[REDACTED]	[REDACTED]
940569	[REDACTED]	[REDACTED]
624101	[REDACTED]	[REDACTED]
631298	[REDACTED]	[REDACTED]
617030	[REDACTED]	[REDACTED]
633663	[REDACTED]	[REDACTED]
633683	[REDACTED]	[REDACTED]
612061	[REDACTED]	[REDACTED]
930364	[REDACTED]	[REDACTED]
933751	[REDACTED]	[REDACTED]
634222	[REDACTED]	[REDACTED]
635896	[REDACTED]	[REDACTED]
851511	[REDACTED]	[REDACTED]
634111	[REDACTED]	[REDACTED]
635565	[REDACTED]	[REDACTED]
850223	[REDACTED]	[REDACTED]
634570	[REDACTED]	[REDACTED]

(b)(2) (b)(2)

Division Phone

184  
774  
774  
688  
775  
181  
732  
772  
731  
194  
183  
730  
687  
653  
191  
683  
773  
488  
697  
610  
775  
683  
470  
470  
682  
638  
688  
181  
771  
698  
684  
610  
620  
730



(b)(2)

RE: Updated user "script"

**Subject:** RE: Updated user "script"  
**From:** "Glenn, K. Robert" <robert.glenn@nist.gov>  
**Date:** Thu, 2 Dec 2010 16:01:31 -0500  
**To:** "Glenn, K. Robert" <robert.glenn@nist.gov>, "Schiller, Susannah B." <susannah.schiller@nist.gov>, "Brockett, Del" <del.brockett@nist.gov>  
**CC:** "Glenn, K. Robert" <robert.glenn@nist.gov>

List of users attached.

Rob G.

---

**From:** Glenn, K. Robert  
**Sent:** Thursday, December 02, 2010 3:48 PM  
**To:** Schiller, Susannah B.; Brockett, Del  
**Cc:** Glenn, K. Robert  
**Subject:** Updated user "script"

Attached is the updated script for users. Mostly minor changes (I included a note so you can mention names of the incident response team). If I notice the user is particularly concerned, I will re-assure them that this inadvertent will not result in them getting into any trouble but we do need them to work with the incident response staff to get this resolved quickly.

The list is almost complete (sans 1 or 2 users) and I'll be sending it shortly, sorted by OU.

Rob G.

<b>wiki-contacts.xls</b>	<b>Content-Description:</b> wiki-contacts.xls <b>Content-Type:</b> application/vnd.ms-excel <b>Content-Encoding:</b> base64
--------------------------	---

Property Number src

User

934346

634222

850752

631634

Prop filled in as XXX

940819

633663

633683

621855

624101

635565

850223

930364

851068

612061

623254

617030

634111

933199

931061

933751

940569

851511

612740

634570

851531

631753

635896

634008

629074

629071

624503

631298

634024

(b)(2)  
(b)(6)



Division	Phone	Employee	OU
181	[REDACTED]	Y	OISM
181	[REDACTED]	Y	
183	[REDACTED]	Y	
184	[REDACTED]	Y	
191	[REDACTED]	Y	OFPM
194	[REDACTED]	Y	
470	[REDACTED]	Y	TIP
470	[REDACTED]	Y	
488	[REDACTED]	Y	MEP
610	[REDACTED]	N	NCNR
610	[REDACTED]	Y	
620	[REDACTED]	Y	CNST
638	[REDACTED]	Y	MML
653	[REDACTED]	N	
682	[REDACTED]	N	PML
683	[REDACTED]	Y	
683	[REDACTED]	N	
684	[REDACTED]	Y	
687	[REDACTED]	N	
688	[REDACTED]	Y	
688	[REDACTED]	N	
697	[REDACTED]	N	
698	[REDACTED]	Y	
730	[REDACTED]	Y	EL
730	[REDACTED]	Y	
731	[REDACTED]	N	
732	[REDACTED]	Y	
771	[REDACTED]	Y	ITL
772	[REDACTED]	Y	
773	[REDACTED]	Y	
774	[REDACTED]	N	
774	[REDACTED]	Y	
775	[REDACTED]	Y	
775	[REDACTED]	Y	

(b)(2)

RE: Urgent: need to confirm user assigned to IP: 1...

(b)(2)

**Subject:** RE: Urgent: need to confirm user assigned to IP: [REDACTED]  
**From:** "Cochran, Brian" <brian.cochran@nist.gov>  
**Date:** Fri, 3 Dec 2010 09:15:23 -0500  
**To:** "Garris, Michael D." <michael.garris@nist.gov>  
**CC:** "Watson, Craig I." <craig.watson@nist.gov>, "Flanagan, Patricia A." <patricia.flanagan@nist.gov>, "Kustaborder, David P." <david.kustaborder@nist.gov>

Good morning Mike and David,

(b)(2)

Yes, you are correct. That machine is an iMAC assigned to [REDACTED] NIST # 634024  
machine name [REDACTED] MAC address [REDACTED]

(b)(2)

Regards,

Brian

---

**From:** Garris, Michael D.  
**Sent:** Friday, December 03, 2010 8:37 AM  
**To:** Cochran, Brian  
**Cc:** Watson, Craig I.; Flanagan, Patricia A.; Kustaborder, David P.  
**Subject:** Urgent: need to confirm user assigned to IP: [REDACTED]

(b)(2)

Brian,

I have a time-sensitive action that I need you to take. (My understanding is that both Craig and Pat are out of the office today.)

David Kustaborder of OISM needs to verify who the user is assigned to IP:

[REDACTED] It is a MAC OS machine, and he thinks it is assigned to [REDACTED] (b)(2)

(b)(2)

Can you please verify and then email me and David (@ [kustv@nist.gov](mailto:kustv@nist.gov)) with your determination?

I am in a management planning meeting all day today, so I can check my Blackberry at a break to get status. If you need to reach me, feel free to come to LR-E.

Thanks for your prompt action.

Mike

=====  
Michael D. Garris  
Image Group Leader  
mgarris@nist.gov  
VOICE: 301-975-2928

RE: Urgent: need to confirm user assigned to IP: 1...

FAX: 301-975-5287

National Institute of Standards and Technology  
100 Bureau Drive Stop 8940  
Gaithersburg, MD 20899-8940

---

RE: Updated user "script"

**Subject:** RE: Updated user "script"

**From:** "Schiller, Susannah B." <susannah.schiller@nist.gov>

**Date:** Fri, 3 Dec 2010 10:55:19 -0500

**To:** "Glenn, K. Robert" <robert.glenn@nist.gov>, "Brockett, Del" <del.brockett@nist.gov>

Seems like overkill to me – he'd be a good candidate for an email, IMHO

---

**From:** Glenn, K. Robert

**Sent:** Friday, December 03, 2010 10:54 AM

**To:** Brockett, Del; Schiller, Susannah B.

**Cc:** Glenn, K. Robert

**Subject:** RE: Updated user "script"

Thanks, Del. (b)(6) has been a more difficult case as he doesn't have voicemail on his phone. I appreciate the update. May have to set an alarm clock to get in touch with him early enough.

Rob G.

---

**From:** Brockett, Del

**Sent:** Friday, December 03, 2010 10:46 AM

**To:** Schiller, Susannah B.; Glenn, K. Robert

**Subject:** RE: Updated user "script"

I just heard back from Rob D.

(b)(6) is working the 11 pm – 7 am shift in the reactor. I am getting confirmation that he will be there tonight.

Del

---

**From:** Schiller, Susannah B.

**Sent:** Friday, December 03, 2010 10:40 AM

**To:** Glenn, K. Robert; Brockett, Del

**Subject:** RE: Updated user "script"

I'm making progress. I've tried everyone in Gburg at least 3 times, and have reached all but 2 of them. I'm getting ready to do second tries for 3 Boulder folks.

A couple of computers aren't used by the people listed. Darrin Santay was able to identify the right guy for his, and I've talked to that person and noted it in my spreadsheet that I'll send.

Judy Terrill checked all the boxes in her office and couldn't find the property number, so she asked that we work with Don Koss to identify where the computer is and who might have used it. The relevant property number is 635896 and the IP address is (b)(6)

After I take another stab at my Boulder folks, I'm all in favor of sending the remaining people the email. Not sure it's even worth leaving voicemail.

---

**From:** Glenn, K. Robert

**Sent:** Friday, December 03, 2010 10:31 AM

**To:** Glenn, K. Robert; Schiller, Susannah B.; Brockett, Del

E: Updated user "script"

**Cc:** Glenn, K. Robert

**Subject:** RE: Updated user "script"

After 1 attempt yesterday and 2 attempts today, I'm still unable to get in touch with 6 out of 17 users (Susannah ?). I plan on trying 1 more time before lunch. At what point can we leave them a voicemail reassuring them that they are not in trouble; but we need to work with them to have their computer sanitized, and let them know we'll send the details in an email?

Rob G.

---

**From:** Glenn, K. Robert

**Sent:** Thursday, December 02, 2010 3:48 PM

**To:** Schiller, Susannah B.; Brockett, Del

**Cc:** Glenn, K. Robert

**Subject:** Updated user "script"

Attached is the updated script for users. Mostly minor changes (I included a note so you can mention names of the incident response team). If I notice the user is particularly concerned, I will re-assure them that this inadvertent will not result in them getting into any trouble but we do need them to work with the incident response staff to get this resolved quickly.

The list is almost complete (sans 1 or 2 users) and I'll be sending it shortly, sorted by OU.

Rob G.

**Schiller, Susannah B.**

---

**From:** Schiller, Susannah B.  
**Sent:** Friday, December 03, 2010 11:01 AM  
**To:** Glenn, K. Robert; Brockett, Del  
**Subject:** RE: Updated user "script"  
**Attachments:** Wikileaks email to staff v4.docx

OK, here's my official count:

3 in Boulder have not been contacted yet (tried once yesterday and once today).

2 in Gaithersburg have not been contacted yet (tried once yesterday and twice today).

The computer listed for Judy Terrill needs to be tracked down -- where it is, who might have used it. Don Koss should be able to help.

My notes are attached (see second page of document)

**From:** Glenn, K. Robert  
**Sent:** Friday, December 03, 2010 10:54 AM  
**To:** Brockett, Del; Schiller, Susannah B.  
**Cc:** Glenn, K. Robert  
**Subject:** RE: Updated user "script"

Thanks, Del. (b)(6) has been a more difficult case as he doesn't have voicemail on his phone. I appreciate the update. May have to set an alarm clock to get in touch with him early enough.

Rob G.

**From:** Brockett, Del  
**Sent:** Friday, December 03, 2010 10:46 AM  
**To:** Schiller, Susannah B.; Glenn, K. Robert  
**Subject:** RE: Updated user "script"

I just heard back from Rob D.

(b)(2) is working the 11 pm - 7 am shift in the reactor. I am getting confirmation that he will be there tonight.

Del

**From:** Schiller, Susannah B.  
**Sent:** Friday, December 03, 2010 10:40 AM  
**To:** Glenn, K. Robert; Brockett, Del  
**Subject:** RE: Updated user "script"

I'm making progress. I've tried everyone in Gburg at least 3 times, and have reached all but 2 of them. I'm getting ready to do second tries for 3 Boulder folks.

A couple of computers aren't used by the people listed. Darrin Santay was able to identify the right guy for his, and I've talked to that person and noted it in my spreadsheet that I'll send.

Judy Terrill checked all the boxes in her office and couldn't find the property number, so she asked that we work with Don Koss to identify where the computer is and who might have used it. The relevant property number is 635896 and the IP address is (b)(2)

After I take another stab at my Boulder folks, I'm all in favor of sending the remaining people the email. Not sure it's even worth leaving voicemail.

---

**From:** Glenn, K. Robert  
**Sent:** Friday, December 03, 2010 10:31 AM  
**To:** Glenn, K. Robert; Schiller, Susannah B.; Brockett, Del  
**Cc:** Glenn, K. Robert  
**Subject:** RE: Updated user "script"

After 1 attempt yesterday and 2 attempts today, I'm still unable to get in touch with 6 out of 17 users (Susannah ?). I plan on trying 1 more time before lunch. At what point can we leave them a voicemail reassuring them that they are not in trouble; but we need to work with them to have their computer sanitized, and let them know we'll send the details in an email?

Rob G.

---

**From:** Glenn, K. Robert  
**Sent:** Thursday, December 02, 2010 3:48 PM  
**To:** Schiller, Susannah B.; Brockett, Del  
**Cc:** Glenn, K. Robert  
**Subject:** Updated user "script"

Attached is the updated script for users. Mostly minor changes (I included a note so you can mention names of the incident response team). If I notice the user is particularly concerned, I will re-assure them that this inadvertent will not result in them getting into any trouble but we do need them to work with the incident response staff to get this resolved quickly.

The list is almost complete (sans 1 or 2 users) and I'll be sending it shortly, sorted by OU.

Rob G.

DOC has confirmed that WikiLeaks was accessed from a computer registered to you, which may mean classified information was unknowingly accessed. Because access occurred prior to receiving guidance from DOC this is viewed as an unintentional incident. However, NIST is required to treat the computer as though there is classified data resident (i.e., classified information spillage) and, the computer must be appropriately sanitized to ensure that any classified information is removed.

The NIST Office of Information Systems Management (formerly OCIO) incident response team (note: for Gaithersburg, this will be John Antonishek, Matt Loebach, David Kustaborder, Jeff McIntyre, Al Hurst; for Boulder this will be John Beltz or Robert Sorensen) will contact you to schedule sanitization of the computer. Please do not access, read, forward, or otherwise move any WikiLeaks documents that may have been downloaded. Also, please do not attempt to remove any such documents on your own. Sanitization will include removal of the information in your browser cache/history, temporary files, backups that may contain WikiLeaks documentation, etc., and verification that the information was not forwarded via other methods such as email, instant messaging, etc. During the sanitization, every effort will be made to preserve all other user data. Given the number of incidents within NIST, we ask for your patience in scheduling sanitization. Since classified information is involved, the DOC Office of Security (OSY) will also follow up to schedule an inadvertent disclosure briefing.

As a reminder, please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents.

Do you have any questions or concerns?



634111 [redacted] [redacted]

No contact - tried 3 times. (b)(2)(b)(6)

634111 [redacted] (b)(6)

(b)(6) Hasn't used this computer much; colleague may have - [redacted] (a fed). [redacted] says he hasn't used the computer to access the internet at all lately.

612740 [redacted]

Explained it to her. (b)(2)(b)(6)

634570 [redacted]

"just poked around - when it asked him to register, he bailed."

631733 [redacted]

Explained it to him. He cleans up cache every few days, may have already done so, but I instructed him not to do any additional cleanup before the incident response team comes to visit. (b)(2)(b)(6)

635896 [redacted]

It wasn't her computer. Work with Don Koss to identify where this computer is and who would have used it. She'd like to know what we find out, and also any recommendations for additional policies she should institute to make her computers safer (she's pretty strict with her group).

(b)(6) 634008 [redacted] (b)(6)

Talked to [redacted] and explained. He said [redacted] is the actual owner of the computer (they aren't good about updating the database, and [redacted] brings in computers by the boatload for his division). Called [redacted] and explained. He said he just went to the site to see the format of the site and didn't download any documents. (b)(2)(b)(6)

629074 [redacted] (b)(2)(b)(6)

Didn't download or view. Doesn't understand why we need to do anything to his computer, but said they can "come on over."

629074 [redacted] (b)(2)(b)(6)

Explained it to him. He didn't go there deliberately - thinks he was looking at CNN.

624503 [redacted] (b)(2)(b)(6)

Explained it to her. She did ask if management had to know (after I'd already reassured her she didn't do anything wrong), and I told her about Pat's strong advocacy for our employees. (b)(2)

631298 [redacted]

No contact - tried 3 times. (b)(2)(b)(6)

851531 [redacted] (b)(2)(b)(6)

Explained it to him. He just looked at a couple of documents. (b)(2)(b)(6)

933199 [redacted]

No contact - tried twice. No voicemail on this number.

931061 [redacted]

No contact - tried twice. (b)(2)(b)(6)

933751 [redacted]

No contact - tried twice.

940569 [redacted]

Explained it to him. (b)(2)(b)(6)

[redacted] (Guest Researcher)

Unix machine - his main lab machine. It is a NIST-owned computer. Asked me to send him an email, which I did.

**McIntyre, Jeffrey J.**

---

**From:** David Kustaborder [kusty@nist.gov]  
**Sent:** Friday, December 03, 2010 11:18 AM  
**To:** Glenn, K. Robert  
**Cc:** siirt  
**Subject:** Re: Updated user "script"

The user is (Guest Researcher):

(b)(6)  
[REDACTED] (Gaithersburg) - [REDACTED]@nist.gov  
name: [REDACTED] (Gaithersburg)  
phone: [REDACTED] (b)(6)  
depart: Applied and Computational Mathematics Division (771)  
office: [REDACTED]  
agency: [REDACTED] (b)(2)  
address: 100 Bureau Drive, Stop 8911  
: Gaithersburg, MD 20899-8911  
email: [REDACTED]@nist.gov  
alternate email: [REDACTED]@nist.gov  
Last Updated: Fri Dec 3 2:45:02 2010  
(b)(6)

On 12/03/2010 10:51 AM, Glenn, K. Robert wrote:  
SIIRT, see the note from Judy and see what we can do to find that computer and the relevant user.

Thanks,

Rob G.

---

**From:** Schiller, Susannah B.  
**Sent:** Friday, December 03, 2010 10:40 AM  
**To:** Glenn, K. Robert; Brockett, Del  
**Subject:** RE: Updated user "script"

I'm making progress. I've tried everyone in Gburg at least 3 times, and have reached all but 2 of them. I'm getting ready to do second tries for 3 Boulder folks.

A couple of computers aren't used by the people listed. Darrin Santay was able to identify the right guy for his, and I've talked to that person and noted it in my spreadsheet that I'll send.

Judy Terrill checked all the boxes in her office and couldn't find the property number, so she asked that we work with Don Koss to identify where the computer is and who might have used it. The relevant property number is 635896 and the IP address is [REDACTED] (b)(2)

After I take another stab at my Boulder folks, I'm all in favor of sending the remaining people the email. Not sure it's even worth leaving voicemail.

---

**From:** Glenn, K. Robert  
**Sent:** Friday, December 03, 2010 10:31 AM

**To:** Glenn, K. Robert; Schiller, Susannah B.; Brockett, Del  
**Cc:** Glenn, K. Robert  
**Subject:** RE: Updated user "script"

After 1 attempt yesterday and 2 attempts today, I'm still unable to get in touch with 6 out of 17 users (Susannah ?). I plan on trying 1 more time before lunch. At what point can we leave them a voicemail reassuring them that they are not in trouble; but we need to work with them to have their computer sanitized, and let them know we'll send the details in an email?

Rob G.

---

**From:** Glenn, K. Robert  
**Sent:** Thursday, December 02, 2010 3:48 PM  
**To:** Schiller, Susannah B.; Brockett, Del  
**Cc:** Glenn, K. Robert  
**Subject:** Updated user "script"

Attached is the updated script for users. Mostly minor changes (I included a note so you can mention names of the incident response team). If I notice the user is particularly concerned, I will re-assure them that this inadvertent will not result in them getting into any trouble but we do need them to work with the incident response staff to get this resolved quickly.

The list is almost complete (sans 1 or 2 users) and I'll be sending it shortly, sorted by OU.

Rob G.

**Schiller, Susannah B.**

---

**From:** Schiller, Susannah B.  
**Sent:** Friday, December 03, 2010 11:52 AM  
**To:** Glenn, K. Robert; Brockett, Del  
**Subject:** RE: Updated user "script"

(b)(7)(b)(7)  
I hadn't followed up with [REDACTED] but I just tried to call after getting your email, and got his voice mail. I'll try again after lunch.

---

**From:** Glenn, K. Robert  
**Sent:** Friday, December 03, 2010 11:48 AM  
**To:** Schiller, Susannah B.; Brockett, Del  
**Cc:** Glenn, K. Robert  
**Subject:** RE: Updated user "script"

(b)(7)(b)(7) Did you follow-up with [REDACTED] In looking at SIIRT's notes, they had his name as the potential user (but went with [REDACTED] as the highest probability). I really haven't been giving them enough time to guarantee accuracy, particularly as I did not initially let them call people to help track things down. Overall, though it has been much more hit than miss.

We now have the name of one of the missing ones in ITL (tried to call her, but got voicemail), and they are working to track down the last name – and I've told them they can solicit help from within the division.

Rob G.

---

**From:** Schiller, Susannah B.  
**Sent:** Friday, December 03, 2010 11:35 AM  
**To:** Glenn, K. Robert; Brockett, Del  
**Subject:** RE: Updated user "script"

Great, thanks!

---

**From:** Glenn, K. Robert  
**Sent:** Friday, December 03, 2010 11:35 AM  
**To:** Schiller, Susannah B.; Brockett, Del  
**Cc:** Glenn, K. Robert  
**Subject:** RE: Updated user "script"

No need, I ran through the script with him.

Rob G.

---

**From:** Schiller, Susannah B.  
**Sent:** Friday, December 03, 2010 11:34 AM  
**To:** Glenn, K. Robert; Brockett, Del  
**Subject:** RE: Updated user "script"

(b)(7)(b)(7)  
So do you need me to do the wikileaks cal to [REDACTED] or was that part of your conversation?

---

**From:** Glenn, K. Robert  
**Sent:** Friday, December 03, 2010 11:33 AM

**To:** Schiller, Susannah B.; Brockett, Del  
**Cc:** Glenn, K. Robert  
**Subject:** RE: Updated user "script"

We have now tracked down the computer listed for Judy, belonging to a guest researcher, (b)(6) I've asked Yali for a nationality check. I've also called and spoke with (b)(6) and based on the conversation, confirmed he is the correct person for this computer.

Rob G.

---

**From:** Schiller, Susannah B.  
**Sent:** Friday, December 03, 2010 11:01 AM  
**To:** Glenn, K. Robert; Brockett, Del  
**Subject:** RE: Updated user "script"

OK, here's my official count:

3 in Boulder have not been contacted yet (tried once yesterday and once today).

2 in Gaithersburg have not been contacted yet (tried once yesterday and twice today).

The computer listed for Judy Terrill needs to be tracked down -- where it is, who might have used it. Don Koss should be able to help.

My notes are attached (see second page of document)

---

**From:** Glenn, K. Robert  
**Sent:** Friday, December 03, 2010 10:54 AM  
**To:** Brockett, Del; Schiller, Susannah B.  
**Cc:** Glenn, K. Robert  
**Subject:** RE: Updated user "script"

Thanks, Del. (b)(6) has been a more difficult case as he doesn't have voicemail on his phone. I appreciate the update. May have to set an alarm clock to get in touch with him early enough.

Rob G.

---

**From:** Brockett, Del  
**Sent:** Friday, December 03, 2010 10:46 AM  
**To:** Schiller, Susannah B.; Glenn, K. Robert  
**Subject:** RE: Updated user "script"

I just heard back from Rob D.

(b)(6) is working the 11 pm - 7 am shift in the reactor. I am getting confirmation that he will be there tonight.

Del

---

**From:** Schiller, Susannah B.  
**Sent:** Friday, December 03, 2010 10:40 AM  
**To:** Glenn, K. Robert; Brockett, Del  
**Subject:** RE: Updated user "script"

I'm making progress. I've tried everyone in Gburg at least 3 times, and have reached all but 2 of them. I'm getting ready to do second tries for 3 Boulder folks.

DOC has confirmed that WikiLeaks was accessed from a computer registered to you, which may mean classified information was unknowingly accessed. Because access occurred prior to receiving guidance from DOC this is viewed as an unintentional incident. However, NIST is required to treat the computer as though there is classified data resident (i.e., classified information spillage) and, the computer must be appropriately sanitized to ensure that any classified information is removed.

The NIST Office of Information Systems Management (formerly OCIO) incident response team (note: for Gaithersburg, this will be John Antonishek, Matt Loebach, David Kustaborder, Jeff McIntyre, Al Hurst; for Boulder this will be John Beltz or Robert Sorensen) will contact you to schedule sanitization of the computer. Please do not access, read, forward, or otherwise move any WikiLeaks documents that may have been downloaded. Also, please do not attempt to remove any such documents on your own. Sanitization will include removal of the information in your browser cache/history, temporary files, backups that may contain WikiLeaks documentation, etc., and verification that the information was not forwarded via other methods such as email, instant messaging, etc. During the sanitization, every effort will be made to preserve all other user data. Given the number of incidents within NIST, we ask for your patience in scheduling sanitization. Since classified information is involved, the DOC Office of Security (OSY) will also follow up to schedule an inadvertent disclosure briefing.

As a reminder, please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents.

Do you have any questions or concerns?

(b)(2) (b)(6)  
[REDACTED] 634111 [REDACTED]  
Explained it to him. He thinks he went to it because he was reading at a news site.

(b)(2) (b)(6) (b)(6) (b)(6) (b)(6)  
[REDACTED] 851511 [REDACTED] (a fed, x [REDACTED] says  
Hasn't used this computer much; colleague may have - [REDACTED]  
he hasn't used the computer to access the internet at all lately. I spoke to Iosif also and explained.  
He and [REDACTED] will both be taking leave in the next week or two, but he didn't think their leave overlaps, and both have access to the computer.

(b)(2) (b)(6)  
[REDACTED] 612740 [REDACTED]  
Explained it to her.

[REDACTED] 634570 [REDACTED]  
"just poked around - when it asked him to register, he bailed."

(b)(2) (b)(6)  
[REDACTED] 631753 [REDACTED]  
Explained it to him. He cleans up cache every few days, may have already done so, but I instructed him not to do any additional cleanup before the incident response team comes to visit.

(b)(2) (b)(6)  
[REDACTED] 635896 [REDACTED]  
It wasn't her computer. Work with Don Koss to identify where this computer is and who would have used it. She'd like to know what we find out, and also any recommendations for additional policies she should institute to make her computers safer (she's pretty strict with her group).

(b)(2) (b)(6)  
[REDACTED] 634008 [REDACTED]  
Talked to [REDACTED] and explained. He said [REDACTED] is the actual owner of the computer (they aren't good about updating the database, and Darrin brings in computers by the boatload for his division). Called [REDACTED] and explained. He said he just went to the site to see the format of the site and didn't download any documents.

(b)(2) (b)(6)  
[REDACTED] 629074 [REDACTED]  
Didn't download or view. Doesn't understand why we need to do anything to his computer, but said they can "come on over."

(b)(2) (b)(6)  
[REDACTED] 629071 [REDACTED]  
Explained it to him. He didn't go there deliberately - thinks he was looking at CNN.

(b)(2) (b)(6)  
[REDACTED] 624503 [REDACTED]  
Explained it to her. She did ask if management had to know (after I'd already reassured her she didn't do anything wrong), and I told her about Pat's strong advocacy for our employees.

(b)(2) (b)(6)  
[REDACTED] 631298 [REDACTED]  
No contact - tried 4 times.

(b)(2) (b)(6)  
[REDACTED] 851531 [REDACTED]  
Explained it to him. He just looked at a couple of documents.

(b)(2) (b)(6)  
[REDACTED] 933199 [REDACTED]  
No contact - tried 3 times. No voicemail on this number.

(b)(2) (b)(6)  
[REDACTED] 931061 [REDACTED]  
No contact - tried 3 times.

(b)(2) (b)(6)  
[REDACTED] 933751 [REDACTED]  
No contact - tried 3 times.

(b)(2) (b)(6)  
[REDACTED] 940569 [REDACTED]  
Explained it to him.

(b)(2) (b)(6) (Guest Researcher)  
[REDACTED]  
Unix machine - his main lab machine. It is a NIST-owned computer. Asked me to send him an email, which I did.

A couple of computers aren't used by the people listed. Darrin Santay was able to identify the right guy for his, and I've talked to that person and noted it in my spreadsheet that I'll send.

Judy Terrill checked all the boxes in her office and couldn't find the property number, so she asked that we work with Don Koss to identify where the computer is and who might have used it. The relevant property number is 635896 and the IP address is [REDACTED] (b)(2)

After I take another stab at my Boulder folks, I'm all in favor of sending the remaining people the email. Not sure it's even worth leaving voicemail.

---

**From:** Glenn, K. Robert  
**Sent:** Friday, December 03, 2010 10:31 AM  
**To:** Glenn, K. Robert; Schiller, Susannah B.; Brockett, Del  
**Cc:** Glenn, K. Robert  
**Subject:** RE: Updated user "script"

After 1 attempt yesterday and 2 attempts today, I'm still unable to get in touch with 6 out of 17 users (Susannah?). I plan on trying 1 more time before lunch. At what point can we leave them a voicemail reassuring them that they are not in trouble; but we need to work with them to have their computer sanitized, and let them know we'll send the details in an email?

Rob G.

---


**From:** Glenn, K. Robert  
**Sent:** Thursday, December 02, 2010 3:48 PM  
**To:** Schiller, Susannah B.; Brockett, Del  
**Cc:** Glenn, K. Robert  
**Subject:** Updated user "script"

Attached is the updated script for users. Mostly minor changes (I included a note so you can mention names of the incident response team). If I notice the user is particularly concerned, I will re-assure them that this inadvertent will not result in them getting into any trouble but we do need them to work with the incident response staff to get this resolved quickly.

The list is almost complete (sans 1 or 2 users) and I'll be sending it shortly, sorted by OU.

Rob G.





933199  
931061  
933751

631298

(b)(2)

**Antonishek, John K.**

---

**From:** Glenn, K. Robert  
**Sent:** Friday, December 03, 2010 12:07 PM  
**To:** Coalmon, Barbara C.  
**Cc:** siirt; Glenn, K. Robert  
**Subject:** RE: Guidance regarding WikiLeaks

Barbara, I've now reached to the affected CNST user. Here is the additional information.

850223 (b)(2) (b)(6)

It is important that this issue be treated delicately and that this information not spread nor used to embarrass the users and they should continue to be reassured that they will not be getting into any trouble over this as long as they continue to refrain from accessing wikileaks documentation.

SIIRT will be following up to schedule desanitization. OSY will be following up to give them an inadvertent disclosure briefing.

Rob G.

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

**From:** ou\_secur@nist.gov [mailto:ou\_secur@nist.gov] On Behalf Of Glenn, K. Robert  
**Sent:** Friday, December 03, 2010 8:09 AM  
**To:** Multiple recipients of list  
**Subject:** RE: Guidance regarding WikiLeaks

OU ITSOs,

In close consultation with the NIST Director's Office and DoC, we now have a plan to move forward for NIST computers that connected to wikileaks before blocks were implemented. I've included some details and highlights of the plan below; the technical work will be performed by SIIRT (and given that there are 36 computers involved, this could impact other priorities).

1) Notify users verbally that their computer has been identified as having accessed Wikileaks documentation and as a result, may have unknowingly accessed classified information. Users are re-assured that they are not in trouble over this as the access was done prior to DoC guidance being issued. The notification will also explain that over the next several days NIST OISM incident response staff will work with them to properly sanitize their computer. Until the sanitization is complete, users may continue using their computer, but they are not to access, read, or move any Wikileaks documentation downloaded to their computer. Users are also not to try to sanitize their own computers. Users will also be notified that DoC OSY will follow-up with them to provide an inadvertent disclosure briefing. Those with clearances may be asked (by OSY) to take refresher training.

> Status: Susannah and I started contacting users late yesterday afternoon and will try to complete this today.

2) Notify OU Directors and OU ITSOs that have affected computers in their OUs;

> Status: Del started contacting OU Directors late yesterday afternoon. This email is your initial notification. Once all users in your OU have been contacted, I will then send the relevant OU ITSO the list of their affected users/computers.

- 3) SIIRT to complete detailed analysis of network logs to prioritize the order for which computers will be sanitized. Computers that have accessed the site the most or downloaded the most documentation will be sanitized first.
- 4) For each computer to be sanitized SIIRT will schedule time with each user (in prioritized order) to:
  - a) Identify the browser used; for each browser, clear cache, history, temporary files, etc.
  - b) Verify if the user stored any downloaded files elsewhere (e.g., thumb drives, CDs, DVDs, backups, etc.). Verify that nothing was forwarded to other people via other methods such as email, IM, etc..
  - c) Delete all other files and completely erase all unused data sectors on all relevant media and hard disks.
  - d) Sanitize or destroy any mobile media or backup storage used to store Wikileaks documentation.
  - e) Document all steps performed, responses from the user to questions, and any errors that may arise during the procedure.
- 5) Notify DoC OCIO that clean up has been completed and that specific details are available as needed.

=====.

Note, that while the technical steps follow standard operating procedures for classified spillage clean-up, some aspects of the overall procedures (e.g. allowing users to continue using the computer) are only being done due to the massively public nature of the spillage. For more typically spillage incidents, the computer would be immediately removed from the network and sanitization would be immediate. For larger spillages, the hard drive would be removed, labeled, and stored in an approved container until the sanitization could be completed. The plan above was reviewed and approved by the Director's Office.

# of users/computers per OU (for OUs is not listed, there were no computers identified at this time):

OISM: 4 (1 in Boulder)  
OFPM: 2 (both in Boulder)  
TIP: 2  
MEP: 1  
NCNR: 2  
CNST: 1  
MML: 2 (both in Boulder)  
PML: 9 (4 in Boulder)  
EL: 4  
ITL: 9

Rob G.

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

From: allstaff@nist.gov [mailto:allstaff@nist.gov] On Behalf Of NIST IT Assistance Center  
Sent: Wednesday, December 01, 2010 2:45 PM  
To: Multiple recipients of list  
Subject: RE: Guidance regarding WikiLeaks

Attention NIST Staff:

To clarify the guidance that the Department of Commerce issued earlier today we ask that you not use the Commerce contact information provided in that email. Instead, direct any

questions or notifications of access to WikiLeaks documents to the NIST IT Assistance Center (iTAC).

iTAC  
IT Assistance Center  
itac@nist.gov

303-497-5375 (Boulder)  
301-975-5375 (Gaithersburg)

Hours of Operation:

Boulder: 7:30am - 5:30pm (Mountain Time) Monday - Friday  
Gaithersburg: 7:30am - 5:30pm (Eastern Time) Monday - Friday

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

From: allstaff@nist.gov [mailto:allstaff@nist.gov] On Behalf Of Broadcast, DOC  
Sent: Wednesday, December 01, 2010 11:11 AM  
To: Multiple recipients of list  
Subject: Guidance regarding Wikileaks

To: All Commerce Employees and Contractors

Recent reports indicate that a number of government documents have been posted on the WikiLeaks website. These documents may or may not contain information that is considered National Security Information (classified information) and as such, the information is NOT authorized for downloading, viewing, printing, processing, copying, or transmitting via non-classified Government-issued computers, laptops, blackberries, or other communication devices and is not an authorized use of DOC IT equipment. Doing so would introduce potentially classified information onto our unclassified networks and represent a potential security incident.

There has been a rumor that the information is no longer classified since it resides in the public domain. This is NOT true. Executive Order 13526, Section I.1(4)(2) states "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information." The information was neither properly nor improperly "declassified" by the appropriate authority and requires continued classification or reclassification.

Please do not attempt to access any of the Wikileaks documents via the Wikileaks website or through other websites hosting those documents because these documents may contain classified information. Accessing the Wikileaks documents will lead to sanitization of your PC to remove any potentially classified information from the system and result in possible data loss.

If you have questions regarding this broadcast or have accessed the Wikileaks documents, please contact the DOC Computer Incident Response Team at email doc-cirt@doc.gov or call (202) 482-4000.

---

This message was authorized by the Office of Secretary OSY/OCIO.

Please do not reply to this message. The broadcast email account is not monitored for incoming mail.

Please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents because these documents may contain classified information. Accessing the WikiLeaks documents will lead to sanitization of your PC to remove any potentially classified information from the system and result in possible data loss.

If you have questions regarding this broadcast or have accessed the WikiLeaks documents, please contact the DOC Computer Incident Response Team at email [doc-cirt@doc.gov](mailto:doc-cirt@doc.gov) or call (202) 482-4000.

---

This message was authorized by the Office of Secretary OSY/OCIO.

Please do not reply to this message. The broadcast email account is not monitored for incoming mail.

**Antonishek, John K.**

---

**From:** Glenn, K. Robert  
**Sent:** Friday, December 03, 2010 12:09 PM  
**To:** siirt; Sorensen, Robert; Beltz, John  
**Cc:** Glenn, K. Robert  
**Subject:** RE: Guidance regarding WikiLeaks

SIIRT, Robert, & John B, Please make sure you are all on the same page with how the clean up will proceed. As I send these emails (i.e. stating that the user has been contacted), that is your go ahead to proceed with following up with them to schedule sanitization. Please track status on these and send me periodic updates until they are all completed..

Thanks,

Rob G.

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

**From:** Glenn, K. Robert  
**Sent:** Friday, December 03, 2010 11:11 AM  
**To:** Eater, Charles L.  
**Cc:** siirt; Glenn, K. Robert  
**Subject:** RE: Guidance regarding WikiLeaks

Chuck, I've now reached all affected OISM users. Here is the additional information.

934346	[REDACTED]	181
634222	[REDACTED]	181
850752	[REDACTED]	183
631634	[REDACTED]	(b)(6)

It is important that this issue be treated delicately and that this information not spread nor used to embarrass the users and they should continue to be reassured that they will not be getting into any trouble over this as long as they continue to refrain from accessing wikileaks documentation.

SIIRT will be following up to schedule desanitization. OSY will be following up to give them an inadvertent disclosure briefing.

Rob G.

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

**From:** ou\_secur@nist.gov [mailto:ou\_secur@nist.gov] On Behalf Of Glenn, K. Robert  
**Sent:** Friday, December 03, 2010 8:09 AM  
**To:** Multiple recipients of list  
**Subject:** RE: Guidance regarding WikiLeaks

OU ITSOs,

In close consultation with the NIST Director's Office and DoC, we now have a plan to move forward for NIST computers that connected to wikileaks before blocks were implemented. I've included some details and highlights of the plan below; the technical work will be performed by SIIRT (and given that there are 36 computers involved, this could impact other priorities).

1) Notify users verbally that their computer has been identified as having accessed Wikileaks documentation and as a result, may have unknowingly accessed classified information. Users are re-assured that they are not in trouble over this as the access was done prior to DoC guidance being issued. The notification will also explain that over the next several days NIST OISM incident response staff will work with them to properly sanitize their computer. Until the sanitization is complete, users may continue using their computer, but they are not to access, read, or move any Wikileaks documentation downloaded to their computer. Users are also not to try to sanitize their own computers. Users will also be notified that DoC OSY will follow-up with them to provide an inadvertent disclosure briefing. Those with clearances may be asked (by OSY) to take refresher training.

> Status: Susannah and I started contacting users late yesterday afternoon and will try to complete this today.

2) Notify OU Directors and OU ITSOs that have affected computers in their OUs;

> Status: Del started contacting OU Directors late yesterday afternoon. This email is your initial notification. Once all users in your OU have been contacted, I will then send the relevant OU ITSO the list of their affected users/computers.

3) SIIRT to complete detailed analysis of network logs to prioritize the order for which computers will be sanitized. Computers that have accessed the site the most or downloaded the most documentation will be sanitized first.

4) For each computer to be sanitized SIIRT will schedule time with each user (in prioritized order) to:

a) Identify the browser used; for each browser, clear cache, history, temporary files, etc.

b) Verify if the user stored any downloaded files elsewhere (e.g., thumb drives, CDs, DVDs, backups, etc.). Verify that nothing was forwarded to other people via other methods such as email, IM, etc.

c) Delete all other files and completely erase all unused data sectors on all relevant media and hard disks.

d) Sanitize or destroy any mobile media or backup storage used to store Wikileaks documentation.

e) Document all steps performed, responses from the user to questions, and any errors that may arise during the procedure.

5) Notify DoC OCIO that clean up has been completed and that specific details are available as needed.

=====

Note, that while the technical steps follow standard operating procedures for classified spillage clean-up, some aspects of the overall procedures (e.g. allowing users to continue using the computer) are only being done due to the massively public nature of the spillage. For more typically spillage incidents, the computer would be immediately removed from the network and sanitization would be immediate. For larger spillages, the hard drive would be removed, labeled, and stored in an approved container until the sanitization could be completed. The plan above was reviewed and approved by the Director's Office.

# of users/computers per OU (for OUs is not listed, there were no computers identified at this time):

OISM: 4 (1 in Boulder)  
OFPM: 2 (both in Boulder)  
TIP: 2  
MEP: 1  
NCNR: 2

CNST: 1  
MML: 2 (both in Boulder)  
PML: 9 (4 in Boulder)  
EL: 4  
ITL: 9

Rob G.

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

From: allstaff@nist.gov [mailto:allstaff@nist.gov] On Behalf Of NIST IT Assistance Center  
Sent: Wednesday, December 01, 2010 2:45 PM  
To: Multiple recipients of list  
Subject: RE: Guidance regarding Wikileaks

Attention NIST Staff:

To clarify the guidance that the Department of Commerce issued earlier today we ask that you not use the Commerce contact information provided in that email. Instead, direct any questions or notifications of access to WikiLeaks documents to the NIST IT Assistance Center (iTAC).

iTAC  
IT Assistance Center  
itac@nist.gov

303-497-5375 (Boulder)  
301-975-5375 (Gaithersburg)

Hours of Operation:

Boulder: 7:30am - 5:30pm (Mountain Time) Monday - Friday  
Gaithersburg: 7:30am - 5:30pm (Eastern Time) Monday - Friday

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

From: allstaff@nist.gov [mailto:allstaff@nist.gov] On Behalf Of Broadcast, DOC  
Sent: Wednesday, December 01, 2010 11:11 AM  
To: Multiple recipients of list  
Subject: Guidance regarding Wikileaks

To: All Commerce Employees and Contractors

Recent reports indicate that a number of government documents have been posted on the Wikileaks website. These documents may or may not contain information that is considered National Security Information (classified information) and as such, the information is NOT authorized for downloading, viewing, printing, processing, copying, or transmitting via non-classified Government-issued computers, laptops, blackberries, or other communication devices and is not an authorized use of DOC IT equipment. Doing so would introduce potentially classified information onto our unclassified networks and represent a potential security incident.

There has been a rumor that the information is no longer classified since it resides in the public domain. This is NOT true. Executive Order 13526, Section I.1(4)(2) states "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information." The information was neither properly nor improperly "declassified" by the appropriate authority and requires continued classification or reclassification.



Please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents because these documents may contain classified information. Accessing the WikiLeaks documents will lead to sanitization of your PC to remove any potentially classified information from the system and result in possible data loss.

If you have questions regarding this broadcast or have accessed the WikiLeaks documents, please contact the DOC Computer Incident Response Team at email [doc-cirt@doc.gov](mailto:doc-cirt@doc.gov) or call (202) 482-4000.

---

This message was authorized by the Office of Secretary OSY/OCIO.

Please do not reply to this message. The broadcast email account is not monitored for incoming mail.

**Subject:** RE: Guidance regarding WikiLeaks  
**From:** "Glenn, K. Robert" <robert.glenn@nist.gov>  
**Date:** Fri, 3 Dec 2010 12:12:47 -0500  
**To:** "Rowland, Carolyn D." <carolyn.rowland@nist.gov>  
**CC:** siirt <siirt@nist.gov>, "Glenn, K. Robert" <robert.glenn@nist.gov>

Carolyn, Susannah has now contacted all affected EL users. Here is the additional information.

612740  
634570  
851531  
631753

(b)(2)  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted] (b)(6)

It is important that this issue be treated delicately and that this information not spread nor used to embarrass the users and they should continue to be reassured that they will not be getting into any trouble over this as long as they continue to refrain from accessing wikileaks documentation.

SIIRT will be following up to schedule desanitization. OSY will be following up to give them an inadvertent disclosure briefing.

Rob G.

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

From: [ou\\_secur@nist.gov](mailto:ou_secur@nist.gov) [mailto:[ou\\_secur@nist.gov](mailto:ou_secur@nist.gov)] On Behalf Of Glenn, K. Robert  
Sent: Friday, December 03, 2010 8:09 AM  
To: Multiple recipients of list  
Subject: RE: Guidance regarding WikiLeaks

OU ITSOs,

In close consultation with the NIST Director's Office and DoC, we now have a plan to move forward for NIST computers that connected to wikileaks before blocks were implemented. I've included some details and highlights of the plan below; the technical work will be performed by SIIRT (and given that there are 36 computers involved, this could impact other priorities).

1) Notify users verbally that their computer has been identified as having accessed Wikileaks documentation and as a result, may have unknowingly accessed classified information. Users are re-assured that they are not in trouble over this as the access was done prior to DoC guidance being issued. The notification will also explain that over the next several days NIST OISM incident response staff will work with them to properly sanitize their computer. Until the sanitization is complete, users may continue using their computer, but they are not to access, read, or move any Wikileaks documentation downloaded to their computer. Users are also not to try to sanitize their own computers. Users will also be notified that DoC OSY will follow-up with them to provide a inadvertent disclosure briefing. Those with clearances may be asked (by OSY) to take refresher training.

> Status: Susannah and I started contacting users late yesterday afternoon and will try to complete this today.

2) Notify OU Directors and OU ITSOs that have affected computers in their OUs;

> Status: Del started contacting OU Directors late yesterday afternoon. This email is your initial notification. Once all users in your OU have been contacted, I will then send the relevant OU ITSO the list of their affected users/computers.

RE: Guidance regarding WikiLeaks

- 3) SIIRT to complete detailed analysis of network logs to prioritize the order for which computers will be sanitized. Computers that have accessed the site the most or downloaded the most documentation will be sanitized first.
- 4) For each computer to be sanitized SIIRT will schedule time with each user (in prioritized order) to:
  - a) Identify the browser used; for each browser, clear cache, history, temporary files, etc.
  - b) Verify if the user stored any downloaded files elsewhere (e.g., thumb drives, CDs, DVDs, backups, etc.). Verify that nothing was forwarded to other people via other methods such as email, IM, etc.
  - c) Delete all other files and completely erase all unused data sectors on all relevant media and hard disks.
  - d) Sanitize or destroy any mobile media or backup storage used to store Wikileaks documentation.
  - e) Document all steps performed, responses from the user to questions, and any errors that may arise during the procedure.
- 5) Notify DoC OClO that clean up has been completed and that specific details are available as needed.

=====

Note, that while the technical steps follow standard operating procedures for classified spillage clean-up, some aspects of the overall procedures (e.g. allowing users to continue using the computer) are only being done due to the massively public nature of the spillage. For more typically spillage incidents, the computer would be immediately removed from the network and sanitization would be immediate. For larger spillages, the hard drive would be removed, labeled, and stored in an approved container until the sanitization could be completed. The plan above was reviewed and approved by the Director's Office.

# of users/computers per OU (for OUs is not listed, there were no computers identified at this time):

OISM: 4 (1 in Boulder)  
OFPM: 2 (both in Boulder)  
TIP: 2  
MEP: 1  
NCNR: 2  
CNST: 1  
MML: 2 (both in Boulder)  
PML: 9 (4 in Boulder)  
EL: 4  
ITL: 9

Rob G.

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

From: [allstaff@nist.gov](mailto:allstaff@nist.gov) [<mailto:allstaff@nist.gov>] On Behalf Of NIST IT Assistance Center

Sent: Wednesday, December 01, 2010 2:45 PM

To: Multiple recipients of list

Subject: RE: Guidance regarding WikiLeaks

Attention NIST Staff:

To clarify the guidance that the Department of Commerce issued earlier today we ask that you not use the Commerce contact information provided in that email. Instead, direct any questions or notifications of access to WikiLeaks documents to the NIST IT Assistance Center (iTAC).

iTAC  
IT Assistance Center

[itac@nist.gov](mailto:itac@nist.gov)

303-497-5375 (Boulder)  
301-975-5375 (Gaithersburg)

Hours of Operation:

Boulder: 7:30am - 5:30pm (Mountain Time) Monday - Friday

Gaithersburg: 7:30am - 5:30pm (Eastern Time) Monday - Friday

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

From: [allstaff@nist.gov](mailto:allstaff@nist.gov) [mailto:[allstaff@nist.gov](mailto:allstaff@nist.gov)] On Behalf Of Broadcast, DOC  
Sent: Wednesday, December 01, 2010 11:11 AM  
To: Multiple recipients of list  
Subject: Guidance regarding WikiLeaks

To: All Commerce Employees and Contractors

Recent reports indicate that a number of government documents have been posted on the WikiLeaks website. These documents may or may not contain information that is considered National Security Information (classified information) and as such, the information is NOT authorized for downloading, viewing, printing, processing, copying, or transmitting via non-classified Government-issued computers, laptops, blackberries, or other communication devices and is not an authorized use of DOC IT equipment. Doing so would introduce potentially classified information onto our unclassified networks and represent a potential security incident.

There has been a rumor that the information is no longer classified since it resides in the public domain. This is NOT true. Executive Order 13526, Section I.1(4)(2) states "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information." The information was neither properly nor improperly "declassified" by the appropriate authority and requires continued classification or reclassification.

Please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents because these documents may contain classified information. Accessing the WikiLeaks documents will lead to sanitization of your PC to remove any potentially classified information from the system and result in possible data loss.

If you have questions regarding this broadcast or have accessed the WikiLeaks documents, please contact the DOC Computer Incident Response Team at email [doc-cirt@doc.gov](mailto:doc-cirt@doc.gov) or call (202) 482-4000.

---

This message was authorized by the Office of Secretary OSY/OCIO.

Please do not reply to this message. The broadcast email account is not monitored for incoming mail.

**McIntyre, Jeffrey J.**

---

**From:** Hurst V, Alfred Coulter  
**Sent:** Friday, December 03, 2010 2:16 PM  
**To:** McIntyre, Jeffrey J.  
**Subject:** FW: wiki  
**Attachments:** wiki\_sources(with\_users).xls

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

**From:** David Kustaborder [<mailto:kusty@nist.gov>]  
**Sent:** ~~Thursday, December 02, 2010 1:33 PM~~  
**To:** Loebach, Matthew T.; Hurst V, Alfred Coulter  
**Subject:** wiki

Sheet1

Property Number	src	count	percent	NNIS Primary User	Property User	LANDesk User	Division
634024	(b)(2)	29	10.320285	(b)(6)	(b)(6)		774
631634	(b)(2)	26	9.252669	(b)(6)	(b)(6)		184
	(b)(2)	18	6.405694	(b)(6)	(b)(6)	Data not filled in	
629071	(b)(2)	17	6.049822	(b)(6)	(b)(6)		774
931061	(b)(2)	16	5.693950	(b)(6)	(b)(6)		688
624503	(b)(2)	14	4.982206	(b)(6)	(b)(6)		775
934346	(b)(2)	10	3.558719	(b)(6)	(b)(6)		181
631753	(b)(2)	10	3.558719	(b)(6)	(b)(6)		732
634008	(b)(2)	10	3.558719	(b)(6)	(b)(6)		772
851531	(b)(2)	10	3.558719	(b)(6)	(b)(6)		731
940819	(b)(2)	9	3.202847	(b)(6)	(b)(6)		194
850752	(b)(2)	9	3.202847	(b)(6)	(b)(6)		183
612740	(b)(2)	9	3.202847	(b)(6)	(b)(6)		730
933199	(b)(2)	8	2.846975	(b)(6)	(b)(6)		687
851068	(b)(2)	6	2.135231	(b)(6)	(b)(6)		653
Prop filled in as XXX	(b)(2)	6	2.135231	(b)(6)	(b)(6)		191
623254	(b)(2)	6	2.135231	(b)(6)	(b)(6)		683
629074	(b)(2)	6	2.135231	(b)(6)	(b)(6)		773
621855	(b)(2)	6	2.135231	(b)(6)	(b)(6)		488
940569	(b)(2)	5	1.779359	(b)(6)	(b)(6)		697
624101	(b)(2)	5	1.779359	(b)(6)	(b)(6)		610
631298	(b)(2)	4	1.423488	(b)(6)	(b)(6)		775
617030	(b)(2)	4	1.423488	(b)(6)	(b)(6)		683
633663	(b)(2)	4	1.423488	(b)(6)	(b)(6)		470
633683	(b)(2)	4	1.423488	(b)(6)	(b)(6)		470
612061	(b)(2)	4	1.423488	(b)(6)	(b)(6)		682
930364	(b)(2)	3	1.067616	(b)(6)	(b)(6)		638
933751	(b)(2)	3	1.067616	(b)(6)	(b)(6)		688
634222	(b)(2)	3	1.067616	(b)(6)	(b)(6)		181
635896	(b)(2)	3	1.067616	(b)(6)	(b)(6)		771
851511	(b)(2)	3	1.067616	(b)(6)	(b)(6)		836
634111	(b)(2)	3	1.067616	(b)(6)	(b)(6)		840
635565	(b)(2)	3	1.067616	(b)(6)	(b)(6)		610
850223	(b)(2)	2	0.711744	(b)(6)	(b)(6)		620
634570	(b)(2)	2	0.711744	(b)(6)	(b)(6)		730
	(b)(2)	1	0.355872	(b)(6)	(b)(6)		

IISC Info

[REDACTED] (b)(6)

(b)(6)  
Was [REDACTED] Desktop computer, now [REDACTED] has it

[REDACTED] (b)(2)

First person

**Subject:** First person

**From:** "Hurst V, Alfred Coulter" <alfred.hurst@nist.gov>

**Date:** Fri, 3 Dec 2010 15:06:12 -0500

**To:** "Kustaborder, David P." <david.kustaborder@nist.gov>

(b)(6) (b)(7)(C) (Gaithersburg) [REDACTED]@nist.gov

name: [REDACTED] (Gaithersburg)

phone: (301) 975 [REDACTED]

depart: Information Access Division (774)

office: [REDACTED]

agency: [REDACTED] (b)(2)

address: 100 Bureau Drive, Stop 8940

: Gaithersburg, MD 20899-8940

email: [REDACTED]@nist.gov

alternate email: [REDACTED]@nist.gov

: [REDACTED]@nist.gov

Last Updated: Fri Dec 3 2:45:02 2010

(b)(6)



Subject: RE: Guidance regarding WikiLeaks  
From: "Glenn, K. Robert" <robert.glenn@nist.gov>  
Date: Fri, 3 Dec 2010 15:09:36 -0500  
To: "Eater, Charles L." <ceater@nist.gov>  
CC: "Glenn, K. Robert" <robert.glenn@nist.gov>

Chuck, that is correct. This was provided simply as an FYI.

Rob G.

---

From: Charles L. Eater [mailto:ceater@nist.gov]  
Sent: Friday, December 03, 2010 2:58 PM  
To: Glenn, K. Robert  
Subject: Re: Guidance regarding WikiLeaks

Rob,

Since you say you've contacted these people, am I correct in assuming that you've already told them that SIIRT and OSY will be following up with them?

Chuck

— Glenn, K. Robert wrote the following at 12/3/2010 11:11 AM:  
Chuck, I've now reached all affected OISM users. Here is the additional information.

934346  
634222  
850752  
631634

It is important that this issue be treated delicately and that this information not spread nor used to embarrass the users and they should continue to be reassured that they will not be getting into any  
SIIRT will be following up to schedule desanization. OSY will be following up to give them an inadvertent disclosure briefing.

Rob G.

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

From: [ou\\_secur@nist.gov](mailto:ou_secur@nist.gov) [mailto:[ou\\_secur@nist.gov](mailto:ou_secur@nist.gov)] On Behalf Of Glenn, K. Robert  
Sent: Friday, December 03, 2010 8:09 AM  
To: Multiple recipients of list  
Subject: RE: Guidance regarding WikiLeaks

OU ITSOs,

In close consultation with the NIST Director's Office and DoC, we now have a plan to move forward for NIST computers that connected to wikileaks before blocks were implemented. I've included s

1) Notify users verbally that their computer has been identified as having accessed Wikileaks documentation and as a result, may have unknowingly accessed classified information. Users are re-ass

> Status: Susannah and I started contacting users late yesterday afternoon and will try to complete this today.

2) Notify OU Directors and OU ITSOs that have affected computers in their OUs;

> Status: Del started contacting OU Directors late yesterday afternoon. This email is your initial notification. Once all users in your OU have been contacted, I will then send the relevant OU ITSO

3) SIIRT to complete detailed analysis of network logs to prioritize the order for which computers will be sanitized. Computers that have accessed the site the most or downloaded the most docu

4) For each computer to be sanitized SIIRT will schedule time with each user (in prioritized order) to:

- a) Identify the browser used; for each browser, clear cache, history, temporary files, etc.
  - b) Verify if the user stored any downloaded files elsewhere (e.g., thumb drives, CDs, DVDs, backups, etc.). Verify that nothing was forwarded to other people via other methods such as er
  - c) Delete all other files and completely erase all unused data sectors on all relevant media and hard disks.
  - d) Sanitize or destroy any mobile media or backup storage used to store Wikileaks documentation.
  - e) Document all steps performed, responses from the user to questions, and any errors that may arise during the procedure.
- 5) Notify DoC OCIO that clean up has been completed and that specific details are available as needed.

=====  
Note, that while the technical steps follow standard operating procedures for classified spillage clean-up, some aspects of the overall procedures (e.g. allowing users to continue using the computer)

# of users/computers per OU (for OUs not listed, there were no computers identified at this time):

OISM: 4 (1 in Boulder)  
OFPM: 2 (both in Boulder)  
TIP: 2  
MEP: 1  
NCNR: 2  
CNST: 1  
MML: 2 (both in Boulder)  
PML: 9 (4 in Boulder)  
EL: 4  
ITL: 9

Rob G.

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

From: [allstaff@nist.gov](mailto:allstaff@nist.gov) [mailto:[allstaff@nist.gov](mailto:allstaff@nist.gov)] On Behalf Of NIST IT Assistance Center  
Sent: Wednesday, December 01, 2010 2:45 PM  
To: Multiple recipients of list  
Subject: RE: Guidance regarding WikiLeaks

Attention NIST Staff:

To clarify the guidance that the Department of Commerce issued earlier today we ask that you not use the Commerce contact information provided in that email. Instead, direct any questions or not

## TE: Guidance regarding WikiLeaks

ITAC  
IT Assistance Center  
[itac@nist.gov](mailto:itac@nist.gov)

303-497-5375 (Boulder)  
301-975-5375 (Gaithersburg)

### Hours of Operation:

Boulder: 7:30am - 5:30pm (Mountain Time) Monday - Friday  
Gaithersburg: 7:30am - 5:30pm (Eastern Time) Monday - Friday

### -----Original Message-----

From: [allstaff@nist.gov](mailto:allstaff@nist.gov) (<mailto:allstaff@nist.gov>) On Behalf Of Broadcast, DOC  
Sent: Wednesday, December 01, 2010 11:11 AM  
To: Multiple recipients of list  
Subject: Guidance regarding WikiLeaks

To: All Commerce Employees and Contractors

Recent reports indicate that a number of government documents have been posted on the WikiLeaks website. These documents may or may not contain information that is considered National Security Information.

There has been a rumor that the information is no longer classified since it resides in the public domain. This is NOT true. Executive Order 13526, Section 1.1(4)(2) states "Classified Information shall remain classified regardless of the medium in which it is stored."

Please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents because these documents may contain classified information.

If you have questions regarding this broadcast or have accessed the WikiLeaks documents, please contact the DOC Computer Incident Response Team at email [doc-cirt@doc.gov](mailto:doc-cirt@doc.gov) or call (202) 482-2800.

---

This message was authorized by the Office of Secretary OSY/OCIO.

Please do not reply to this message. The broadcast email account is not monitored for incoming mail.

Re: Guidance regarding WikiLeaks

**Subject:** Re: Guidance regarding WikiLeaks  
**From:** David Kustaborder <kusty@nist.gov>  
**Date:** Fri, 3 Dec 2010 15:15:56 -0500  
**To:** "Glenn, K. Robert" <robert.glenn@nist.gov>

I just spoke to Larry Keys on the phone. He is actually off today. I explained the discreteness of the situation. He can have a username Monday morning if that is ok with you.

This is for [REDACTED] (b)(2)

-kusty

On 12/03/2010 12:12 PM, Glenn, K. Robert wrote:

Carolyn, Susannah has now contacted all affected EL users. Here is the additional information.

612740  
634570  
851531  
631753

[REDACTED] (b)(2)  
[REDACTED] (b)(2)  
It is important that this issue be treated delicately and that this information not spread nor used to embarrass the users and they should continue to be reassured that they will not be getting into any trouble over this as long as they continue to refrain from accessing wikileaks documentation.

SIIRT will be following up to schedule desanitization. OSY will be following up to give them an inadvertent disclosure briefing.

Rob G.

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

From: [ou\\_secur@nist.gov](mailto:ou_secur@nist.gov) [mailto:[ou\\_secur@nist.gov](mailto:ou_secur@nist.gov)] On Behalf Of Glenn, K. Robert  
Sent: Friday, December 03, 2010 8:09 AM  
To: Multiple recipients of list  
Subject: RE: Guidance regarding WikiLeaks

OU ITSOs,

In close consultation with the NIST Director's Office and DoC, we now have a plan to move forward for NIST computers that connected to wikileaks before blocks were implemented. I've included some details and highlights of the plan below; the technical work will be performed by SIIRT (and given that there are 36 computers involved, this could impact other priorities).

1) Notify users verbally that their computer has been identified as having accessed Wikileaks documentation and as a result, may have unknowingly accessed classified information. Users are re-assured that they are not in trouble over this as the access was done prior to DoC guidance being issued. The notification will also explain that over the next several days NIST OISM incident response staff will work with them to properly sanitize their computer. Until the sanitization is complete, users may continue using their computer, but they are not to access, read, or move any Wikileaks documentation downloaded to their computer. Users are also not to try to sanitize their own computers. Users will also be notified that DoC OSY will follow-up

with them to provide a inadvertent disclosure briefing. Those with clearances may be asked (by OSY) to take refresher training.

> Status: Susannah and I started contacting users late yesterday afternoon and will try to complete this today.

2) Notify OU Directors and OU ITSOs that have affected computers in their OUs;

> Status: Del started contacting OU Directors late yesterday afternoon. This email is your initial notification. Once all users in your OU have been contacted, I will then send the relevant OU ITSO the list of their affected users/computers.

3) SIIRT to complete detailed analysis of network logs to prioritize the order for which computers will be sanitized. Computers that have accessed the site the most or downloaded the most documentation will be sanitized first.

4) For each computer to be sanitized SIIRT will schedule time with each user (in prioritized order) to:

a) Identify the browser used; for each browser, clear cache, history, temporary files, etc.

b) Verify if the user stored any downloaded files elsewhere (e.g., thumb drives, CDs, DVDs, backups, etc.). Verify that nothing was forwarded to other people via other methods such as email, IM, etc.

c) Delete all other files and completely erase all unused data sectors on all relevant media and hard disks.

d) Sanitize or destroy any mobile media or backup storage used to store Wikileaks documentation.

e) Document all steps performed, responses from the user to questions, and any errors that may arise during the procedure.

5) Notify DoC OCIO that clean up has been completed and that specific details are available as needed.

---

Note, that while the technical steps follow standard operating procedures for classified spillage clean-up, some aspects of the overall procedures (e.g. allowing users to continue using the computer) are only being done due to the massively public nature of the spillage. For more typically spillage incidents, the computer would be immediately removed from the network and sanitization would be immediate. For larger spillages, the hard drive would be removed, labeled, and stored in an approved container until the sanitization could be completed. The plan above was reviewed and approved by the Director's Office.

# of users/computers per OU (for OUs is not listed, there were no computers identified at this time):

OISM: 4 (1 in Boulder)

OFPM: 2 (both in Boulder)

TIP: 2

MEP: 1

NCNR: 2

CNST: 1

MML: 2 (both in Boulder)

PML: 9 (4 in Boulder)

EL: 4

ITL: 9

Rob G.

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

From: [allstaff@nist.gov](mailto:allstaff@nist.gov) [mailto:[allstaff@nist.gov](mailto:allstaff@nist.gov)] On Behalf Of NIST IT Assistance Center

Sent: Wednesday, December 01, 2010 2:45 PM

To: Multiple recipients of list

Subject: RE: Guidance regarding WikiLeaks

Attention NIST Staff:

To clarify the guidance that the Department of Commerce issued earlier today we ask that you not use the Commerce contact information provided in that email. Instead, direct any questions or notifications of access to WikiLeaks documents to the NIST IT Assistance Center (iTAC).

iTAC

IT Assistance Center

[itac@nist.gov](mailto:itac@nist.gov)

303-497-5375 (Boulder)

301-975-5375 (Gaithersburg)

Hours of Operation:

Boulder: 7:30am - 5:30pm (Mountain Time) Monday - Friday

Gaithersburg: 7:30am - 5:30pm (Eastern Time) Monday - Friday

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

From: [allstaff@nist.gov](mailto:allstaff@nist.gov) [mailto:[allstaff@nist.gov](mailto:allstaff@nist.gov)] On Behalf Of Broadcast, DOC

Sent: Wednesday, December 01, 2010 11:11 AM

To: Multiple recipients of list

Subject: Guidance regarding WikiLeaks

To: All Commerce Employees and Contractors

Recent reports indicate that a number of government documents have been posted on the WikiLeaks website. These documents may or may not contain information that is considered National Security Information (classified information) and as such, the information is NOT authorized for downloading, viewing, printing, processing, copying, or transmitting via non-classified Government-issued computers, laptops, blackberries, or other communication devices and is not an authorized use of DOC IT equipment. Doing so would introduce potentially classified information onto our unclassified networks and represent a potential security incident.

There has been a rumor that the information is no longer classified since it resides in the public domain. This is NOT true. Executive Order 13526, Section I.1(4)(2) states "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information." The information was neither properly nor improperly "declassified" by the appropriate authority and requires continued classification or reclassification.

Please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents because these documents may contain classified information. Accessing the WikiLeaks documents will lead to sanitization of your PC to remove any potentially classified information from the system and result in possible data loss.

Re: Guidance regarding WikiLeaks

If you have questions regarding this broadcast or have accessed the WikiLeaks documents, please contact the DOC Computer Incident Response Team at email [doc-cirt@doc.gov](mailto:doc-cirt@doc.gov) or call (202) 482-4000.

---

This message was authorized by the Office of Secretary OSY/OCIO.

Please do not reply to this message. The broadcast email account is not monitored for incoming mail.

**Antonishek, John K.**

---

**From:** Glenn, K. Robert  
**Sent:** Friday, December 03, 2010 3:22 PM  
**To:** Kustaborder, David P.  
**Cc:** siirt; Glenn, K. Robert  
**Subject:** RE: Wiki Contact.

David, I'm confused. What do you mean you started the sanitization process (i.e. I don't believe I sent an email for cleaning ITL computers yet)?

Any word on the CSD computer?

Rob G.

---

**From:** David Kustaborder [mailto:kusty@nist.gov]  
**Sent:** Friday, December 03, 2010 3:14 PM  
**To:** Glenn, K. Robert; siirt  
**Subject:** Wiki Contact.

FYI,

We had a contact wrong on the wiki list. We did start the sanitization process, but do you want to make the phone call to him?

629071 [REDACTED]

774

4262

(b)(6)

Contact should be the guest researcher listed below.

[REDACTED] (Gaithersburg) [REDACTED]@nist.gov

name: [REDACTED] (Gaithersburg)  
phone: (301) 975-[REDACTED] (b)(6)  
depart: Information Access Division (774)  
office: [REDACTED] (b)(2)  
agency: [REDACTED]  
address: 100 Bureau Drive, Stop 8940  
: Gaithersburg, MD 20899-8940  
email: [REDACTED]@nist.gov  
alternate email: [REDACTED]@nist.gov  
: [REDACTED]@nist.gov  
Last Updated: Fri Dec 3 2:45:02 2010

(b)(6)

**Subject:** 129.6.54.14

**From:** David Kustaborder <kusty@nist.gov>

**Date:** Mon, 6 Dec 2010 09:03:44 -0500

**To:** "Glenn, K. Robert" <robert.glenn@nist.gov>

User of system is a Guest Researcher.

(b)(6)  
[REDACTED] (Gaithersburg) - [REDACTED]@nist.gov

name: [REDACTED] (Gaithersburg)

phone: (301) 975- [REDACTED] (b)(6)

depart: Computer Security Division (773)

office: [REDACTED] (b)(2)

agency:

(b)(6) address: 100 Bureau Drive, Stop 8930

: Gaithersburg, MD 20899-8930

email: [REDACTED]@nist.gov

alternate email: [REDACTED]@nist.gov

Last Updated: Fri Dec 3 2:45:02 2010

(b)(6)  
[Is Your Directory Information Incorrect?](#) | [DoC Directory](#)



**Loebach, Matthew T.**

---

**From:** Glenn, K. Robert  
**Sent:** Monday, December 06, 2010 11:57 AM  
**To:** McKay, Richard; Zheng, Kathy; Swicegood, David J.  
**Cc:** siirt; Sorensen, Robert; Beltz, John; Glenn, K. Robert  
**Subject:** RE: Guidance regarding WikiLeaks

Rich, Kathy, & David,

Both OFPM users have been contacted. Note those labeled as (email) means that I was only able to reach them via email and do not have confirmation that they read the message. All others were contacted verbally. Here is the additional information.

Prop filled in as XXX (b)(2) (b)(7)(D) 191  
940819 (b)(2) 194 (email)

It is important that this issue be treated delicately and that this information not spread nor used to embarrass the users and they should continue to be reassured that they will not be getting into any trouble over this as long as they continue to refrain from accessing wikileaks documentation.

SIIRT will be following up to schedule desanitization. OSY will be following up to give them an inadvertent disclosure briefing.

Rob G.

PS - it appears that there may be a LANDesk discrepancy with (b)(6) desktop.

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

**From:** ou\_secu@nist.gov [mailto:ou\_secu@nist.gov] On Behalf Of Glenn, K. Robert  
**Sent:** Friday, December 03, 2010 8:09 AM  
**To:** Multiple recipients of list  
**Subject:** RE: Guidance regarding WikiLeaks

OU ITSOs,

In close consultation with the NIST Director's Office and DoC, we now have a plan to move forward for NIST computers that connected to wikileaks before blocks were implemented. I've included some details and highlights of the plan below; the technical work will be performed by SIIRT (and given that there are 36 computers involved, this could impact other priorities).

1) Notify users verbally that their computer has been identified as having accessed Wikileaks documentation and as a result, may have unknowingly accessed classified information. Users are re-assured that they are not in trouble over this as the access was done prior to DoC guidance being issued. The notification will also explain that over the next several days NIST OISM incident response staff will work with them to properly sanitize their computer. Until the sanitization is complete, users may continue using their computer, but they are not to access, read, or move any Wikileaks documentation downloaded to their computer. Users are also not to try to sanitize their own computers. Users will also be notified that DoC OSY will follow-up with them to provide an inadvertent disclosure briefing. Those with clearances may be asked (by OSY) to take refresher training.

> Status: Susannah and I started contacting users late yesterday afternoon and will try to complete this today.

2) Notify OU Directors and OU ITSOs that have affected computers in their OUs;

> Status: Del started contacting OU Directors late yesterday afternoon. This email is your initial notification. Once all users in your OU have been contacted, I will then send the relevant OU ITSO the list of their affected users/computers.

3) SIIRT to complete detailed analysis of network logs to prioritize the order for which computers will be sanitized. Computers that have accessed the site the most or downloaded the most documentation will be sanitized first.

4) For each computer to be sanitized SIIRT will schedule time with each user (in prioritized order) to:

a) Identify the browser used; for each browser, clear cache, history, temporary files, etc.

b) Verify if the user stored any downloaded files elsewhere (e.g., thumb drives, CDs, DVDs, backups, etc.). Verify that nothing was forwarded to other people via other methods such as email, IM, etc.

c) Delete all other files and completely erase all unused data sectors on all relevant media and hard disks.

d) Sanitize or destroy any mobile media or backup storage used to store Wikileaks documentation.

e) Document all steps performed, responses from the user to questions, and any errors that may arise during the procedure.

5) Notify DoC OCIO that clean up has been completed and that specific details are available as needed.

=====

Note, that while the technical steps follow standard operating procedures for classified spillage clean-up, some aspects of the overall procedures (e.g. allowing users to continue using the computer) are only being done due to the massively public nature of the spillage. For more typically spillage incidents, the computer would be immediately removed from the network and sanitization would be immediate. For larger spillages, the hard drive would be removed, labeled, and stored in an approved container until the sanitization could be completed. The plan above was reviewed and approved by the Director's Office.

# of users/computers per OU (for OUs is not listed, there were no computers identified at this time):

OISM: 4 (1 in Boulder)

OFPM: 2 (both in Boulder)

TIP: 2

MEP: 1

NCNR: 2

CNST: 1

MML: 2 (both in Boulder)

PML: 9 (4 in Boulder)

EL: 4

ITL: 9

Rob G.

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

From: allstaff@nist.gov [mailto:allstaff@nist.gov] On Behalf Of NIST IT Assistance Center

Sent: Wednesday, December 01, 2010 2:45 PM

To: Multiple recipients of list

Subject: RE: Guidance regarding Wikileaks

Attention NIST Staff:

To clarify the guidance that the Department of Commerce issued earlier today we ask that you not use the Commerce contact information provided in that email. Instead, direct any questions or notifications of access to WikiLeaks documents to the NIST IT Assistance Center (iTAC).

iTAC  
IT Assistance Center  
itac@nist.gov

303-497-5375 (Boulder)  
301-975-5375 (Gaithersburg)

Hours of Operation:

Boulder: 7:30am - 5:30pm (Mountain Time) Monday - Friday  
Gaithersburg: 7:30am - 5:30pm (Eastern Time) Monday - Friday

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

From: allstaff@nist.gov [mailto:allstaff@nist.gov] On Behalf Of Broadcast, DOC  
Sent: Wednesday, December 01, 2010 11:11 AM  
To: Multiple recipients of list  
Subject: Guidance regarding WikiLeaks

To: All Commerce Employees and Contractors

Recent reports indicate that a number of government documents have been posted on the WikiLeaks website. These documents may or may not contain information that is considered National Security Information (classified information) and as such, the information is NOT authorized for downloading, viewing, printing, processing, copying, or transmitting via non-classified Government-issued computers, laptops, blackberries, or other communication devices and is not an authorized use of DOC IT equipment. Doing so would introduce potentially classified information onto our unclassified networks and represent a potential security incident.

There has been a rumor that the information is no longer classified since it resides in the public domain. This is NOT true. Executive Order 13526, Section I.1(4)(2) states "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information." The information was neither properly nor improperly "declassified" by the appropriate authority and requires continued classification or reclassification.

Please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents because these documents may contain classified information. Accessing the WikiLeaks documents will lead to sanitization of your PC to remove any potentially classified information from the system and result in possible data loss.

If you have questions regarding this broadcast or have accessed the WikiLeaks documents, please contact the DOC Computer Incident Response Team at email doc-cirt@doc.gov or call (202) 482-4000.

---

This message was authorized by the Office of Secretary OSY/OCIO.

Please do not reply to this message. The broadcast email account is not monitored for incoming mail.

Loebach, Matthew T.

---

From: Glenn, K. Robert  
Sent: Monday, December 06, 2010 12:04 PM  
To: Klosowski, Przemek  
Cc: siirt; Glenn, K. Robert  
Subject: RE: Guidance regarding WikiLeaks

Przemek,

Both NCNR users have been contacted. Note those labeled as (email) means that I was only able to reach them via email and do not have confirmation that they read the message. All others were contacted verbally. Here is the additional information.

624101 (b)(7) 610  
635565 (b)(7) 610 (email)

It is important that this issue be treated delicately and that this information not spread nor used to embarrass the users and they should continue to be reassured that they will not be getting into any trouble over this as long as they continue to refrain from accessing wikileaks documentation.

SIIRT will be following up to schedule desanitization. OSY will be following up to give them an inadvertent disclosure briefing.

Rob G.

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

From: ou\_secur@nist.gov [mailto:ou\_secur@nist.gov] On Behalf Of Glenn, K. Robert  
Sent: Friday, December 03, 2010 8:09 AM  
To: Multiple recipients of list  
Subject: RE: Guidance regarding Wikileaks

OU ITSOs,

In close consultation with the NIST Director's Office and DoC, we now have a plan to move forward for NIST computers that connected to wikileaks before blocks were implemented. I've included some details and highlights of the plan below; the technical work will be performed by SIIRT (and given that there are 36 computers involved, this could impact other priorities).

1) Notify users verbally that their computer has been identified as having accessed Wikileaks documentation and as a result, may have unknowingly accessed classified information. Users are re-assured that they are not in trouble over this as the access was done prior to DoC guidance being issued. The notification will also explain that over the next several days NIST OISM incident response staff will work with them to properly sanitize their computer. Until the sanitization is complete, users may continue using their computer, but they are not to access, read, or move any Wikileaks documentation downloaded to their computer. Users are also not to try to sanitize their own computers. Users will also be notified that DoC OSY will follow-up with them to provide a inadvertent disclosure briefing. Those with clearances may be asked (by OSY) to take refresher training.

> Status: Susannah and I started contacting users late yesterday afternoon and will try to complete this today.

2) Notify OU Directors and OU ITSOs that have affected computers in their OUs;

> Status: Del started contacting OU Directors late yesterday afternoon. This email is your initial notification. Once all users in your OU have been contacted, I will then send the relevant OU ITSO the list of their affected users/computers.

3) SIIRT to complete detailed analysis of network logs to prioritize the order for which computers will be sanitized. Computers that have accessed the site the most or downloaded the most documentation will be sanitized first.

4) For each computer to be sanitized SIIRT will schedule time with each user (in prioritized order) to:

a) Identify the browser used; for each browser, clear cache, history, temporary files, etc.

b) Verify if the user stored any downloaded files elsewhere (e.g., thumb drives, CDs, DVDs, backups, etc.). Verify that nothing was forwarded to other people via other methods such as email, IM, etc.

c) Delete all other files and completely erase all unused data sectors on all relevant media and hard disks.

d) Sanitize or destroy any mobile media or backup storage used to store Wikileaks documentation.

e) Document all steps performed, responses from the user to questions, and any errors that may arise during the procedure.

5) Notify DoC OCIO that clean up has been completed and that specific details are available as needed.

=====

Note, that while the technical steps follow standard operating procedures for classified spillage clean-up, some aspects of the overall procedures (e.g. allowing users to continue using the computer) are only being done due to the massively public nature of the spillage. For more typically spillage incidents, the computer would be immediately removed from the network and sanitization would be immediate. For larger spillages, the hard drive would be removed, labeled, and stored in an approved container until the sanitization could be completed. The plan above was reviewed and approved by the Director's Office.

# of users/computers per OU (for OUs is not listed, there were no computers identified at this time):

OISM: 4 (1 in Boulder)

OFPM: 2 (both in Boulder)

TIP: 2

MEP: 1

NCNR: 2

CNST: 1

MML: 2 (both in Boulder)

PML: 9 (4 in Boulder)

EL: 4

ITL: 9

Rob G.

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

From: allstaff@nist.gov [mailto:allstaff@nist.gov] On Behalf Of NIST IT Assistance Center

Sent: Wednesday, December 01, 2010 2:45 PM

To: Multiple recipients of list

Subject: RE: Guidance regarding WikiLeaks

Attention NIST Staff:

To clarify the guidance that the Department of Commerce issued earlier today we ask that you not use the Commerce contact information provided in that email. Instead, direct any questions or notifications of access to WikiLeaks documents to the NIST IT Assistance Center (iTAC).

iTAC  
IT Assistance Center  
itac@nist.gov

303-497-5375 (Boulder)  
301-975-5375 (Gaithersburg)

Hours of Operation:

Boulder: 7:30am - 5:30pm (Mountain Time) Monday - Friday  
Gaithersburg: 7:30am - 5:30pm (Eastern Time) Monday - Friday

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

From: allstaff@nist.gov [mailto:allstaff@nist.gov] On Behalf Of Broadcast, DOC  
Sent: Wednesday, December 01, 2010 11:11 AM  
To: Multiple recipients of list  
Subject: Guidance regarding WikiLeaks

To: All Commerce Employees and Contractors

Recent reports indicate that a number of government documents have been posted on the WikiLeaks website. These documents may or may not contain information that is considered National Security Information (classified information) and as such, the information is NOT authorized for downloading, viewing, printing, processing, copying, or transmitting via non-classified Government-issued computers, laptops, blackberries, or other communication devices and is not an authorized use of DOC IT equipment. Doing so would introduce potentially classified information onto our unclassified networks and represent a potential security incident.

There has been a rumor that the information is no longer classified since it resides in the public domain. This is NOT true. Executive Order 13526, Section I.1(4)(2) states "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information." The information was neither properly nor improperly "declassified" by the appropriate authority and requires continued classification or reclassification.

Please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents because these documents may contain classified information. Accessing the WikiLeaks documents will lead to sanitization of your PC to remove any potentially classified information from the system and result in possible data loss.

If you have questions regarding this broadcast or have accessed the WikiLeaks documents, please contact the DOC Computer Incident Response Team at email doc-cirt@doc.gov or call (202) 482-4000.

---

This message was authorized by the Office of Secretary OSY/OCIO.

Please do not reply to this message. The broadcast email account is not monitored for incoming mail.



**Loebach, Matthew T.**

---

**From:** Glenn, K. Robert  
**Sent:** Monday, December 06, 2010 12:07 PM  
**To:** Fein, Aaron P.  
**Cc:** siirt; Sorensen, Robert; Beltz, John; Glenn, K. Robert  
**Subject:** RE: Guidance regarding WikiLeaks

Aaron,

All PML users have been contacted. Note those labeled as (email) means that I was only able to reach them via email and do not have confirmation that they read the message. All others were contacted verbally. Here is the additional information.

612061	(b)(2) (b)(6)	682
623254	(b)(6)	683 (email)
617030	(b)(6)	683 (email)
634111	(b)(2)	684
933199	(b)(6)	687 (email)
931061	(b)(6)	688 (email)
933751	(b)(2)	688 (email)
940569		697
851511	(b)(6)	698

It is important that this issue be treated delicately and that this information not spread nor used to embarrass the users and they should continue to be reassured that they will not be getting into any trouble over this as long as they continue to refrain from accessing wikileaks documentation.

SIIRT will be following up to schedule desanitization. OSY will be following up to give them an inadvertent disclosure briefing.

Rob G.

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

**From:** ou\_secur@nist.gov [mailto:ou\_secur@nist.gov] On Behalf Of Glenn, K. Robert  
**Sent:** Friday, December 03, 2010 8:09 AM  
**To:** Multiple recipients of list  
**Subject:** RE: Guidance regarding WikiLeaks

OU ITSOs,

In close consultation with the NIST Director's Office and DoC, we now have a plan to move forward for NIST computers that connected to wikileaks before blocks were implemented. I've included some details and highlights of the plan below; the technical work will be performed by SIIRT (and given that there are 36 computers involved, this could impact other priorities).

1) Notify users verbally that their computer has been identified as having accessed Wikileaks documentation and as a result, may have unknowingly accessed classified information. Users are re-assured that they are not in trouble over this as the access was done prior to DoC guidance being issued. The notification will also explain that over the next several days NIST OISM incident response staff will work with them to properly sanitize their computer. Until the sanitization is complete, users may continue using their computer, but they are not to access, read, or move any Wikileaks documentation downloaded to their computer. Users are

also not to try to sanitize their own computers. Users will also be notified that DoC OSY will follow-up with them to provide a inadvertent disclosure briefing. Those with clearances may be asked (by OSY) to take refresher training.

> Status: Susannah and I started contacting users late yesterday afternoon and will try to complete this today.

2) Notify OU Directors and OU ITSOs that have affected computers in their OUs;

> Status: Del started contacting OU Directors late yesterday afternoon. This email is your initial notification. Once all users in your OU have been contacted, I will then send the relevant OU ITSO the list of their affected users/computers.

3) SIIRT to complete detailed analysis of network logs to prioritize the order for which computers will be sanitized. Computers that have accessed the site the most or downloaded the most documentation will be sanitized first.

4) For each computer to be sanitized SIIRT will schedule time with each user (in prioritized order) to:

a) Identify the browser used; for each browser, clear cache, history, temporary files, etc.

b) Verify if the user stored any downloaded files elsewhere (e.g., thumb drives, CDs, DVDs, backups, etc.). Verify that nothing was forwarded to other people via other methods such as email, IM, etc.

c) Delete all other files and completely erase all unused data sectors on all relevant media and hard disks.

d) Sanitize or destroy any mobile media or backup storage used to store Wikileaks documentation.

e) Document all steps performed, responses from the user to questions, and any errors that may arise during the procedure.

5) Notify DoC OCIO that clean up has been completed and that specific details are available as needed.

=====

Note, that while the technical steps follow standard operating procedures for classified spillage clean-up, some aspects of the overall procedures (e.g. allowing users to continue using the computer) are only being done due to the massively public nature of the spillage. For more typically spillage incidents, the computer would be immediately removed from the network and sanitization would be immediate. For larger spillages, the hard drive would be removed, labeled, and stored in an approved container until the sanitization could be completed. The plan above was reviewed and approved by the Director's Office.

# of users/computers per OU (for OUs is not listed, there were no computers identified at this time):

OISM: 4 (1 in Boulder)

OFPM: 2 (both in Boulder)

TIP: 2

MEP: 1

NCNR: 2

CNST: 1

MML: 2 (both in Boulder)

PML: 9 (4 in Boulder)

EL: 4

ITL: 9

Rob G.

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

From: allstaff@nist.gov [mailto:allstaff@nist.gov] On Behalf Of NIST IT Assistance Center  
Sent: Wednesday, December 01, 2010 2:45 PM  
To: Multiple recipients of list  
Subject: RE: Guidance regarding Wikileaks

Attention NIST Staff:

To clarify the guidance that the Department of Commerce issued earlier today we ask that you not use the Commerce contact information provided in that email. Instead, direct any questions or notifications of access to Wikileaks documents to the NIST IT Assistance Center (iTAC).

iTAC  
IT Assistance Center  
itac@nist.gov

303-497-5375 (Boulder)  
301-975-5375 (Gaithersburg)

Hours of Operation:

Boulder: 7:30am - 5:30pm (Mountain Time) Monday - Friday  
Gaithersburg: 7:30am - 5:30pm (Eastern Time) Monday - Friday

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

From: allstaff@nist.gov [mailto:allstaff@nist.gov] On Behalf Of Broadcast, DOC  
Sent: Wednesday, December 01, 2010 11:11 AM  
To: Multiple recipients of list  
Subject: Guidance regarding Wikileaks

To: All Commerce Employees and Contractors

Recent reports indicate that a number of government documents have been posted on the Wikileaks website. These documents may or may not contain information that is considered National Security Information (classified information) and as such, the information is NOT authorized for downloading, viewing, printing, processing, copying, or transmitting via non-classified Government-issued computers, laptops, blackberries, or other communication devices and is not an authorized use of DOC IT equipment. Doing so would introduce potentially classified information onto our unclassified networks and represent a potential security incident.

There has been a rumor that the information is no longer classified since it resides in the public domain. This is NOT true. Executive Order 13526, Section I.1(4)(2) states "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information." The information was neither properly nor improperly "declassified" by the appropriate authority and requires continued classification or reclassification.

Please do not attempt to access any of the Wikileaks documents via the Wikileaks website or through other websites hosting those documents because these documents may contain classified information. Accessing the Wikileaks documents will lead to sanitization of your PC to remove any potentially classified information from the system and result in possible data loss.

If you have questions regarding this broadcast or have accessed the Wikileaks documents, please contact the DOC Computer Incident Response Team at email [doc-cirt@doc.gov](mailto:doc-cirt@doc.gov) or call (202) 482-4000.

---

This message was authorized by the Office of Secretary OSY/OCIO.

Please do not reply to this message. The broadcast email account is not monitored for incoming mail.

RE: Guidance regarding WikiLeaks

**Subject:** RE: Guidance regarding WikiLeaks  
**From:** "Rickerds, Ann R." <ann.rickerds@nist.gov>  
**Date:** Mon, 6 Dec 2010 12:36:07 -0500  
**To:** "Glenn, K. Robert" <robert.glenn@nist.gov>

Rob,

Thanks for the information. Let me know if you or the team need any assistance.

Thanks,

Ann Rickerds  
ITL IT Security Officer  
[x2055/ann@nist.gov](mailto:x2055/ann@nist.gov)  
-----Original Message-----

From: Glenn, K. Robert  
Sent: Monday, December 06, 2010 12:09 PM  
To: Rickerds, Ann R.  
Cc: siirt; Glenn, K. Robert  
Subject: RE: Guidance regarding WikiLeaks

Ann,

All ITL users have been contacted. Note those labeled as (email) means that I was only able to reach them via email and do not have confirmation that they read the message. All others were contacted verbally. Here is the additional information.

635896	(b)(2)	(b)(6)	771	
634008			772	
629074			773	(b)(6)
				774
629071				(b)(6)
624503	(b)(2)		775	(b)(6)
631298			775	(email)
634024			774	
			773	

It is important that this issue be treated delicately and that this information not spread nor used to embarrass the users and they should continue to be reassured that they will not be getting into any trouble over this as long as they continue to refrain from accessing wikileaks documentation.

SIIRT will be following up to schedule desanitization. OSY will be following up to give them an inadvertent disclosure briefing.

Rob G.

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

From: [ou\\_secur@nist.gov](mailto:ou_secur@nist.gov) [mailto:[ou\\_secur@nist.gov](mailto:ou_secur@nist.gov)] On Behalf Of Glenn, K. Robert  
Sent: Friday, December 03, 2010 8:09 AM  
To: Multiple recipients of list  
Subject: RE: Guidance regarding WikiLeaks

OU ITSOs,

In close consultation with the NIST Director's Office and DoC, we now have a plan to move forward for NIST computers that connected to wikileaks before blocks were implemented. I've included some details and highlights of the plan below; the technical work will be performed by SIIRT (and given that there are 36 computers involved, this could impact other priorities).

1) Notify users verbally that their computer has been identified as having accessed Wikileaks documentation and as a result, may have unknowingly accessed classified information. Users are re-assured that they are not in trouble over this as the access was done prior to DoC guidance being issued. The notification will also explain that over the next several days NIST OISM incident response staff will work with them to properly sanitize their computer. Until the sanitization is complete, users may continue using their computer, but they are not to access, read, or move any Wikileaks documentation downloaded to their computer. Users are also not to try to sanitize their own computers. Users will also be notified that DoC OSY will follow-up with them to provide a inadvertent disclosure briefing. Those with clearances may be asked (by OSY) to take refresher training.

> Status: Susannah and I started contacting users late yesterday afternoon and will try to complete this today.

2) Notify OU Directors and OU ITSOs that have affected computers in their OUs;

> Status: Del started contacting OU Directors late yesterday afternoon. This email is your initial notification. Once all users in your OU have been contacted, I will then send the relevant OU ITSO the list of their affected users/computers.

3) SIIRT to complete detailed analysis of network logs to prioritize the order for which computers will be sanitized. Computers that have accessed the site the most or downloaded the most documentation will be sanitized first.

4) For each computer to be sanitized SIIRT will schedule time with each user (in prioritized order) to:

a) Identify the browser used; for each browser, clear cache, history, temporary files, etc.

b) Verify if the user stored any downloaded files elsewhere (e.g., thumb drives, CDs, DVDs, backups, etc.). Verify that nothing was forwarded to other people via other methods such as email, IM, etc.

c) Delete all other files and completely erase all unused data sectors on all relevant media and hard disks.

d) Sanitize or destroy any mobile media or backup storage used to store Wikileaks documentation.

e) Document all steps performed, responses from the user to questions, and any errors that may arise during the procedure.

5) Notify DoC OCIO that clean up has been completed and that specific details are available as needed.

=====

Note, that while the technical steps follow standard operating procedures for classified spillage clean-up, some aspects of the overall procedures (e.g. allowing users to continue using the computer) are only being done due to the massively public nature of the spillage. For more typically spillage incidents, the computer would be immediately removed from the network and sanitization would be immediate. For larger spillages, the hard drive would be removed, labeled, and stored in an approved container until the sanitization could be completed. The plan above was reviewed and approved by the Director's Office.

# of users/computers per OU (for OUs is not listed, there were no computers identified at this time):

OISM: 4 (1 in Boulder)

OFPM: 2 (both in Boulder)

TIP: 2

MEP: 1

NCNR: 2

CNST: 1

MML: 2 (both in Boulder)

PML: 9 (4 in Boulder)

RE: Guidance regarding WikiLeaks

EL: 4  
ITL: 9

Rob G.

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

From: [allstaff@nist.gov](mailto:allstaff@nist.gov) [<mailto:allstaff@nist.gov>] On Behalf Of NIST IT Assistance Center

Sent: Wednesday, December 01, 2010 2:45 PM

To: Multiple recipients of list

Subject: RE: Guidance regarding WikiLeaks

Attention NIST Staff:

To clarify the guidance that the Department of Commerce issued earlier today we ask that you not use the Commerce contact information provided in that email. Instead, direct any questions or notifications of access to WikiLeaks documents to the NIST IT Assistance Center (iTAC).

iTAC  
IT Assistance Center  
[itac@nist.gov](mailto:itac@nist.gov)

303-497-5375 (Boulder)  
301-975-5375 (Gaithersburg)

Hours of Operation:

Boulder: 7:30am - 5:30pm (Mountain Time) Monday - Friday

Gaithersburg: 7:30am - 5:30pm (Eastern Time) Monday - Friday

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

From: [allstaff@nist.gov](mailto:allstaff@nist.gov) [<mailto:allstaff@nist.gov>] On Behalf Of Broadcast, DOC

Sent: Wednesday, December 01, 2010 11:11 AM

To: Multiple recipients of list

Subject: Guidance regarding WikiLeaks

To: All Commerce Employees and Contractors

Recent reports indicate that a number of government documents have been posted on the WikiLeaks website. These documents may or may not contain information that is considered National Security Information (classified information) and as such, the information is NOT authorized for downloading, viewing, printing, processing, copying, or transmitting via non-classified Government-issued computers, laptops, blackberries, or other communication devices and is not an authorized use of DOC IT equipment. Doing so would introduce potentially classified information onto our unclassified networks and represent a potential security incident.

There has been a rumor that the information is no longer classified since it resides in the public domain. This is NOT true. Executive Order 13526, Section I.1(4)(2) states "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information." The information was neither properly nor improperly "declassified" by the appropriate authority and requires continued classification or reclassification.

Please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents because these documents may contain classified information. Accessing the WikiLeaks documents will lead to sanitization of your PC to remove any potentially classified information from the system and result in possible data loss.

If you have questions regarding this broadcast or have accessed the WikiLeaks

documents, please contact the DOC Computer Incident Response Team at email [doc-cirt@doc.gov](mailto:doc-cirt@doc.gov) or call (202) 482-4000.

---

This message was authorized by the Office of Secretary OSY/OCIO.

Please do not reply to this message. The broadcast email account is not monitored for incoming mail.



RE: Guidance regarding WikiLeaks

**Subject:** RE: Guidance regarding WikiLeaks  
**From:** "Long, Kathleen" <kathleen.long@nist.gov>  
**Date:** Tue, 7 Dec 2010 12:04:43 -0500  
**To:** "Glenn, K. Robert" <robert.glenn@nist.gov>

Thanks. I have followed up with his manager to make sure he got the message and knows how what to expect.

Kathleen Long, CISSP  
Manufacturing Extension Partnership  
National Institute of Standards and Technology  
100 Bureau Drive, Stop 4800  
Gaithersburg, MD 20899  
Ph: 301-975-2474

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

From: Glenn, K. Robert  
Sent: Monday, December 06, 2010 11:59 AM  
To: Long, Kathleen  
Cc: siirt; Glenn, K. Robert  
Subject: RE: Guidance regarding WikiLeaks

Kathy,

The MEP user has been contacted. Note, I was only able to contact him by email and do not have confirmation that they read the message. All others were contacted verbally. Here is the additional information.

621855 [REDACTED] (b)(7)(D) 488

It is important that this issue be treated delicately and that this information not spread nor used to embarrass the users and they should continue to be reassured that they will not be getting into any trouble over this as long as they continue to refrain from accessing wikileaks documentation.

SIIRT will be following up to schedule desanitization. OSY will be following up to give them an inadvertent disclosure briefing.

Rob G.

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

From: [ou\\_secur@nist.gov](mailto:ou_secur@nist.gov) [mailto:[ou\\_secur@nist.gov](mailto:ou_secur@nist.gov)] On Behalf Of Glenn, K. Robert  
Sent: Friday, December 03, 2010 8:09 AM  
To: Multiple recipients of list  
Subject: RE: Guidance regarding WikiLeaks

OU ITSOs,

In close consultation with the NIST Director's Office and DoC, we now have a plan to move forward for NIST computers that connected to wikileaks before blocks were implemented. I've included some details and highlights of the plan below; the technical work will be performed by SIIRT (and given that there are 36 computers involved, this could impact other priorities).

1) Notify users verbally that their computer has been identified as having accessed Wikileaks documentation and as a result, may have unknowingly accessed classified information. Users are re-assured that they are not in trouble over this as the access was done prior to DoC guidance being issued. The notification will also explain that over the next several days NIST OISM incident response staff will work

with them to properly sanitize their computer. Until the sanitization is complete, users may continue using their computer, but they are not to access, read, or move any Wikileaks documentation downloaded to their computer. Users are also not to try to sanitize their own computers. Users will also be notified that DoC OSY will follow-up with them to provide a inadvertent disclosure briefing. Those with clearances may be asked (by OSY) to take refresher training.

> Status: Susannah and I started contacting users late yesterday afternoon and will try to complete this today.

2) Notify OU Directors and OU ITSOs that have affected computers in their OUs;

> Status: Del started contacting OU Directors late yesterday afternoon. This email is your initial notification. Once all users in your OU have been contacted, I will then send the relevant OU ITSO the list of their affected users/computers.

3) SIIRT to complete detailed analysis of network logs to prioritize the order for which computers will be sanitized. Computers that have accessed the site the most or downloaded the most documentation will be sanitized first.

4) For each computer to be sanitized SIIRT will schedule time with each user (in prioritized order) to:

a) Identify the browser used; for each browser, clear cache, history, temporary files, etc.

b) Verify if the user stored any downloaded files elsewhere (e.g., thumb drives, CDs, DVDs, backups, etc.). Verify that nothing was forwarded to other people via other methods such as email, IM, etc.

c) Delete all other files and completely erase all unused data sectors on all relevant media and hard disks.

d) Sanitize or destroy any mobile media or backup storage used to store Wikileaks documentation.

e) Document all steps performed, responses from the user to questions, and any errors that may arise during the procedure.

5) Notify DoC OCIO that clean up has been completed and that specific details are available as needed.

=====

Note, that while the technical steps follow standard operating procedures for classified spillage clean-up, some aspects of the overall procedures (e.g. allowing users to continue using the computer) are only being done due to the massively public nature of the spillage. For more typically spillage incidents, the computer would be immediately removed from the network and sanitization would be immediate. For larger spillages, the hard drive would be removed, labeled, and stored in an approved container until the sanitization could be completed. The plan above was reviewed and approved by the Director's Office.

# of users/computers per OU (for OUs is not listed, there were no computers identified at this time):

OISM: 4 (1 in Boulder)

OFPM: 2 (both in Boulder)

TIP: 2

MEP: 1

NCNR: 2

CNST: 1

MML: 2 (both in Boulder)

PML: 9 (4 in Boulder)

EL: 4

ITL: 9

Rob G.

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

RE: Guidance regarding WikiLeaks

From: [allstaff@nist.gov](mailto:allstaff@nist.gov) [<mailto:allstaff@nist.gov>] On Behalf Of NIST IT Assistance Center  
Sent: Wednesday, December 01, 2010 2:45 PM  
To: Multiple recipients of list  
Subject: RE: Guidance regarding WikiLeaks

Attention NIST Staff:

To clarify the guidance that the Department of Commerce issued earlier today we ask that you not use the Commerce contact information provided in that email. Instead, direct any questions or notifications of access to WikiLeaks documents to the NIST IT Assistance Center (iTAC).

iTAC  
IT Assistance Center  
[itac@nist.gov](mailto:itac@nist.gov)

303-497-5375 (Boulder)  
301-975-5375 (Gaithersburg)

Hours of Operation:  
Boulder: 7:30am - 5:30pm (Mountain Time) Monday - Friday  
Gaithersburg: 7:30am - 5:30pm (Eastern Time) Monday - Friday

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

From: [allstaff@nist.gov](mailto:allstaff@nist.gov) [<mailto:allstaff@nist.gov>] On Behalf Of Broadcast, DOC  
Sent: Wednesday, December 01, 2010 11:11 AM  
To: Multiple recipients of list  
Subject: Guidance regarding WikiLeaks

To: All Commerce Employees and Contractors

Recent reports indicate that a number of government documents have been posted on the WikiLeaks website. These documents may or may not contain information that is considered National Security Information (classified information) and as such, the information is NOT authorized for downloading, viewing, printing, processing, copying, or transmitting via non-classified Government-issued computers, laptops, blackberries, or other communication devices and is not an authorized use of DOC IT equipment. Doing so would introduce potentially classified information onto our unclassified networks and represent a potential security incident.

There has been a rumor that the information is no longer classified since it resides in the public domain. This is NOT true. Executive Order 13526, Section I.1(4)(2) states "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information." The information was neither properly nor improperly "declassified" by the appropriate authority and requires continued classification or reclassification.

Please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents because these documents may contain classified information. Accessing the WikiLeaks documents will lead to sanitization of your PC to remove any potentially classified information from the system and result in possible data loss.

If you have questions regarding this broadcast or have accessed the WikiLeaks documents, please contact the DOC Computer Incident Response Team at email [doc-cirt@doc.gov](mailto:doc-cirt@doc.gov) or call (202) 482-4000.

---

This message was authorized by the Office of Secretary OSY/OCIO.

Please do not reply to this message. The broadcast email account is not monitored

E: Guidance regarding WikiLeaks

for incoming mail.

**Subject:** RE: IMPORTANT - RE: Guidance regarding WikiLeaks  
**From:** "Glenn, K. Robert" <robert.glenn@nist.gov>  
**Date:** Tue, 7 Dec 2010 13:34:20 -0500  
**To:** "Bruno, Thomas J. Dr." <thomas.bruno@nist.gov>  
**CC:** "Glenn, K. Robert" <robert.glenn@nist.gov>

Tom, I'll have my staff follow-up with you to perform an initial sanitization, but they are likely to have questions that only your student can answer. They will need to follow up at a later date and ask if they did any more than just browse the site, and if they downloaded any documentation, where they would have put that documentation.

Regards,

Rob G.

---

**From:** Dr. Tom Bruno [mailto:bruno@boulder.nist.gov]  
**Sent:** Tuesday, December 07, 2010 9:06 AM  
**To:** Glenn, K. Robert  
**Subject:** Re: IMPORTANT - RE: Guidance regarding WikiLeaks

Rob:

Follow up with me, not him. He has finals this week and then will be on break for some time.

Tom

Dr. Thomas J. Bruno, Group Leader  
Experimental Properties of Fluids  
Thermophysical Properties Division  
National Institute of Standards and Technology  
325 Broadway, MS 638.00  
Boulder, CO 80305  
303-497-5158 (office)  
303-497-5978 (lab)  
303-497-5044 (fax)

On 12/7/2010 6:33 AM, Glenn, K. Robert wrote:  
Tom,

We don't know the format or much else about the specific classified documents; I suspect given the quantity of material leaked from the site, that few know what is and is not classified. DoC has required that we remove all traces of access to the wikileaks websites as well as any files that may have been downloaded.

I'll have my staff follow up with (b)(6) to have the computer cleaned. After removing any relevant files, clearing browser history and temporary files, etc., they install software that will permanently erase any/all deleted files. This is a routine process for removing these types of files from computers and should not affect any other user data stored on the computer.

Regards,

RE: IMPORTANT - RE: Guidance regarding WikiLeaks

Rob G.

---

**From:** Dr. Tom Bruno [mailto:bruno@boulder.nist.gov]  
**Sent:** Monday, December 06, 2010 4:01 PM  
**To:** Glenn, K. Robert  
**Subject:** Re: IMPORTANT - RE: Guidance regarding WikiLeaks

Is this a ppt? His name is [REDACTED] (b)(6)

Dr. Thomas J. Bruno, Group Leader  
Experimental Properties of Fluids  
Thermophysical Properties Division  
National Institute of Standards and Technology  
325 Broadway, MS 638.00  
Boulder, CO 80305  
303-497-5158 (office)  
303-497-5978 (lab)  
303-497-5044 (fax)

(b)(2)  
On 12/6/2010 10:02 AM, Glenn, K. Robert wrote:

Tom, The address is [REDACTED], property # 930364. Please send the name of the student, so OSY can send them the inadvertent disclosure briefing.

Thanks,

Rob G.

---

**From:** Dr. Tom Bruno [mailto:bruno@boulder.nist.gov]  
**Sent:** Monday, December 06, 2010 11:59 AM  
**To:** Glenn, K. Robert  
**Subject:** Re: IMPORTANT - RE: Guidance regarding WikiLeaks

Rob:

Apparently this was done by a student. I have already spoken to the individual. Can you give me the IP address of the computer?

Tom

Dr. Thomas J. Bruno, Group Leader  
Experimental Properties of Fluids  
Thermophysical Properties Division  
National Institute of Standards and Technology  
325 Broadway, MS 638.00  
Boulder, CO 80305  
303-497-5158 (office)  
303-497-5978 (lab)  
303-497-5044 (fax)

On 12/6/2010 9:32 AM, Glenn, K. Robert wrote:

Dear Dr. Bruno,

I am the NIST IT Security Officer and I have been asked to contact all NIST staff who may have had a computer that connected to WikiLeaks prior to the guidance issued by DoC. Please be assured, that due to the nature of this issue, while this deals with access to potential classified information and we are required by DoC to respond to this incident, no one at NIST who went to the site prior to the guidance issued by DoC is going to get into any trouble. In fact, several NIST staff computers connected to the site prior to the issuance of the DoC guidance.

DOC has confirmed that WikiLeaks was accessed from a computer registered to you, which may mean classified information was unknowingly accessed. Because access occurred prior to receiving guidance from DOC (see below), this is viewed as an unintentional incident. However, NIST is required to treat the computer as though there is classified data resident (i.e., classified information spillage) and, the computer must be appropriately sanitized to ensure that any classified information is removed.

**The NIST Office of Information Systems Management (formerly OCIO) incident response team (Robert Sorensen or John Beltz) will contact you to schedule sanitization of the computer.** Please do not access, read, forward, or otherwise move any WikiLeaks documents that may have been downloaded. Also, please do not attempt to remove any such documents on your own. Sanitization will include removal of the information in your browser cache/history, temporary files, backups that may contain WikiLeaks documentation, etc., and verification that the information was not forwarded via other methods such as email, instant messaging, etc. Every effort will be made to preserve all other user data on the computer (i.e. ***this is a routine process and user data should not be affected***). Given the number of incidents within NIST, we ask for your patience in scheduling sanitization. Since classified information is involved, **the DOC Office of Security (OSY) will likely follow up and send you an inadvertent disclosure briefing which includes a reminder to not disclose any sensitive information you may have seen when going to the WikiLeaks site.**

As a reminder, please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents.

Please do not hesitate to contact me personally if you have any questions or concerns.

Regards,

Rob Glenn  
IT Security Officer, NIST

[rob.glenn@nist.gov](mailto:rob.glenn@nist.gov)  
301-975-3667

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

From: [allstaff@nist.gov](mailto:allstaff@nist.gov) [mailto:[allstaff@nist.gov](mailto:allstaff@nist.gov)] On Behalf Of NIST IT Assistance Center  
Sent: Wednesday, December 01, 2010 2:45 PM  
To: Multiple recipients of list

Subject: RE: Guidance regarding WikiLeaks

Attention NIST Staff:

To clarify the guidance that the Department of Commerce issued earlier today we ask that you not use the Commerce contact information provided in that email. Instead, direct any questions or notifications of access to WikiLeaks documents to the NIST IT Assistance Center (iTAC).

iTAC

IT Assistance Center

[itac@nist.gov](mailto:itac@nist.gov)

303-497-5375 (Boulder)

301-975-5375 (Gaithersburg)

Hours of Operation:

Boulder: 7:30am - 5:30pm (Mountain Time) Monday - Friday

Gaithersburg: 7:30am - 5:30pm (Eastern Time) Monday - Friday

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

From: [allstaff@nist.gov](mailto:allstaff@nist.gov) [mailto:[allstaff@nist.gov](mailto:allstaff@nist.gov)] On Behalf Of Broadcast, DOC

Sent: Wednesday, December 01, 2010 11:11 AM

To: Multiple recipients of list

Subject: Guidance regarding WikiLeaks



To: All Commerce Employees and Contractors

Recent reports indicate that a number of government documents have been posted on the WikiLeaks website. These documents may or may not contain information that is considered National Security Information (classified information) and as such, the information is NOT authorized for downloading, viewing, printing, processing, copying, or transmitting via non-classified Government-issued computers, laptops, blackberries, or other communication devices and is not an authorized use of DOC IT equipment. Doing so would introduce potentially classified information onto our unclassified networks and represent a potential security incident.

There has been a rumor that the information is no longer classified since it resides in the public domain. This is NOT true. Executive Order 13526, Section 1.1(4)(2) states "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information." The information was neither properly nor improperly "declassified" by the appropriate authority and requires continued classification or reclassification.

Please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents because these documents may contain classified information. Accessing the WikiLeaks documents will lead to sanitization of your PC to remove any potentially classified information from the system and result in possible data loss.

If you have questions regarding this broadcast or have accessed the WikiLeaks documents, please contact the DOC Computer Incident Response Team at email [doc-cirt@doc.gov](mailto:doc-cirt@doc.gov) or call (202) 482-4000.

---

This message was authorized by the Office of Secretary OSY/OCIO.

Please do not reply to this message. The broadcast email account is not monitored for incoming mail.

E: IMPORTANT - RE: Guidance regarding WikiLeaks

**McIntyre, Jeffrey J.**

---

**From:** David Kustaborder [kusty@nist.gov]  
**Sent:** Tuesday, December 07, 2010 3:41 PM  
**To:** Glenn, K. Robert; siirt  
**Subject:** Wiki Status  
**Attachments:** wiki-contact.xls

---

Sheet1

Property Number	src	User	Division	Phone	Associate	Sanitized
634024				184		Complete
631634				774	Y	Complete
629071				774		Complete
931061				688		
624503				775		
934346				181		
631753				732		In Progress
634008				772		
851531				731		In Progress
940819				194		
850752				183		Complete
612740				730		In Progress
933199				687		
851068				653		
				191		
623254				683		
629074				773		
621855				488		
940569				697		
624101				610		
631298				775		
617030				683	N	
633663				470	E	In Progress
633683				470	E	In Progress
612061				682	N	
930364				638	E	In Progress
933751				688	N	
634222				181	E	Complete
635896				771	E	
851511				698	E	
634111				684	E	
635565				610	E	
850223				620	E	
634570				730		Complete

**McIntyre, Jeffrey J.**

---

**From:** David Kustaborder [kusty@nist.gov]  
**Sent:** Tuesday, December 07, 2010 4:01 PM  
**To:** Glenn, K. Robert  
**Cc:** siirt  
**Subject:** wiki status (fixed)  
**Attachments:** wiki-contact.xls

---

Property Number	src	User	Division	Phone	Associate	Sanitized
634024	[REDACTED]	[REDACTED]		184		Complete
631634	[REDACTED]	[REDACTED]		774	Y	Complete
629071	[REDACTED]	[REDACTED]		774		Complete
931061	[REDACTED]	[REDACTED]		688		
624503	[REDACTED]	[REDACTED]		775		
934346	[REDACTED]	[REDACTED]		181		
631753	[REDACTED]	[REDACTED]		732		In Progress
634008	[REDACTED]	[REDACTED]		772		
851531	[REDACTED]	[REDACTED]		731		In Progress
940819	[REDACTED]	[REDACTED]		194		
850752	[REDACTED]	[REDACTED]		183		Complete
612740	[REDACTED]	[REDACTED]		730		In Progress
933199	[REDACTED]	[REDACTED]		687		
851068	[REDACTED]	[REDACTED]		653		
	[REDACTED]	[REDACTED]		191		
623254	[REDACTED]	[REDACTED]		683		
629074	[REDACTED]	[REDACTED]		773		
621855	[REDACTED]	[REDACTED]		488		
940569	[REDACTED]	[REDACTED]		697		
624101	[REDACTED]	[REDACTED]		610		
631298	[REDACTED]	[REDACTED]		775		
617030	[REDACTED]	[REDACTED]		683	N	
633663	[REDACTED]	[REDACTED]		470	E	In Progress
633683	[REDACTED]	[REDACTED]		470	E	In Progress
612061	[REDACTED]	[REDACTED]		682	N	In Progress
930364	[REDACTED]	[REDACTED]		638	E	
933751	[REDACTED]	[REDACTED]		688	N	
634222	[REDACTED]	[REDACTED]		181	E	Complete
635896	[REDACTED]	[REDACTED]		771	E	
851511	[REDACTED]	[REDACTED]		698	E	
634111	[REDACTED]	[REDACTED]		684	E	
635565	[REDACTED]	[REDACTED]		610	E	
850223	[REDACTED]	[REDACTED]		620	E	
634570	[REDACTED]	[REDACTED]		730		Complete

RE: Guidance regarding WikiLeaks

**Subject:** RE: Guidance regarding WikiLeaks  
**From:** "Long, Kathleen" <kathleen.long@nist.gov>  
**Date:** Tue, 7 Dec 2010 16:44:57 -0500  
**To:** "Glenn, K. Robert" <robert.glenn@nist.gov>, siirt <siirt@nist.gov>

Thank you and yes, I understand I don't want to see anything that may have been downloaded. I am more interested in the process.

Kathleen Long, CISSP  
Manufacturing Extension Partnership  
National Institute of Standards and Technology  
100 Bureau Drive, Stop 4800  
Gaithersburg, MD 20899  
Ph: 301-975-2474

---

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

From: Glenn, K. Robert  
Sent: Tuesday, December 07, 2010 4:26 PM  
To: siirt  
Cc: Long, Kathleen; Glenn, K. Robert  
Subject: FW: Guidance regarding WikiLeaks

SIIRT, Please invite Kathy, if possible.

Kathy, You won't be able to observe directly any files that have to be looked at, unless we can confirm with OSY that you are cleared at the Secret level. That said, I don't anticipate this would be a problem in the case of this specific incident.

Rob G.

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

From: Long, Kathleen  
Sent: Tuesday, December 07, 2010 2:49 PM  
To: Glenn, K. Robert  
Subject: RE: Guidance regarding WikiLeaks

Is it possible to sit in when SIIRT meets with ? It would be nice to see first-hand how these are handled.

Kathleen Long, CISSP  
Manufacturing Extension Partnership  
National Institute of Standards and Technology  
100 Bureau Drive, Stop 4800  
Gaithersburg, MD 20899  
Ph: 301-975-2474

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

From: Glenn, K. Robert  
Sent: Monday, December 06, 2010 11:59 AM  
To: Long, Kathleen

RE: Guidance regarding WikiLeaks

Cc: siirt; Glenn, K. Robert  
Subject: RE: Guidance regarding WikiLeaks

Kathy,

The MEP user has been contacted. Note, I was only able to contact him by email and do not have confirmation that they read the message. All others were contacted verbally. Here is the additional information.

621855 [REDACTED] (b)(2) (b)(7) 488

It is important that this issue be treated delicately and that this information not spread nor used to embarrass the users and they should continue to be reassured that they will not be getting into any trouble over this as long as they continue to refrain from accessing wikileaks documentation.

SIIRT will be following up to schedule desanitization. OSY will be following up to give them an inadvertent disclosure briefing.

Rob G.

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

From: [ou\\_secu@nist.gov](mailto:ou_secu@nist.gov) [mailto:[ou\\_secu@nist.gov](mailto:ou_secu@nist.gov)] On Behalf Of Glenn, K. Robert  
Sent: Friday, December 03, 2010 8:09 AM  
To: Multiple recipients of list  
Subject: RE: Guidance regarding WikiLeaks

OU ITSOs,

In close consultation with the NIST Director's Office and DoC, we now have a plan to move forward for NIST computers that connected to wikileaks before blocks were implemented. I've included some details and highlights of the plan below; the technical work will be performed by SIIRT (and given that there are 36 computers involved, this could impact other priorities).

1) Notify users verbally that their computer has been identified as having accessed Wkileaks documentation and as a result, may have unknowingly accessed classified information. Users are re-assured that they are not in trouble over this as the access was done prior to DoC guidance being issued. The notification will also explain that over the next several days NIST OISM incident response staff will work with them to properly sanitize their computer. Until the sanitization is complete, users may continue using their computer, but they are not to access, read, or move any Wikileaks documentation downloaded to their computer. Users are also not to try to sanitize their own computers. Users will also be notified that DoC OSY will follow-up with them to provide a inadvertent disclosure briefing. Those with clearances may be asked (by OSY) to take refresher training.

> Status: Susannah and I started contacting users late yesterday afternoon and will try to complete this today.

2) Notify OU Directors and OU ITSOs that have affected computers in their OUs;

> Status: Del started contacting OU Directors late yesterday afternoon. This email is your initial notification. Once all users in your OU have been contacted, I will then send the relevant OU ITSO the list of their affected users/computers.



- 3) SIIRT to complete detailed analysis of network logs to prioritize the order for which computers will be sanitized. Computers that have accessed the site the most or downloaded the most documentation will be sanitized first.
- 4) For each computer to be sanitized SIIRT will schedule time with each user (in prioritized order) to:
  - a) Identify the browser used; for each browser, clear cache, history, temporary files, etc.
  - b) Verify if the user stored any downloaded files elsewhere (e.g., thumb drives, CDs, DVDs, backups, etc.). Verify that nothing was forwarded to other people via other methods such as email, IM, etc.
  - c) Delete all other files and completely erase all unused data sectors on all relevant media and hard disks.
  - d) Sanitize or destroy any mobile media or backup storage used to store Wikileaks documentation.
  - e) Document all steps performed, responses from the user to questions, and any errors that may arise during the procedure.
- 5) Notify DoC OCIO that clean up has been completed and that specific details are available as needed.

---

Note, that while the technical steps follow standard operating procedures for classified spillage clean-up, some aspects of the overall procedures (e.g. allowing users to continue using the computer) are only being done due to the massively public nature of the spillage. For more typically spillage incidents, the computer would be immediately removed from the network and sanitization would be immediate. For larger spillages, the hard drive would be removed, labeled, and stored in an approved container until the sanitization could be completed. The plan above was reviewed and approved by the Director's Office.

# of users/computers per OU (for OUs is not listed, there were no computers identified at this time):

OISM: 4 (1 in Boulder)  
OFPM: 2 (both in Boulder)  
TIP: 2  
MEP: 1  
NCNR: 2  
CNST: 1  
MML: 2 (both in Boulder)  
PML: 9 (4 in Boulder)  
EL: 4  
ITL: 9

Rob G.

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

From: [allstaff@nist.gov](mailto:allstaff@nist.gov) [mailto:[allstaff@nist.gov](mailto:allstaff@nist.gov)] On Behalf Of NIST IT Assistance Center  
Sent: Wednesday, December 01, 2010 2:45 PM  
To: Multiple recipients of list  
Subject: RE: Guidance regarding WikiLeaks

Attention NIST Staff:

To clarify the guidance that the Department of Commerce issued earlier today we ask that you not

RE: Guidance regarding WikiLeaks

use the Commerce contact information provided in that email. Instead, direct any questions or notifications of access to WikiLeaks documents to the NIST IT Assistance Center (iTAC).

iTAC  
IT Assistance Center  
[itac@nist.gov](mailto:itac@nist.gov)

303-497-5375 (Boulder)  
301-975-5375 (Gaithersburg)

Hours of Operation:  
Boulder: 7:30am - 5:30pm (Mountain Time) Monday - Friday  
Gaithersburg: 7:30am - 5:30pm (Eastern Time) Monday - Friday

---

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

From: [allstaff@nist.gov](mailto:allstaff@nist.gov) [mailto:[allstaff@nist.gov](mailto:allstaff@nist.gov)] On Behalf Of Broadcast, DOC  
Sent: Wednesday, December 01, 2010 11:11 AM  
To: Multiple recipients of list  
Subject: Guidance regarding Wikileaks

To: All Commerce Employees and Contractors

Recent reports indicate that a number of government documents have been posted on the WikiLeaks website. These documents may or may not contain information that is considered National Security Information (classified information) and as such, the information is NOT authorized for downloading, viewing, printing, processing, copying, or transmitting via non-classified Government-issued computers, laptops, blackberries, or other communication devices and is not an authorized use of DOC IT equipment. Doing so would introduce potentially classified information onto our unclassified networks and represent a potential security incident.

There has been a rumor that the information is no longer classified since it resides in the public domain. This is NOT true. Executive Order 13526, Section I.1(4)(2) states "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information." The information was neither properly nor improperly "declassified" by the appropriate authority and requires continued classification or reclassification.

Please do not attempt to access any of the Wikileaks documents via the Wikileaks website or through other websites hosting those documents because these documents may contain classified information. Accessing the Wikileaks documents will lead to sanitization of your PC to remove any potentially classified information from the system and result in possible data loss.

If you have questions regarding this broadcast or have accessed the Wikileaks documents, please contact the DOC Computer Incident Response Team at email [doc-cirt@doc.gov](mailto:doc-cirt@doc.gov) or call (202) 482-4000.

---

This message was authorized by the Office of Secretary OSY/OCIO.

Please do not reply to this message. The broadcast email account is not monitored for incoming mail.



**McIntyre, Jeffrey J.**

---

**From:** David Kustaborder [kusty@nist.gov]  
**Sent:** Wednesday, December 08, 2010 4:13 PM  
**To:** Glenn, K. Robert  
**Cc:** siirt  
**Subject:** Wiki Status  
**Attachments:** wiki-contact.xls

FYI.

---

Property Number	src	User	Division	Phone	Associate	Sanitized
634024	(b)(2)	(b)(6)	184	(b)(6)		Complete
631634			774		Y	Complete
629071			774			Complete
931061			688			In Progress
624503			775			Complete
934346			181			Complete
631753			732			Complete
634008			772			Complete
851531			731			Complete
940819			194			Complete
850752			183			Complete
612740			730			Complete
933199			687			
851068			653			
			191			
623254			683			Complete
629074			773			Complete
621855			488			
940569			697			
624101			610			
631298			775			
617030			683		N	
633663			470		E	Complete
633683			470		E	Complete
612061			682		N	Complete
930364			638		E	
933751			688		N	
634222			181		E	Complete
635896			771		E	
851511			698		E	Scheduled for tomorrow
634111			684		E	
635565			610		E	
850223			620		E	Complete
634570			730			Complete
						In Progress

Cavanagh, Richard R. Dr.

From: Glenn, K. Robert  
Sent: Friday, December 10, 2010 11:06 AM  
To: Morey, Adam  
Cc: Cavanagh, Richard R. Dr.; Leith, Ann; Glenn, K. Robert  
Subject: RE: Guidance regarding WikiLeaks

Adam, I'll defer to you, Rich, and Tom to determine if that would be helpful. I'm happy to talk to him, but I suspect Tom has already relayed everything I had sent to him in email.

Rob. G.

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

From: Morey, Adam  
Sent: Wednesday, December 08, 2010 9:16 AM  
To: Glenn, K. Robert  
Cc: Cavanagh, Richard R. Dr.; Leith, Ann  
Subject: Re: Guidance regarding WikiLeaks

Thanks Rob,

Should we coordinate a conversation between [REDACTED] and John or Rob?

Adam

(b)(6)

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

From: Glenn, K. Robert  
To: Leith, Ann; Morey, Adam  
Cc: siirt; Beltz, John; Sorensen, Robert; Glenn, K. Robert  
Sent: Tue Dec 07 13:58:43 2010  
Subject: RE: Guidance regarding WikiLeaks

Adam and Ann,

Both MML users [REDACTED] have been contacted. Note I have had several email exchanges with Dr. Bruno. [REDACTED] is a student that is currently away from NIST and working on final exams. Dr. Bruno did not provide me with a date for when [REDACTED] will be back at NIST. Here is the additional information.

[REDACTED] (b)(6) (b)(6) (b)(6) (student - POC: Dr. Thomas Bruno) 638

It is important that this issue be treated delicately and that this information not spread nor used to embarrass the users and they should continue to be reassured that they will not be getting into any trouble over this as long as they continue to refrain from accessing wikileaks documentation.

SIIRT will be following up to schedule desanitization. OSY will be following up to give them an inadvertent disclosure briefing.

Robert & John B., Please work with Dr. Thomas Bruno for the identified computer. I have explained to him that you will work with him to do an initial sanitization, but would then

(b)(6)

need to follow-up at a later date with [REDACTED] to ask if any files were downloaded and if so, additional questions on where those files were put.

Rob G.

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

From: ou\_secur@nist.gov [mailto:ou\_secur@nist.gov] On Behalf Of Glenn, K. Robert

Sent: Friday, December 03, 2010 8:09 AM

To: Multiple recipients of list

Subject: RE: Guidance regarding Wikileaks

OU ITSOs,

In close consultation with the NIST Director's Office and DoC, we now have a plan to move forward for NIST computers that connected to wikileaks before blocks were implemented. I've included some details and highlights of the plan below; the technical work will be performed by SIIRT (and given that there are 36 computers involved, this could impact other priorities).

1) Notify users verbally that their computer has been identified as having accessed Wkileaks documentation and as a result, may have unknowingly accessed classified information. Users are re-assured that they are not in trouble over this as the access was done prior to DoC guidance being issued. The notification will also explain that over the next several days NIST OISM incident response staff will work with them to properly sanitize their computer. Until the sanitization is complete, users may continue using their computer, but they are not to access, read, or move any Wikileaks documentation downloaded to their computer. Users are also not to try to sanitize their own computers. Users will also be notified that DoC OSY will follow-up with them to provide a inadvertent disclosure briefing. Those with clearances may be asked (by OSY) to take refresher training.

> Status: Susannah and I started contacting users late yesterday afternoon and will try to complete this today.

2) Notify OU Directors and OU ITSOs that have affected computers in their OUs;

> Status: Del started contacting OU Directors late yesterday afternoon. This email is your initial notification. Once all users in your OU have been contacted, I will then send the relevant OU ITSO the list of their affected users/computers.

3) SIIRT to complete detailed analysis of network logs to prioritize the order for which computers will be sanitized. Computers that have accessed the site the most or downloaded the most documentation will be sanitized first.

4) For each computer to be sanitized SIIRT will schedule time with each user (in prioritized order) to:

a) Identify the browser used; for each browser, clear cache, history, temporary files, etc.

b) Verify if the user stored any downloaded files elsewhere (e.g., thumb drives, CDs, DVDs, backups, etc.). Verify that nothing was forwarded to other people via other methods such as email, IM, etc.

c) Delete all other files and completely erase all unused data sectors on all relevant media and hard disks.

d) Sanitize or destroy any mobile media or backup storage used to store Wikileaks documentation.

e) Document all steps performed, responses from the user to questions, and any errors that may arise during the procedure.

5) Notify DoC OCIO that clean up has been completed and that specific details are available as needed.

=====

Note, that while the technical steps follow standard operating procedures for classified spillage clean-up, some aspects of the overall procedures (e.g. allowing users to continue using the computer) are only being done due to the massively public nature of the spillage. For more typically spillage incidents, the computer would be immediately removed from the network and sanitization would be immediate. For larger spillages, the hard drive would be removed, labeled, and stored in an approved container until the sanitization could be completed. The plan above was reviewed and approved by the Director's Office.

# of users/computers per OU (for OUs is not listed, there were no computers identified at this time):

OISM: 4 (1 in Boulder)  
OFPM: 2 (both in Boulder)  
TIP: 2  
MEP: 1  
NCNR: 2  
CNST: 1  
MML: 2 (both in Boulder)  
PML: 9 (4 in Boulder)  
EL: 4  
ITL: 9

Rob G.

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

From: allstaff@nist.gov [mailto:allstaff@nist.gov] On Behalf Of NIST IT Assistance Center  
Sent: Wednesday, December 01, 2010 2:45 PM  
To: Multiple recipients of list  
Subject: RE: Guidance regarding WikiLeaks

Attention NIST Staff:

To clarify the guidance that the Department of Commerce issued earlier today we ask that you not use the Commerce contact information provided in that email. Instead, direct any questions or notifications of access to WikiLeaks documents to the NIST IT Assistance Center (iTAC).

iTAC  
IT Assistance Center  
itac@nist.gov

303-497-5375 (Boulder)  
301-975-5375 (Gaithersburg)

Hours of Operation:

Boulder: 7:30am - 5:30pm (Mountain Time) Monday - Friday  
Gaithersburg: 7:30am - 5:30pm (Eastern Time) Monday - Friday

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

From: allstaff@nist.gov [mailto:allstaff@nist.gov] On Behalf Of Broadcast, DOC  
Sent: Wednesday, December 01, 2010 11:11 AM



To: Multiple recipients of list  
Subject: Guidance regarding WikiLeaks

To: All Commerce Employees and Contractors

Recent reports indicate that a number of government documents have been posted on the WikiLeaks website. These documents may or may not contain information that is considered National Security Information (classified information) and as such, the information is NOT authorized for downloading, viewing, printing, processing, copying, or transmitting via non-classified Government-issued computers, laptops, blackberries, or other communication devices and is not an authorized use of DOC IT equipment. Doing so would introduce potentially classified information onto our unclassified networks and represent a potential security incident.

There has been a rumor that the information is no longer classified since it resides in the public domain. This is NOT true. Executive Order 13526, Section I.1(4)(2) states "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information." The information was neither properly nor improperly "declassified" by the appropriate authority and requires continued classification or reclassification.

Please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents because these documents may contain classified information. Accessing the WikiLeaks documents will lead to sanitization of your PC to remove any potentially classified information from the system and result in possible data loss.

If you have questions regarding this broadcast or have accessed the WikiLeaks documents, please contact the DOC Computer Incident Response Team at email [doc-cirt@doc.gov](mailto:doc-cirt@doc.gov) or call (202) 482-4000.

---

This message was authorized by the Office of Secretary OSY/OCIO.

Please do not reply to this message. The broadcast email account is not monitored for incoming mail.

**Subject:** Wikileak status (Updated 12/15)

**From:** "Beltz, John" <jbeltz@nist.gov>

**Date:** Wed, 15 Dec 2010 12:21:26 -0500

**To:** "Kustaborder, David P." <david.kustaborder@nist.gov>, "Sorensen, Robert" <robert.sorensen@nist.gov>

(b)(2) (b)(6) (b)(6)  
Contacted employee, trying to set a time:  
[redacted] (Windows) 933751 [redacted] 697

(b)(6) (b)(6) (b)(6)  
X [redacted] Left a message on voicemail. [redacted] called and left John a message at 3pm on 12/9/10. Called [redacted] back on 12/14, left vmail.

(b)(6) (b)(6) (b)(6)  
[redacted] (Windows) 931061 [redacted] 688

(b)(6) (b)(6)  
(email) [redacted]  
X [redacted] Left a message on voicemail on 12/8/10. Another vmail on 12/14. Left email as well on 12/14. [redacted] and I spoke, he will call me when leaving for the day. 12/15.

(b)(6) (b)(6) (b)(6)  
[redacted] (Windows) 933199 [redacted] 687

(b)(6) (b)(6)  
(email) [redacted]  
X [redacted] No answer? No voicemail available. Left email on NIST account and gmail account on 12/14. Started process 12/14, will complete 12/15.

(b)(2) (b)(6) (b)(6)  
Completed:  
[redacted] (Windows) 940819 [redacted] 194

(b)(6) (b)(6)  
(email) [redacted]  
X [redacted] Spoke with [redacted], anytime tomorrow, just call him before. Started Eraser on 12/9/10. Check back for completion. Completed by Robert on 12/10.

(b)(2) (b)(6) (b)(6)  
[redacted] (Windows) 930364 [redacted]

(b)(6) (b)(6)  
(student - POC: Dr. Thomas Bruno) 638  
X [redacted] Set a meeting for tomorrow at 9am. Started Eraser on 12/9/10. Check back for completion. Also need to follow up with the student when they return. Completed by Robert on 12/10.

(b)(2) (b)(6) (b)(6)  
[redacted] (Windows) 851068 [redacted] 653

(b)(6) (b)(6) (b)(6)  
X [redacted] Said anytime tomorrow.ok. Just call him. Complete!

(b)(2) (b)(6) (b)(6)  
[redacted] (Windows) XXX [redacted] 191

(b)(6) (b)(6)  
X [redacted] Left a message on voicemail. Scheduled for 10am on 12/14. Completed 12/14.

(b)(6) (b)(6) (b)(6)  
Non-Windows  
[redacted] ( [redacted] Box)  
Waiting for Instructions.

(b)(2) (b)(6)  
[redacted] (Mac).  
Waiting for instructions.

Loebach, Matthew T.

From: David Kustaborder [kusty@nist.gov]  
Sent: Wednesday, December 15, 2010 3:28 PM  
To: Glenn, K. Robert  
Cc: siirt  
Subject: wiki-status  
Attachments: wiki-contact.xls

FYI,

Below is the status from Boulder

Contacted employee, trying to set a time:

(b)(2) (b)(6)  
[redacted] (Windows) 933751 [redacted] 697  
X [redacted] Left a message on voicemail. [redacted] called and left John a message at 3pm on 12/9/10. Called [redacted] back on 12/14, left vmail. (b)(6)

(b)(2) (b)(6)  
[redacted] (Windows) 931061 [redacted] 688 (email)  
X [redacted] Left a message on voicemail on 12/8/10. Another vmail on 12/14. Left email as well on 12/14. [redacted] and I spoke, he will call me when leaving for the day. 12/15. (b)(2)

(b)(2) (b)(6)  
[redacted] (Windows) 933199 [redacted] 687 (email)  
X [redacted] No answer? No voicemail available. Left email on NIST account and gmail account on 12/14. Started process 12/14, will complete 12/15.

Completed:

(b)(2) (b)(6)  
[redacted] (Windows) 940819 [redacted] 194 (email)  
X [redacted] Spoke with [redacted] anytime tomorrow, just call him before. Started Eraser on 12/9/10. Check back for completion. Completed by Robert on 12/10. (b)(2)

(b)(2) (b)(6)  
[redacted] (Windows) 930364 [redacted] (student - POC: Dr. Thomas Bruno) 638

X [redacted] Set a meeting for tomorrow at 9am. Started Eraser on 12/9/10. Check back for completion. Also need to follow up with the student when they return. Completed by Robert on 12/10. (b)(2)

(b)(2) (b)(6)  
[redacted] (Windows) 851068 [redacted] 653  
X [redacted] Said anytime tomorrow ok. Just call him. Complete! (b)(2)

(b)(2) (b)(6)  
[redacted] (Windows) XXX [redacted] 191  
X [redacted] Left a message on voicemail. Scheduled for 10am on 12/14. Completed 12/14. (b)(2)

Non-Windows

(b)(2) (b)(6)  
[redacted] (Mac).  
Waiting for Instructions. (b)(2)

[redacted] (Mac).  
Waiting for instructions.

(b)(2) (b)(6) sheet1

Property Number	src	User	Division	Phone	(b)(6) Associate
634024	[REDACTED]	[REDACTED]		184	
631634	[REDACTED]	[REDACTED]		774	
	[REDACTED]	[REDACTED]		774	Y
629071	[REDACTED]	[REDACTED]		688	
931061	[REDACTED]	[REDACTED]		775	
624503	[REDACTED]	[REDACTED]		181	
934346	[REDACTED]	[REDACTED]		732	
631753	[REDACTED]	[REDACTED]		772	
634008	[REDACTED]	[REDACTED]		731	
851531	[REDACTED]	[REDACTED]		194	
940819	[REDACTED]	[REDACTED]		183	
850752	[REDACTED]	[REDACTED]		730	
612740	[REDACTED]	[REDACTED]		687	
933199	[REDACTED]	[REDACTED]		653	
851068	[REDACTED]	[REDACTED]		191	
	[REDACTED]	[REDACTED]		683	
623254	[REDACTED]	[REDACTED]		773	
629074	[REDACTED]	[REDACTED]		488	
621855	[REDACTED]	[REDACTED]		697	
940569	[REDACTED]	[REDACTED]		610	
624101	[REDACTED]	[REDACTED]		775	
631298	[REDACTED]	[REDACTED]		683	N
617030	[REDACTED]	[REDACTED]		470	E
633663	[REDACTED]	[REDACTED]		470	E
633683	[REDACTED]	[REDACTED]		682	E
612061	[REDACTED]	[REDACTED]		638	N
930364	[REDACTED]	[REDACTED]		688	E
933751	[REDACTED]	[REDACTED]		181	N
634222	[REDACTED]	[REDACTED]		771	E
635896	[REDACTED]	[REDACTED]		698	E
851511	[REDACTED]	[REDACTED]		684	E
634111	[REDACTED]	[REDACTED]		610	E
635565	[REDACTED]	[REDACTED]		620	E
850223	[REDACTED]	[REDACTED]		730	E
634570	[REDACTED]	[REDACTED]			

Sheet 1

Sanitized

Mac Safari

Complete

Linux Firefox

Complete

Complete

Complete

Complete

Complete

Complete

Complete

Complete

Complete

Complete

Complete

Complete

Windows Firefox

Linux Chrome

Windows IE

Complete

Complete

Complete

Complete

Students machine.

(b)(2)

Complete

In Progress

NetBSD mozilla

Complete

Complete

Complete

Re: Guidance regarding WikiLeaks

**Subject:** Re: Guidance regarding WikiLeaks  
**From:** David Kustaborder <kusty@nist.gov>  
**Date:** Thu, 16 Dec 2010 09:39:31 -0500  
**To:** "Long, Kathleen" <kathleen.long@nist.gov>

Sounds good I will give you a call tomorrow.

Thanks,

kusty

On 12/16/2010 09:19 AM, Long, Kathleen wrote:

I am working from home today, but will be there all day tomorrow.

Kathleen Long, CISSP  
Manufacturing Extension Partnership  
National Institute of Standards and Technology  
100 Bureau Drive, Stop 4800  
Gaithersburg, MD 20899  
Ph: 301-975-2474

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

From: David Kustaborder [mailto:kusty@nist.gov]  
Sent: Thursday, December 16, 2010 9:12 AM  
Cc: Long, Kathleen  
Subject: Re: Guidance regarding WikiLeaks

Kathy,

I am trying to coordinate with you and [redacted] to work on cleaning his machine. [redacted] said he is here till 12 today and around all day tomorrow. Would either of these days work for you?

Thanks,

kusty

On 12/06/2010 11:59 AM, Glenn, K. Robert wrote:

Kathy,

The MEP user has been contacted. Note, I was only able to contact him by email and do not have confirmation that they read the message. All others were contacted verbally. Here is the additional information.

621855 [redacted] [redacted] 488

It is important that this issue be treated delicately and that this information not spread nor used to embarrass the users and they should continue to be reassured that they will not be getting into any trouble over this as long as they continue to refrain from accessing wikileaks documentation.

SIIRT will be following up to schedule desanitization. OSY will be following up to give

them an inadvertent disclosure briefing.

Rob G.

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

From: [ou\\_secu@nist.gov](mailto:ou_secu@nist.gov) [mailto:[ou\\_secu@nist.gov](mailto:ou_secu@nist.gov)] On Behalf Of Glenn, K. Robert

Sent: Friday, December 03, 2010 8:09 AM

To: Multiple recipients of list

Subject: RE: Guidance regarding WikiLeaks

OU ITSOs,

In close consultation with the NIST Director's Office and DoC, we now have a plan to move forward for NIST computers that connected to wikileaks before blocks were implemented. I've included some details and highlights of the plan below; the technical work will be performed by SIIRT (and given that there are 36 computers involved, this could impact other priorities).

1) Notify users verbally that their computer has been identified as having accessed Wikileaks documentation and as a result, may have unknowingly accessed classified information. Users are re-assured that they are not in trouble over this as the access was done prior to DoC guidance being issued. The notification will also explain that over the next several days NIST OISM incident response staff will work with them to properly sanitize their computer. Until the sanitization is complete, users may continue using their computer, but they are not to access, read, or move any Wikileaks documentation downloaded to their computer. Users are also not to try to sanitize their own computers. Users will also be notified that DoC OSY will follow-up with them to provide an inadvertent disclosure briefing. Those with clearances may be asked (by OSY) to take refresher training.

> Status: Susannah and I started contacting users late yesterday afternoon and will try to complete this today.

2) Notify OU Directors and OU ITSOs that have affected computers in their OUs;

> Status: Del started contacting OU Directors late yesterday afternoon. This email is your initial notification. Once all users in your OU have been contacted, I will then send the relevant OU ITSO the list of their affected users/computers.

3) SIIRT to complete detailed analysis of network logs to prioritize the order for which computers will be sanitized. Computers that have accessed the site the most or downloaded the most documentation will be sanitized first.

4) For each computer to be sanitized SIIRT will schedule time with each user (in prioritized order) to:

a) Identify the browser used; for each browser, clear cache, history, temporary files, etc.

b) Verify if the user stored any downloaded files elsewhere (e.g., thumb drives, CDs, DVDs, backups, etc.). Verify that nothing was forwarded to other people via other methods such as email, IM, etc.

c) Delete all other files and completely erase all unused data sectors on all relevant media and hard disks.

d) Sanitize or destroy any mobile media or backup storage used to store Wikileaks documentation.

e) Document all steps performed, responses from the user to questions, and any errors that may arise during the procedure.

5) Notify DoC OCIO that clean up has been completed and that specific details are available as needed.

---

Note, that while the technical steps follow standard operating procedures for classified spillage clean-up, some aspects of the overall procedures (e.g. allowing users to continue using the computer) are only being done due to the massively public nature of the spillage. For more typically spillage incidents, the computer would be immediately removed from the network and sanitization would be immediate. For larger spillages, the hard drive would be removed, labeled, and stored in an approved container until the sanitization could be completed. The plan above was reviewed and approved by the Director's Office.

# of users/computers per OU (for OUs is not listed, there were no computers identified at this time):

OISM: 4 (1 in Boulder)  
OFPM: 2 (both in Boulder)  
TIP: 2  
MEP: 1  
NCNR: 2  
CNST: 1  
MML: 2 (both in Boulder)  
PML: 9 (4 in Boulder)  
EL: 4  
ITL: 9

Rob G.

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

From: [allstaff@nist.gov](mailto:allstaff@nist.gov) [<mailto:allstaff@nist.gov>] On Behalf Of NIST IT Assistance Center  
Sent: Wednesday, December 01, 2010 2:45 PM  
To: Multiple recipients of list  
Subject: RE: Guidance regarding WikiLeaks

Attention NIST Staff:

To clarify the guidance that the Department of Commerce issued earlier today we ask that you not use the Commerce contact information provided in that email. Instead, direct any questions or notifications of access to WikiLeaks documents to the NIST IT Assistance Center (iTAC).

iTAC  
IT Assistance Center  
[itac@nist.gov](mailto:itac@nist.gov)

303-497-5375 (Boulder)  
301-975-5375 (Gaithersburg)

Hours of Operation:  
Boulder: 7:30am - 5:30pm (Mountain Time) Monday - Friday  
Gaithersburg: 7:30am - 5:30pm (Eastern Time) Monday - Friday

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



From: [allstaff@nist.gov](mailto:allstaff@nist.gov) [mailto:[allstaff@nist.gov](mailto:allstaff@nist.gov)] On Behalf Of Broadcast, DOC  
Sent: Wednesday, December 01, 2010 11:11 AM  
To: Multiple recipients of list  
Subject: Guidance regarding WikiLeaks

To: All Commerce Employees and Contractors

Recent reports indicate that a number of government documents have been posted on the WikiLeaks website. These documents may or may not contain information that is considered National Security Information (classified information) and as such, the information is NOT authorized for downloading, viewing, printing, processing, copying, or transmitting via non-classified Government-issued computers, laptops, blackberries, or other communication devices and is not an authorized use of DOC IT equipment. Doing so would introduce potentially classified information onto our unclassified networks and represent a potential security incident.

There has been a rumor that the information is no longer classified since it resides in the public domain. This is NOT true. Executive Order 13526, Section I.1(4)(2) states "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information." The information was neither properly nor improperly "declassified" by the appropriate authority and requires continued classification or reclassification.

Please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents because these documents may contain classified information. Accessing the WikiLeaks documents will lead to sanitization of your PC to remove any potentially classified information from the system and result in possible data loss.

If you have questions regarding this broadcast or have accessed the WikiLeaks documents, please contact the DOC Computer Incident Response Team at email [doc-cirt@doc.gov](mailto:doc-cirt@doc.gov) or call (202) 482-4000.

---

This message was authorized by the Office of Secretary OSY/OCIO.

Please do not reply to this message. The broadcast email account is not monitored for incoming mail.

12-8-2010

[REDACTED]

[REDACTED]

(b)(6) (b)(2)

IP :

[REDACTED]

MAC :

PRIP #: 622177

BROWSER: FIREFOX

GO TO WEB SITE: YES

HOW DO YOU ACCESS SITE: ?

STORE ANY DOWNLOADED FILES: NO

INFO FORWARDED TO OTHER PEOPLE: NO

SMART CTL

Date and Time: 12/21/2010 (b)(6)  
Name: [REDACTED]  
IP Address: [REDACTED]  
MAC Address: [REDACTED]  
Property Number: 624161  
Browser Used: Fire Fox  
O/S: XP

1. Check if the above information matches the information on the user's PC.
2. Did you go to the web site: ✓
3. How did you access the site: Washingtonpost
4. Clear the cache: \_\_\_\_\_
5. Clear the history: \_\_\_\_\_
6. Clear temporary files: \_\_\_\_\_
7. Clear local copies of docs downloaded, such as "Page as" copies N/A
8. Did the user store any downloaded files elsewhere? N/A
9. Detail where the information was stored below.
10. Was any of the information forwarded to other people? N/A  
(i.e. Email, IM)
11. Detail what information was forwarded, and where it went.  
N/A
12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks.
13. Sanitize or destroy any mobile media or backup storage used
14. Remove SIIRT tools (after #12 is complete) – Eraser: <http://eraser.heidi.ie/>

Date and Time: 12-28-2010 (b)(6)  
Name: [REDACTED] [REDACTED] #6292  
IP Address: [REDACTED] (b)(6)  
MAC Address: [REDACTED]  
Property Number: P635565  
Browser Used: I.E.  
O/S: WINDOWS

1. Check if the above information matches the information on the user's PC.
2. Did you go to the web site: YES -
3. How did you access the site: VIA GOOGLE
4. Clear the cache: \_\_\_\_\_
5. Clear the history: \_\_\_\_\_
6. Clear temporary files: \_\_\_\_\_
7. Clear local copies of docs downloaded, such as "Page as" copies \_\_\_\_\_
8. Did the user store any downloaded files elsewhere? NO
9. Detail where the information was stored below. N/A
10. Was any of the information forwarded to other people? NO  
(i.e. Email, IM)
11. Detail what information was forwarded, and where it went. N/A
12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks.
13. Sanitize or destroy any mobile media or backup storage used
14. Remove SIIRT tools (after #12 is complete) – Eraser: <http://eraser.heidi.ie/>

Date and Time:

12/8/2010

(b)(6)

Name:

[REDACTED]

IP Address:

[REDACTED]

(b)(2)

MAC Address:

\_\_\_\_\_

Property Number:

622177

Browser Used:

Firefox

O/S:

XP

1. Check if the above information matches the information on the user's PC. ✓

2. Did you go to the web site: yes

3. How did you access the site: n/a

4. Clear the cache: ✓

5. Clear the history: ✓

6. Clear temporary files: \_\_\_\_\_

7. Clear local copies of docs downloaded, such as "Page as" copies n/a

8. Did the user store any downloaded files elsewhere? n/a

9. Detail where the information was stored below.

10. Was any of the information forwarded to other people? n/a

(i.e. Email, IM)

11. Detail what information was forwarded, and where it went.

12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks. ✓

13. Sanitize or destroy any mobile media or backup storage used

14. Remove SIIRT tools (after #12 is complete) – Eraser: <http://eraser.heidi.ie/>

Date and Time:

12/16/2010

(b)(1)(u)

Name:

[REDACTED]

[REDACTED]

IP Address:

[REDACTED]

MAC Address:

[REDACTED]

(b)(2)

Property Number:

\_\_\_\_\_

Browser Used:

FIREFOX

O/S:

LINUX

1. Check if the above information matches the information on the user's PC.

2. Did you go to the web site: ~~YAHOO~~ WEB SITE YES

3. How did you access the site: YAHOO WEB SITE

4. Clear the cache: \_\_\_\_\_

5. Clear the history: \_\_\_\_\_

6. Clear temporary files: \_\_\_\_\_

7. Clear local copies of docs downloaded, such as "Page as" copies \_\_\_\_\_

8. Did the user store any downloaded files elsewhere? NO

9. Detail where the information was stored below.

N/A

10. Was any of the information forwarded to other people? NO

(i.e. Email, IM)

N/A

11. Detail what information was forwarded, and where it went.

N/A

12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks.

13. Sanitize or destroy any mobile media or backup storage used

14. Remove SIIRT tools (after #12 is complete) – Eraser: <http://eraser.heidi.ie/>

Date and Time: 12/15/2010

Name: [REDACTED]

IP Address: [REDACTED]

MAC Address: [REDACTED]

Property Number: 617030

Browser Used: I.E.

O/S: WINDOWS

(b)(2)

1. Check if the above information matches the information on the user's PC.
2. Did you go to the web site: YES
3. How did you access the site: FROM GOOGLE
4. Clear the cache: \_\_\_\_\_
5. Clear the history: \_\_\_\_\_
6. Clear temporary files: \_\_\_\_\_
7. Clear local copies of docs downloaded, such as "Page as" copies \_\_\_\_\_

8. Did the user store any downloaded files elsewhere? NO

9. Detail where the information was stored below.

N/A

10. Was any of the information forwarded to other people? NO  
(i.e. Email, IM)

11. Detail what information was forwarded, and where it went.

N/A

12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks.

13. Sanitize or destroy any mobile media or backup storage used

14. Remove SIIRT tools (after #12 is complete) – Eraser: <http://eraser.heidi.ie/>



Date and Time:

12/17/2010

Name:

IP Address:

MAC Address:

Property Number:

621855

Browser Used:

Firefox

O/S:

XP

1. Check if the above information matches the information on the user's PC.

2. Did you go to the web site:

3. How did you access the site: dry news INC

4. Clear the cache:

5. Clear the history:

6. Clear temporary files:

7. Clear local copies of docs downloaded, such as "Page as" copies N/A

8. Did the user store any downloaded files elsewhere? N/A

9. Detail where the information was stored below.

10. Was any of the information forwarded to other people? N/A  
(i.e. Email, IM)

11. Detail what information was forwarded, and where it went.

12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks.

13. Sanitize or destroy any mobile media or backup storage used

14. Remove SIIRT tools (after #12 is complete) – Eraser: <http://eraser.heidi.ie/>

X3C85

Date and Time:

12/9/2010

Name:

[REDACTED] (b)(6)

IP Address:

[REDACTED] (b)(6)

[REDACTED]

MAC Address:

[REDACTED]

Property Number:

634008

Browser Used:

Firefox

O/S:

Windows

1. Check if the above information matches the information on the user's PC.
2. Did you go to the web site: Monday Morning
3. How did you access the site: Through a newspaper link
4. Clear the cache: \_\_\_\_\_
5. Clear the history: \_\_\_\_\_
6. Clear temporary files: \_\_\_\_\_
7. Clear local copies of docs downloaded, such as "Page as" copies \_\_\_\_\_

8. Did the user store any downloaded files elsewhere? NO

9. Detail where the information was stored below.

N/A

10. Was any of the information forwarded to other people? NO  
(i.e. Email, IM)

11. Detail what information was forwarded, and where it went.

N/A

12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks.

13. Sanitize or destroy any mobile media or backup storage used

14. Remove SIIRT tools (after #12 is complete) – Eraser: <http://eraser.heidi.ie/>

Date and Time:

12/8/2010

Name:

[REDACTED] (b)(6)

IP Address:

[REDACTED] (b)(6)

MAC Address:

[REDACTED]

Property Number:

624503

Browser Used:

IE.

O/S:

\_\_\_\_\_

1. Check if the above information matches the information on the user's PC.

2. Did you go to the web site: YES COUPLE OF WEEKS AGO

3. How did you access the site: THROUGH MSN OR CNN

4. Clear the cache: \_\_\_\_\_

5. Clear the history: \_\_\_\_\_

6. Clear temporary files: \_\_\_\_\_

7. Clear local copies of docs downloaded, such as "Page as" copies \_\_\_\_\_

8. Did the user store any downloaded files elsewhere? NO

9. Detail where the information was stored below.

N/A

10. Was any of the information forwarded to other people? NO  
(i.e. Email, IM)

11. Detail what information was forwarded, and where it went.

N/A

12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks.

13. Sanitize or destroy any mobile media or backup storage used

14. Remove SIIRT tools (after #12 is complete) – Eraser: <http://eraser.heidi.ie/>

Date and Time:

12/8/2010

Name:

[REDACTED] (b)(6)

IP Address:

[REDACTED] (b)(6)

MAC Address:

[REDACTED]

Property Number:

623254

Browser Used:

I.E.

O/S:

WINDOWS

1. Check if the above information matches the information on the user's PC.

2. Did you go to the web site: YES

3. How did you access the site: LINK FROM THE NEW YORK TIMES

4. Clear the cache: \_\_\_\_\_

5. Clear the history: \_\_\_\_\_

6. Clear temporary files: \_\_\_\_\_

7. Clear local copies of docs downloaded, such as "Page as" copies \_\_\_\_\_

8. Did the user store any downloaded files elsewhere? NO

9. Detail where the information was stored below.

N/A

10. Was any of the information forwarded to other people? NO  
(i.e. Email, IM)

11. Detail what information was forwarded, and where it went.

N/A

12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks.

13. Sanitize or destroy any mobile media or backup storage used

14. Remove SIIRT tools (after #12 is complete) – Eraser: <http://eraser.heidi.ie/>

Date and Time:

12/7/2010

Name:

IP Address:

MAC Address:

Property Number:

612061

Browser Used:

Firefox

O/S:

Windows XP

1. Check if the above information matches the information on the user's PC.

2. Did you go to the web site: YES

3. How did you access the site: THROUGH BBC WEBSITE

4. Clear the cache:

5. Clear the history:

6. Clear temporary files:

7. Clear local copies of docs downloaded, such as "Page as" copies

8. Did the user store any downloaded files elsewhere? NO

9. Detail where the information was stored below.

N/A

10. Was any of the information forwarded to other people? NO

(i.e. Email, IM)

N/A

11. Detail what information was forwarded, and where it went.

N/A

12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks.

13. Sanitize or destroy any mobile media or backup storage used

14. Remove SIIRT tools (after #12 is complete) – Eraser: <http://eraser.heidi.ie/>

Date and Time:

12/8/2010

Name:

IP Address:

MAC Address:

Property Number:

856223

Browser Used:

Firefox And I.E.

O/S:

1. Check if the above information matches the information on the user's PC.

2. Did you go to the web site:

YES

3. How did you access the site:

LINK FROM THE NY TIMES

4. Clear the cache:

5. Clear the history:

6. Clear temporary files:

7. Clear local copies of docs downloaded, such as "Page as" copies

8. Did the user store any downloaded files elsewhere?

NO

9. Detail where the information was stored below.

N/A

10. Was any of the information forwarded to other people?

NO

(i.e. Email, IM)

11. Detail what information was forwarded, and where it went.

N/A

12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks.

13. Sanitize or destroy any mobile media or backup storage used

14. Remove SIIRT tools (after #12 is complete) – Eraser: <http://eraser.heidi.ie/>

Date and Time: 12/6/2010  
Name: [REDACTED]  
IP Address: [REDACTED]  
MAC Address: [REDACTED]  
Property Number: 612740  
Browser Used: ~~FIREFOX~~ IE  
O/S: WINDOWS

1. Check if the above information matches the information on the user's PC.
2. Did you go to the web site: YES
3. How did you access the site: FROM A LINK ON A NEWSPAPER WEBSITE
4. Clear the cache: \_\_\_\_\_
5. Clear the history: \_\_\_\_\_
6. Clear temporary files: \_\_\_\_\_
7. Clear local copies of docs downloaded, such as "Page as" copies \_\_\_\_\_

8. Did the user store any downloaded files elsewhere? NO

9. Detail where the information was stored below.

N/A

10. Was any of the information forwarded to other people? NO  
(i.e. Email, IM)

11. Detail what information was forwarded, and where it went.

N/A

12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks.

13. Sanitize or destroy any mobile media or backup storage used

14. Remove SIIRT tools (after #12 is complete) – Eraser: <http://eraser.heidi.ie/>

Date and Time:

12/7/2010

226

Name:

IP Address:

MAC Address:

Property Number:

631753

Browser Used:

FIREFOX

O/S:

WINDOWS

1. Check if the above information matches the information on the user's PC.

2. Did you go to the web site: YES

3. How did you access the site: ENTERED IT IN DIRECTLY

4. Clear the cache: \_\_\_\_\_

5. Clear the history: \_\_\_\_\_

6. Clear temporary files: \_\_\_\_\_

7. Clear local copies of docs downloaded, such as "Page as" copies \_\_\_\_\_

8. Did the user store any downloaded files elsewhere? NO

9. Detail where the information was stored below.

N/A

10. Was any of the information forwarded to other people? NO  
(i.e. Email, IM)

11. Detail what information was forwarded, and where it went.

N/A

12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks.

13. Sanitize or destroy any mobile media or backup storage used

14. Remove SIIRT tools (after #12 is complete) – Eraser: <http://eraser.heidi.ie/>



Date and Time:

12/7/2010

Name:

IP Address:

MAC Address:

Property Number:

851531

Browser Used:

Firefox

O/S:

XP Sp3

Browser was setup w/  
Private Browsing Session

1. Check if the above information matches the information on the user's PC.

2. Did you go to the web site: YES

3. How did you access the site: LDN1K FROM A NEWS WEBSITE

4. Clear the cache: \_\_\_\_\_

5. Clear the history: \_\_\_\_\_

6. Clear temporary files: \_\_\_\_\_

7. Clear local copies of docs downloaded, such as "Page as" copies \_\_\_\_\_

8. Did the user store any downloaded files elsewhere? NO

9. Detail where the information was stored below.

N/A

10. Was any of the information forwarded to other people? NO

(i.e. Email, IM)

N/A

11. Detail what information was forwarded, and where it went.

N/A

12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks.

13. Sanitize or destroy any mobile media or backup storage used

14. Remove SIIRT tools (after #12 is complete) – Eraser: <http://eraser.heidi.ie/>

Date and Time: 12/7/2010 (b)(6)  
Name: [REDACTED]  
IP Address: [REDACTED] (b)(6)  
MAC Address: [REDACTED]  
Property Number: 633683  
Browser Used: I.E. or Firefox  
O/S: WINDOWS

1. Check if the above information matches the information on the user's PC.
2. Did you go to the web site: 11-30-2010
3. How did you access the site: THROUGH GOOGLE
4. Clear the cache: \_\_\_\_\_
5. Clear the history: \_\_\_\_\_
6. Clear temporary files: \_\_\_\_\_
7. Clear local copies of docs downloaded, such as "Page as" copies \_\_\_\_\_

8. Did the user store any downloaded files elsewhere? NO

9. Detail where the information was stored below.

N/A

10. Was any of the information forwarded to other people? NO  
(i.e. Email, IM)

11. Detail what information was forwarded, and where it went.

N/A

12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks.

13. Sanitize or destroy any mobile media or backup storage used

14. Remove SIIRT tools (after #12 is complete) – Eraser: <http://eraser.heidi.ie/>

Date and Time:

12/7/2010

Name:

[REDACTED]

IP Address:

[REDACTED]

MAC Address:

[REDACTED]

Property Number:

633663

Browser Used:

1

O/S:

I.E.

1. Check if the above information matches the information on the user's PC.

2. Did you go to the web site: YES 11-2-2010

3. How did you access the site: ENTERED IN THE URL

4. Clear the cache: \_\_\_\_\_

5. Clear the history: \_\_\_\_\_

6. Clear temporary files: \_\_\_\_\_

7. Clear local copies of docs downloaded, such as "Page as" copies \_\_\_\_\_

8. Did the user store any downloaded files elsewhere? NO

9. Detail where the information was stored below.

N/A

10. Was any of the information forwarded to other people? NO  
(i.e. Email, IM)

11. Detail what information was forwarded, and where it went.

N/A

12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks.

13. Sanitize or destroy any mobile media or backup storage used

14. Remove SIIRT tools (after #12 is complete) – Eraser: <http://eraser.heidi.ie/>

Date and Time:

12/4/2010

Name:

[REDACTED]

IP Address:

[REDACTED]

MAC Address:

[REDACTED]

Property Number:

634570

Browser Used:

IE

O/S:

XP Sp3

(P)(6)  
(b)(2)

1. Check if the above information matches the information on the user's PC.

2. Did you go to the web site: yes

3. How did you access the site: Googled it

4. Clear the cache: yes

5. Clear the history: yes

6. Clear temporary files: yes

7. Clear local copies of docs downloaded, such as "Page as" copies N/A

8. Did the user store any downloaded files elsewhere? N/A

9. Detail where the information was stored below.

N/A

10. Was any of the information forwarded to other people? N/A

(i.e. Email, IM)

11. Detail what information was forwarded, and where it went. N/A

12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks.

13. Sanitize or destroy any mobile media or backup storage used

14. Remove SIIRT tools (after #12 is complete) – Eraser: <http://eraser.heidi.ie/>

Date and Time: 12/3/2010

✓ Name: [REDACTED] (b)(6)

✓ IP Address: [REDACTED] (b)(2)

✓ MAC Address: [REDACTED]

✓ Property Number: 050752

Browser Used: FIREFOX

O/S: WINDOWS

1. Check if the above information matches the information on the user's PC.

2. Did you go to the web site: YES

3. How did you access the site: FRONT PAGE

4. Clear the cache: 16:02

5. Clear the history: 16:02

6. Clear temporary files: WINDOWS / TEMP; DOCS AND SETTINGS / LOCAL SETTINGS / TEMP

7. Clear local copies of docs downloaded, such as "Page as" copies N/A

8. Did the user store any downloaded files elsewhere? NO

9. Detail where the information was stored below.

N/A

10. Was any of the information forwarded to other people? NO  
(i.e. Email, IM)

11. Detail what information was forwarded, and where it went.

N/A

12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks.

13. Sanitize or destroy any mobile media or backup storage used

14. Remove SIIRT tools (after #12 is complete) – Eraser: <http://eraser.heidi.ie/>

Date and Time: 12-3-10 14:49:45

Name: [REDACTED]

✓ IP Address: [REDACTED] (b)(2) [REDACTED] (b)(6)

✓ MAC Address: [REDACTED]

Property Number: 629071

Browser Used: ? → 4 Browsers

I.E. - NO USED

FIREFOX -

CHROME -

O/S: WINDOWS

WYZO (WYZO) -

1. Check if the above information matches the information on the user's PC.

2. Did you go to the web site: YES

3. How did you access the site: HOME PAGE ACCESSED

4. Clear the cache: FIREFOX, CHROME, WYZO

5. Clear the history: FIREFOX, CHROME, WYZO

6. Clear temporary files: ERASED FILES IN C:\WINDOWS\TEMP

7. Clear local copies of docs downloaded, such as "Page as" copies

RAN CCLEANER AT: 14:52

RAN ERASER AT 14:57

8. Did the user store any downloaded files elsewhere? NO

9. Detail where the information was stored below.

N/A

10. Was any of the information forwarded to other people? NO  
(i.e. Email, IM)

11. Detail what information was forwarded, and where it went.

N/A

12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks.

13. Sanitize or destroy any mobile media or backup storage used

14. Remove SIIRT tools (after #12 is complete) - Eraser: <http://eraser.heidi.ie/>

CCLEANER.COM

Date and Time:

12/3/2010 3:42

Name:

[REDACTED]

IP Address:

[REDACTED]

MAC Address:

[REDACTED]

Property Number:

634222

Browser Used:

Firefox

O/S:

XP

(b)(6)  
(b)(2)

1. Check if the above information matches the information on the user's PC.
2. Did you go to the web site: Yes
3. How did you access the site: via Firefox no download.
4. Clear the cache: ✓
5. Clear the history: ✓
6. Clear temporary files: ✓
7. Clear local copies of docs downloaded, such as "Page as" copies \_\_\_\_\_
8. Did the user store any downloaded files elsewhere? no
9. Detail where the information was stored below.
10. Was any of the information forwarded to other people? \_\_\_\_\_  
(i.e. Email, IM)
11. Detail what information was forwarded, and where it went.
12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks.
13. Sanitize or destroy any mobile media or backup storage used
14. Remove SIIRT tools (after #12 is complete) – Eraser: <http://eraser.heidi.ie/>

Name:

IP Address:

MAC Address:

Property Number:

Browser Used:

63/634

mozilla / firefox Applewebkit Chrome Safari

OS: XP on Linux RH (vmware)

1. Check if the above information matches the information on the user's PC.

2. Did you go to the web site:

yes

3. How did you access the site:

chrome - no download

4. Clear the cache:

5. Clear the history:

6. Clear temporary files:

7. Clear local copies of docs downloaded, such as "Page as" copies

N/A

8. Did the user store any downloaded files elsewhere?

no

9. Detail where the information was stored below.

10. Was any of the information forwarded to other people?

(i.e. Email, IM)

no

11. Detail what information was forwarded, and where it went.

12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks.

13. Sanitize or destroy any mobile media or backup storage used

14. Remove SIIRT tools (after #12 is complete) - Eraser: <http://eraser.heidi.ie/>



Date and Time: 12/2/10 8:42m

Name: [REDACTED]

IP Address: [REDACTED]

MAC Address: [REDACTED]

Property Number: 940569

Browser Used: Firefox

O/S: [REDACTED]

1. Check if the above information matches the information on the user's PC.

2. Did you go to the web site:

yes

3. How did you access the site:

Firefox

4. Clear the cache:

yes

5. Clear the history:

yes

6. Clear temporary files:

yes

7. Clear local copies of docs downloaded, such as "Page as" copies yes

8. Did the user store any downloaded files elsewhere?

NO

9. Detail where the information was stored below.

N/A

10. Was any of the information forwarded to other people?

NO (i.e. Email, IM)

11. Detail what information was forwarded, and where it went.

N/A

12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks.

N/A

13. Sanitize or destroy any mobile media or backup storage used

N/A

14. Remove SIIRT tools (after #12 is complete) - Eraser: <http://eraser.heidi.ie/>

Followed Mac Procedures

Date and Time:

Dec 17, 2016 1:47pm

Name:

IP Address:

MAC Address:

Property Number:

931061

Browser Used:

Firefox / check IE.

O/S:

XP.

1. Check if the above information matches the information on the user's PC.

2. Did you go to the web site: Yes

3. How did you access the site: News Link

4. Clear the cache: Done

5. Clear the history: Done

6. Clear temporary files: Done

7. Clear local copies of docs downloaded, such as "Page as" copies Done

8. Did the user store any downloaded files elsewhere? No

9. Detail where the information was stored below. N/A

10. Was any of the information forwarded to other people? N/A  
(i.e. Email, IM)

11. Detail what information was forwarded, and where it went. N/A

12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks.

13. Sanitize or destroy any mobile media or backup storage used

14. Remove SIIRT tools (after #12 is complete) – Eraser: <http://eraser.heidi.ie/>

12/20 9:45 am verified

Date and Time: \_\_\_\_\_

Name: \_\_\_\_\_

IP Address: \_\_\_\_\_

MAC Address: \_\_\_\_\_

Property Number: \_\_\_\_\_

Browser Used: \_\_\_\_\_

O/S: \_\_\_\_\_

1. Check if the above information matches the information on the user's PC.

2. Did you go to the web site:

3. How did you access the site:

4. Clear the cache:

5. Clear the history:

6. Clear temporary files:

7. Clear local copies of docs downloaded, such as "Page as" copies

8. Did the user store any downloaded files elsewhere?

9. Detail where the information was stored below.

10. Was any of the information forwarded to other people?  
\_\_\_\_\_ (i.e. Email, IM)

11. Detail what information was forwarded, and where it went.

12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks.

13. Sanitize or destroy any mobile media or backup storage used

14. Remove SIIRT tools (after #12 is complete) - Eraser: <http://eraser.heidi.ie/>

[Zachary Johnson]  
C1-3536A

- b(2)

3083 D

12/23 7:57

Date and Time: December 9, 2010 9:55am

Name: Dr Bruno (Care of ....) [REDACTED]

IP Address: [REDACTED] (b)(6)(b)(7)(C)

MAC Address: [REDACTED] (b)(2)

Property Number: 930-364

Browser Used: Firefox or IE (Cleared both)

O/S: Windows XP Professional

User not available

1. Check if the above information matches the information on the user's PC.
2. Did you go to the web site: \_\_\_\_\_
3. How did you access the site: \_\_\_\_\_
4. Clear the cache: Cleared from IE and Firefox
5. Clear the history: Same
6. Clear temporary files: Same
7. Clear local copies of docs downloaded, such as "Page as" copies N/A

8. Did the user store any downloaded files elsewhere? User Not Available

9. Detail where the information was stored below.

10. Was any of the information forwarded to other people? User Not Available  
(i.e. Email, IM)

11. Detail what information was forwarded, and where it went.

See Above.

12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks.

State Eraser Per Instructions.

Running 12/9/10

13. Sanitize or destroy any mobile media or backup storage used

14. Remove SIIRT tools (after #12 is complete) – Eraser: <http://eraser.heidi.ie/>

12/10/10 10:33am [Signature]

Airspeed computer.

(b)(6) (b)(7)(C)  
**Subject:** [REDACTED] computer.

**From:** [REDACTED] <[REDACTED]@nist.gov>

**Date:** Mon, 13 Dec 2010 15:37:45 -0500

**To:** "Kustaborder, David P." <david.kustaborder@nist.gov>

Hi David,

I am back from vacation and expecting your call to schedule the time to sanitize [REDACTED] lab computer. This week my time is rather flexible, so please let me know what time is convenient for you.

(b)(6) (b)(7)(C)  
[REDACTED]  
(301) 975-[REDACTED] (b)(6)  
Process Measurements Division (836), Fluid Metrology Group.

[REDACTED] (b)(6) (b)(7)(C)  
NIST

100 Bureau Drive, Stop 8361 (b)(2)

Gaithersburg, MD 20899-8361

Email(w): [iosif.shinder@nist.gov](mailto:iosif.shinder@nist.gov)

Wikileaks status and files (Updated) 12-14-10 8am.txt

From: Beltz, John  
Sent: Tuesday, December 14, 2010 8:08 AM  
To: Beltz, John; Sorensen, Robert  
Subject: Wikileaks status and files (Updated)

Scheduled:

(b)(6) (b)(6) (Windows) XXX (b)(6) 191

X (b)(6) Left a message on voicemail. Scheduled for 10am on 12/14.

(b)(6) contacted, trying to set a time: (b)(2)

(b)(6) (b)(6) (Windows) 933751 (b)(6) 697

(b)(6) X (b)(6) Left a message on voicemail. Dan called and left John a message at 3pm on 12/9/10. Called dan back on 12/14, left vmail.

Have left vmails, no return:

(b)(6) (b)(6) (Windows) 931061 (b)(6) 688

(b)(6) (email) 7691 (b)(2)

(b)(6) X (b)(6) Left a message on voicemail on 12/8/10. Another vmail on 12/14. Left email as well on 12/14. (b)(6)

(b)(6) (b)(6) (Windows) 933199 (b)(6) 687

(b)(6) (email) (b)(6)

(b)(6) X (b)(6) No answer? No voicemail available. Left email on NIST account and gmail account on 12/14.

Non-Windows (b)(2) (b)(6)

(b)(6) (b)(6) Box)

Waiting for Instructions.

(b)(6) (b)(2) (Mac).

Waiting for instructions.

Completed:

(b)(6) (b)(2) (b)(6) (Windows) 940819 (b)(6) 194

(b)(6) (email) (b)(2)

(b)(6) X (b)(6) Spoke with (b)(6), anytime tomorrow, just call him before. Started Eraser on 12/9/10. Check back for completion. Completed by Robert on 12/10.

(b)(6) (b)(2) (b)(6) (Windows) 930364 (b)(6)

(b)(6) (student - POC: Dr. Thomas Bruno) 638

(b)(6) X (b)(6) Set a meeting for tomorrow at 9am. Started Eraser on 12/9/10. Check back for completion. Also need to follow up with the student when they return. Completed by Robert on 12/10.

(b)(6) (b)(6) (Windows) 851068 (b)(6) 653

(b)(6) X (b)(2) Said anytime tomorrow ok. Just call him. Complete! (b)(6)

Date and Time:

12/8/2010

Name:

IP Address:

MAC Address:

Property Number:

628948

Browser Used:

FIREFOX

O/S:

1. Check if the above information matches the information on the user's PC.

2. Did you go to the web site: YES

3. How did you access the site: LINK FROM CNN

4. Clear the cache:

5. Clear the history:

6. Clear temporary files:

7. Clear local copies of docs downloaded, such as "Page as" copies

8. Did the user store any downloaded files elsewhere?

NO

9. Detail where the information was stored below.

N/A

10. Was any of the information forwarded to other people?

(i.e. Email, IM)

NO

N/A

11. Detail what information was forwarded, and where it went.

N/A

12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks.

13. Sanitize or destroy any mobile media or backup storage used

14. Remove SIIRT tools (after #12 is complete) – Eraser: <http://eraser.heidi.ie/>

OverclockMsgVb.exe

A21 A111



Date and Time: 12/15/2010 (b)(6)  
Name: [REDACTED] (b)(6)  
IP Address: [REDACTED] Multi User  
MAC Address: [REDACTED] They log in as (b)(6)  
Property Number: 851511  
Browser Used: IE  
O/S: \_\_\_\_\_

1. Check if the above information matches the information on the user's PC.
2. Did you go to the web site: yes
3. How did you access the site: clicked a link
4. Clear the cache: ✓
5. Clear the history: ✓
6. Clear temporary files: ✓
7. Clear local copies of docs downloaded, such as "Page as" copies N/A
8. Did the user store any downloaded files elsewhere? N/A
9. Detail where the information was stored below.  
N/A
10. Was any of the information forwarded to other people? N/A  
(i.e. Email, IM)
11. Detail what information was forwarded, and where it went.  
N/A
12. Delete all other files, and completely erase all unused sectors on all relevant media and hard disks.
13. Sanitize or destroy any mobile media or backup storage used
14. Remove SIIRT tools (after #12 is complete) – Eraser: <http://eraser.heidi.ie/>

pw

(b)(6) 4

(b)(6) & (b)(7)(c)

Bequester's cc

All redactions (b) (6) unless  
indicated otherwise

[REDACTED] (b) (6) and (b) (7) (C)

---

**From:** [REDACTED]  
**Sent:** Wednesday, December 01, 2010 8:37 AM  
**To:** [REDACTED] (b) (6) and (b) (7) (C)  
**Subject:** Computer

You have it, right.

[REDACTED]  
Office of the Inspector General  
U.S. Department of Commerce  
Washington DC  
202.482. [REDACTED]

all redactions (b) (6) unless  
otherwise indicated

[REDACTED] (b) (6) and (b) (7) (C)

---

**From:** [REDACTED] (b) (6) and (b) (7)  
**Sent:** Wednesday, December 01, 2010 8:38 AM  
**To:** [REDACTED]  
**Subject:** Re: Computer

Your computer? No  
Sent from my BlackBerry

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

**From:** [REDACTED]  
**To:** [REDACTED] (b) (6) and (b) (7) (C)  
**Sent:** Wed Dec 01 08:36:44 2010  
**Subject:** Computer

You have it, right.

[REDACTED]  
[REDACTED]  
Office of the Inspector General  
U.S. Department of Commerce  
Washington DC  
202.482. [REDACTED]

All redactions (b) (6) unless  
otherwise indicated

[REDACTED] (b) (6) and (b) (7) (C)

---

**From:** [REDACTED]  
**Sent:** Wednesday, December 01, 2010 9:10 AM  
**To:** [REDACTED] (b) (6) and (b) (7) (C)  
**Subject:** Re: Computer

OIG IT has it. They will deliver to you.

[REDACTED]  
Legislative and Public Affairs  
Office of the Inspector General  
U.S. Department of Commerce  
Washington DC  
202.482.6108

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

**From:** [REDACTED] (b) (6) and (b) (7) (C)  
**To:** [REDACTED]  
**Sent:** Wed Dec 01 08:38:20 2010  
**Subject:** Re: Computer

Your computer? No  
Sent from my BlackBerry

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

**From:** [REDACTED]  
**To:** [REDACTED] (b) (6) and (b) (7) (C)  
**Sent:** Wed Dec 01 08:36:44 2010  
**Subject:** Computer

You have it, right.

[REDACTED]  
Office of the Inspector General  
U.S. Department of Commerce  
Washington DC  
202.482. [REDACTED]

All redactions (b) (6) and (b) (7) (C) unless  
otherwise indicated

[REDACTED]

**From:** (b) (6) [REDACTED]  
**Sent:** Wednesday, December 01, 2010 9:11 AM  
**To:** (b) (6) [REDACTED]  
**Subject:** My computer

(b) (6) [REDACTED], [REDACTED] has agreed to wipe my computer. [REDACTED] is in room [REDACTED].

[REDACTED]

(b) (6)

Office of the Inspector General  
U.S. Department of Commerce  
Washington DC  
202.482. [REDACTED] (b) (6)

all redactions (b) (6) unless otherwise indicated

[REDACTED]  
**From:**

**Sent:** Wednesday, December 01, 2010 9:11 AM

**To:** [REDACTED] (b) (6) and (b) (7) (C)

**Subject:** My computer

(b) (6) and (b) (7) (C)

(b) (6) and (b) (7) (C)

[REDACTED], [REDACTED] has agreed to wipe my computer. [REDACTED] is in room [REDACTED].

(b) (6) and (b) (7) (C)

[REDACTED]  
Office of the Inspector General  
U.S. Department of Commerce  
Washington DC  
202.482. [REDACTED]

all redactions (b) (6) unless otherwise indicated

[REDACTED]

---

**From:** [REDACTED]  
**Sent:** Wednesday, December 01, 2010 9:10 AM  
**To:** [REDACTED] (b) (6) and (b) (7) (C)  
**Subject:** Re: Computer

OIG IT has it. They will deliver to you.

[REDACTED]  
Office of the Inspector General  
U.S. Department of Commerce  
Washington DC  
202.482. [REDACTED]

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

**From:** [REDACTED] (b) (6) and (b) (7) (C)  
**To:** [REDACTED]  
**Sent:** Wed Dec 01 08:38:20 2010  
**Subject:** Re: Computer

Your computer? No  
Sent from my BlackBerry

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

**From:** [REDACTED]  
**To:** [REDACTED] (b) (6) and (b) (7) (C)  
**Sent:** Wed Dec 01 08:36:44 2010  
**Subject:** Computer

You have it, right.

[REDACTED]  
Office of the Inspector General  
U.S. Department of Commerce  
Washington DC  
202.482. [REDACTED]



all redactions (b) (6) unless otherwise indicated

[REDACTED]

---

**From:** [REDACTED]  
**Sent:** Wednesday, December 01, 2010 8:37 AM  
**To:** [REDACTED] (b) (6) and (b) (7) (C)  
**Subject:** Computer

You have it, right.

[REDACTED]

Office of the Inspector General  
U.S. Department of Commerce  
Washington DC  
202.482. [REDACTED]

[REDACTED] (b) (6)

**From:** [REDACTED]  
**Sent:** Wednesday, December 01, 2010 11:01 AM  
**To:** [REDACTED] (b) (6)  
**Subject:** FW: Guidance regarding WikiLeaks

Hmmm, do you know anything about this? :)

[REDACTED]  
Special Agent  
Computer Crimes  
United States Department of Commerce  
Office of Inspector General  
1401 Constitution Ave., NW [REDACTED]  
Washington, DC 20230  
(202) 482-[REDACTED] (Office)  
(202) 437-[REDACTED] (Cell)  
(202) 482-[REDACTED] (Fax)

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

**From:** Broadcast, DOC [mailto:broadcast@doc.gov]  
**Sent:** Wednesday, December 01, 2010 10:57 AM  
**To:** Broadcast, DOC  
**Subject:** Guidance regarding WikiLeaks

refer to  
Dept

**To:** All Commerce Employees and Contractors

Recent reports indicate that a number of government documents have been posted on the WikiLeaks website. These documents may or may not contain information that is considered National Security Information (classified information) and as such, the information is NOT authorized for downloading, viewing, printing, processing, copying, or transmitting via non-classified Government-issued computers, laptops, blackberries, or other communication devices and is not an authorized use of DOC IT equipment. Doing so would introduce potentially classified information onto our unclassified networks and represent a potential security incident.

There has been a rumor that the information is no longer classified since it resides in the public domain. This is NOT true. Executive Order 13526, Section I.1(4)(2) states "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information." The information was neither properly nor improperly "declassified" by the appropriate authority and requires continued classification or reclassification.

Please do not attempt to access any of the WikiLeaks documents via the WikiLeaks website or through other websites hosting those documents because these documents may contain classified information. Accessing the WikiLeaks documents will lead to sanitization of your PC to remove any potentially classified information from the system and result in possible data loss.

If you have questions regarding this broadcast or have accessed the WikiLeaks documents, please contact the DOC Computer Incident Response Team at email [doc-cirt@doc.gov](mailto:doc-cirt@doc.gov) or call (202) 482-4000.

refer to  
Dept

This message was authorized by the Office of Secretary OSY/OCIO.

Please do not reply to this message. The broadcast email account is not monitored for incoming mail.

[REDACTED]

---

**From:** [REDACTED]  
**Sent:** Wednesday, December 01, 2010 8:54 AM  
**To:** [REDACTED]  
**Subject:** My computer

(b) (6) and (b) (7) (C)

Is gone but [REDACTED] ofc doesn't have it. Do you know where it is?

[REDACTED]  
Office of the Inspector General  
U.S. Department of Commerce  
Washington DC  
202.482. [REDACTED]

(b) (6)

**From:** [REDACTED]  
**Sent:** Wednesday, December 01, 2010 11:01 AM  
**To:** [REDACTED] (b) (6)  
**Subject:** FW: Guidance regarding WikiLeaks

Hmmm, do you know anything about this? :)

[REDACTED]  
Special Agent  
Computer Crimes  
United States Department of Commerce  
Office of Inspector General  
1401 Constitution Ave., NW [REDACTED]  
Washington, DC 20230  
(202) 482-[REDACTED] (Office)  
(202) 437-[REDACTED] (Cell)  
(202) 482-[REDACTED] (Fax)

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

**From:** Broadcast, DOC [mailto:broadcast@doc.gov]  
**Sent:** Wednesday, December 01, 2010 10:57 AM  
**To:** Broadcast, DOC  
**Subject:** Guidance regarding WikiLeaks

refer to  
Dept

**To:** All Commerce Employees and Contractors

Recent reports indicate that a number of government documents have been posted on the WikiLeaks website. These documents may or may not contain information that is considered National Security Information (classified information) and as such, the information is NOT authorized for downloading, viewing, printing, processing, copying, or transmitting via non-classified Government-issued computers, laptops, blackberries, or other communication devices and is not an authorized use of DOC IT equipment. Doing so would introduce potentially classified information onto our unclassified networks and represent a potential security incident.

There has been a rumor that the information is no longer classified since it resides in the public domain. This is NOT true. Executive Order 13526, Section I.1(4)(2) states "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information." The information was neither properly nor improperly "declassified" by the appropriate authority and requires continued classification or reclassification.

Please do not attempt to access any of the Wikileaks documents via the Wikileaks website or through other websites hosting those documents because these documents may contain classified information. Accessing the Wikileaks documents will lead to sanitization of your PC to remove any potentially classified information from the system and result in possible data loss.

If you have questions regarding this broadcast or have accessed the Wikileaks documents, please contact the DOC Computer Incident Response Team at email [doc-cirt@doc.gov](mailto:doc-cirt@doc.gov) or call (202) 482-4000.

refer to  
Dept

This message was authorized by the Office of Secretary OSY/OCIO.

Please do not reply to this message. The broadcast email account is not monitored for incoming mail.

PW

(b)(2); (b)(6);

& (b)(6) and (b)(7)(C)

Requester's cc

all redactions (b) (6) unless otherwise indicated

(b) (6) and (b) (7) (C)

**From:** (b) (6) and (b) (7) (C)  
**Sent:** Thursday, December 02, 2010 10:56 AM  
**To:** (b) (6) and (b) (7) (C)  
**Cc:** Berenberg, Scott  
**Subject:** RE: My computer

(b) (2)

(b) (2)

(b) (2)

I have forensically wiped both hard drives, (b) (6) and (b) (7) (C), from (b) (6) and (b) (7) (C), and verified that the wipe was successful for the physical devices.

The computer can be picked up from the lab anytime today.

(b) (6) and (b) (7) (C)

Special Agent  
Computer Crimes  
United States Department of Commerce  
Office of Inspector General  
1401 Constitution Ave., NW (b) (6) and (b) (7) (C)  
Washington, DC 20230  
(202) 482- (b) (6) and (b) (7) (C) (Office)  
(202) 437- (b) (6) and (b) (7) (C) (Cell)  
(202) 482- (b) (6) and (b) (7) (C) (Fax)

(b) (6) and (b) (7) (C)

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

(b) (6) and  
(b) (7) (C)

**From:** (b) (6) and (b) (7) (C)  
**Sent:** Wednesday, December 01, 2010 9:52 AM  
**To:** (b) (6) and (b) (7) (C)  
**Cc:** (b) (6) and (b) (7) (C); (b) (6) and (b) (7) (C)  
**Subject:** RE: My computer

Thanks. On my way

Office of the Chief Information Officer  
Office of Inspector General  
U.S. Department of Commerce  
(202) 482- (b) (6) and (b) (7) (C) office  
(202) 680- (b) (6) and (b) (7) (C) cell  
(202) 501- (b) (6) and (b) (7) (C) or (202) 482- (b) (6) and (b) (7) (C) fax  
(b) (6) and (b) (7) (C) @oig.doc.gov

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

**From:** (b) (6) and (b) (7) (C)  
**Sent:** Wednesday, December 01, 2010 9:11 AM  
**To:** (b) (6) and (b) (7) (C); (b) (6) and (b) (7) (C)  
**Subject:** My computer



all redactions (b) (6) unless otherwise indicated

[REDACTED], [REDACTED] has agreed to wipe my computer. [REDACTED] is in room [REDACTED]. (b) (6) and (b) (7) (C)

[REDACTED]  
Office of the Inspector General  
U.S. Department of Commerce  
Washington DC  
202.482. [REDACTED]

all redactions (b) (6) unless otherwise indicated

[REDACTED]  
From: [REDACTED] (b) (6) and (b) (7) (C)  
Sent: Thursday, December 02, 2010 10:56 AM  
To: [REDACTED]  
Cc: [REDACTED] Berenberg, Scott  
Subject: RE: My computer

Gwen,

(b) (2) I have forensically wiped both hard drives, [REDACTED] (b) (2)  
[REDACTED], and verified that the wipe was successful for the physical devices.

The computer can be picked up from the lab anytime today.

[REDACTED] (b) (6) and (b) (7) (C)  
Special Agent  
Computer Crimes  
United States Department of Commerce  
Office of Inspector General  
1401 Constitution Ave., NW Room [REDACTED] (b) (6) and (b) (7) (C)  
Washington, DC 20230  
(202) 482-[REDACTED] (Office)  
(202) 437-[REDACTED] (Cell)  
(202) 482-[REDACTED] (Fax)

(b) (6) and (b) (7) (C)

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

From: [REDACTED]  
Sent: Wednesday, December 01, 2010 9:52 AM  
To: [REDACTED]  
(b) (6) and (b) (7) (C) Cc: [REDACTED]  
Subject: RE: My computer

Thanks. On my way

[REDACTED]  
Office of the Chief Information Officer  
Office of Inspector General  
U.S. Department of Commerce  
(202) 482-[REDACTED] office  
(202) 680-[REDACTED] cell  
(202) 501-[REDACTED] or (202) 482-[REDACTED] fax  
[REDACTED]@oig.doc.gov

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

From: [REDACTED]

all redactions (b) (6) unless otherwise indicated

**Sent: Wednesday, December 01, 2010 9:11 AM**

**To:** [REDACTED] (b) (6) and (b) (7) (C)

**Subject:** My computer

[REDACTED], [REDACTED] has agreed to wipe my computer. [REDACTED] is in room [REDACTED]. (b) (6) and (b) (7) (C)

[REDACTED]  
Office of the Inspector General  
U.S. Department of Commerce  
Washington DC  
202.482. [REDACTED]

[REDACTED]

---

From: Anderson, Jennifer (b) (6) and (b) (7) (C)  
Sent: Thursday, December 02, 2010 10:56 AM  
To: [REDACTED]  
Cc: [REDACTED]; Berenberg, Scott  
Subject: RE: My computer

[REDACTED]

(b) (2) I have forensically wiped both hard drives, [REDACTED] (b) (2)  
(b) (2) [REDACTED] and verified that the wipe was successful for the physical devices.

The computer can be picked up from the lab anytime today.

[REDACTED] (b) (6) and (b) (7)  
(C)  
Special Agent  
Computer Crimes  
United States Department of Commerce  
Office of Inspector General  
1401 Constitution Ave., NW [REDACTED]  
Washington, DC 20230  
(202) 482-[REDACTED] (Office)  
(202) 437-[REDACTED] (Cell)  
(202) 482-[REDACTED] (Fax)

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

From: [REDACTED]  
Sent: Wednesday, December 01, 2010 9:52 AM  
To: [REDACTED]  
(b) (6) and (b) (7) (C) Cc: [REDACTED]  
Subject: RE: My computer

Thanks. On my way

[REDACTED]

Office of the Chief Information Officer  
Office of Inspector General  
U.S. Department of Commerce  
(202) 482-[REDACTED] office  
(202) 680-[REDACTED] cell  
(202) 501-[REDACTED] or (202) 482-[REDACTED] fax  
[REDACTED]@oig.doc.gov

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

From: [REDACTED]  
Sent: Wednesday, December 01, 2010 9:11 AM  
To: [REDACTED] (b) (6) and (b) (7) (C)  
Subject: My computer

all redactions (b) (6) unless otherwise indicated

[REDACTED] [REDACTED] has agreed to wipe my computer. [REDACTED] is in room [REDACTED] (b) (6) and (b) (7) (C)

[REDACTED]

Office of the Inspector General  
U.S. Department of Commerce  
Washington DC  
202.482. [REDACTED]