



governmentattic.org

"Rummaging in the government's attic"

Description of document: Department of Commerce email regarding staff access of the WikiLeaks website, November-December 2010

Requested date: 11-December-2010

Released date: 12-July-2011

Posted date: 25-July-2010

Source of document: Departmental Freedom of Information Officer
Office of Privacy and Open Government
US Department of Commerce
14th and Constitution Avenue NW
Mail Stop H6204
Washington, D.C. 20230
Fax: 202-482-0827
Email: EFoia@doc.gov

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

July 12, 2011

RE: Freedom of Information Act Request CRRIF 11-091

This is an interim response to your Freedom of Information Act (FOIA) request dated December 11, 2010, requesting copies of any records including e-mails concerning the retrieval and sanitizing of USPTO or Commerce Department computers that staff have used to download Wikileaks documents.

Enclosed are responsive documents, which are being released to you in their entirety. Portions of documents that contain non-responsive information have been redacted and marked "NR."

We have not completed the review of responsive documents. Upon completion, we will forward to you a final response.

Please contact me if you have questions at 202-482-3258 or via e-mail at BDolan1@doc.gov.

Sincerely,

Brenda Dolan
Departmental Freedom of Information
and Privacy Act Officer

Enclosures

Dahl, Scott

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

Bergersen, Benjamin

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

Bergersen, Benjamin

From: Bergersen, Benjamin
Sent: Thursday, December 02, 2010 10:28 AM
To: Dahl, Scott; Leiphart, Kristine; Bergersen, Benjamin
Subject: Re: WikiLeaks incident - reminder cautionary tale...

Scott and Kristine -

Agreed.

I will send out a reminder and cautionary tale. It fits in with our continuous security awareness with periodic refreshers as required by FISMA and NIST.

Wrm,
Ben
Benjamin Bergersen
Chief Information Officer

Office of Inspector General
U.S. Commerce Department
202-482-0611 Main Office
benjamin.bergersen@oig.doc.gov

From: Dahl, Scott
To: Leiphart, Kristine
Cc: Bergersen, Benjamin
Sent: Thu Dec 02 10:07:16 2010
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

Dahl, Scott

From: Bergersen, Benjamin
Sent: Thursday, December 02, 2010 10:28 AM
To: Dahl, Scott; Leiphart, Kristine; Bergersen, Benjamin
Subject: Re: WikiLeaks incident - reminder cautionary tale...

Scott and Kriastine -

Agreed.

I will send out a reminder and cautionary tale. It fits in with our continuous security awareness with periodic refreshers as required by FISMA and NIST.

Wrm,
Ben
Benjamin Bergersen
Chief Information Officer

Office of Inspector General
U.S. Commerce Department
202-482-0611 Main Office
benjamin.bergersen@oig.doc.gov

From: Dahl, Scott
To: Leiphart, Kristine
Cc: Bergersen, Benjamin
Sent: Thu Dec 02 10:07:16 2010
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

Bergersen, Benjamin

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 \\\
Attachments: WikiLeaks_2010_12_01[1].pdf
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

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

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

Bergersen, Benjamin

From: McDonnell, Kerry
Sent: Thursday, December 02, 2010 11:04 AM
To: Bergersen, Benjamin
Subject: RE: \\\FOUO \\\ IT Services Notice - Wikileaks Potentially Classified Documents. Gentle reminder of Viruses, and Security - a cautionary tale - \\\FOUO \\\

Who was the OIG employee?
Kerry

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

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

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

Moulder, Pamela

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 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.

DiGiacomo, Brian

From: Counsel, General
Sent: Monday, December 06, 2010 11:08 AM
To: Broadcast, DOC
Subject: Follow-up Guidance on WikiLeaks

Last week, you received notice from the Department's Office of CIO and Office of Security reminding you that, even though the classified government documents released by Wikileaks have been posted online and discussed widely in the media, they remain classified and have to be treated as such by federal employees and contractors.

We received additional guidance from OMB on Friday (which you may have read about over the weekend) about obligations for treatment of classified information and the use of non-classified government information technology systems. OMB's guidance appears below.

Cameron F. Kerry
General Counsel
United States Department of Commerce
1401 Constitution Avenue, NW, Room 5870
Washington, DC 20230

tel: 202-482-4772
email: generalcounsel@doc.gov
web: www.ogc.doc.gov

- 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.

DiGiacomo, Brian

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 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.

DiGiacomo, Brian

From: Kerry, Cameron
Sent: Sunday, December 05, 2010 7:23 PM
To: Szykman, Simon; Ehrenwerth, Justin
Cc: DiGiacomo, Brian; Reich, Jay
Subject: Draft Further Broadcast

Last week, you received notice from the Department's Office of CIO and Office of Security reminding you that, even though the classified government documents released by Wikileaks have been posted online and discussed widely in the media, they remain classified and have to be treated as such by federal employees and contractors.

We received additional guidance from OMB on Friday (which you may have read about over the weekend) about obligations for treatment of classified information and the use of non-classified government information technology systems. OMB's guidance appears below.

Cameron F. Kerry
General Counsel
United States Department of Commerce
1401 Constitution Avenue, NW, Room 5870
Washington, DC 20230

tel: 202-482-4772
email: generalcounsel@doc.gov
web: www.ogc.doc.gov

- 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.

Murphy, Latoya

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 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.

Dolphin, Tene

From: Counsel, General
Sent: Monday, December 06, 2010 11:08 AM
To: Broadcast, DOC
Subject: Follow-up Guidance on WikiLeaks

Last week, you received notice from the Department's Office of CIO and Office of Security reminding you that, even though the classified government documents released by Wikileaks have been posted online and discussed widely in the media, they remain classified and have to be treated as such by federal employees and contractors.

We received additional guidance from OMB on Friday (which you may have read about over the weekend) about obligations for treatment of classified information and the use of non-classified government information technology systems. OMB's guidance appears below.

Cameron F. Kerry
General Counsel
United States Department of Commerce
1401 Constitution Avenue, NW, Room 5870
Washington, DC 20230

tel: 202-482-4772
email: generalcounsel@doc.gov
web: www.ogc.doc.gov

- 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.

Kramer, Shira

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 or call (202) 482-4000.

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

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

Keegan, Corrie

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 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.

Steve Needle

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

Steve Needle

From: Alan Willard
Sent: Tuesday, November 30, 2010 4:43 PM
To: Steve Needle
Subject: RE: Wikileaks Site Block ***Situational Awareness***

Thank you Steve – I agree, however there have been further developments. I may need to see you Wed. morning.

Alan

From: Steve Needle
Sent: Tuesday, November 30, 2010 2:27 PM
To: Alan Willard
Subject: RE: Wikileaks Site Block ***Situational Awareness***

I would wait until the end of the day and just send an e-mail giving them the info that there were two PCs involved and the ID numbers and request further guidance on whether we should take any further action to secure them. I would wait to see if they ask for the names tomorrow. It's possible other components may also have qualms and this part might be conveniently dropped. I'm no IT maven but it seems to me that their first concern should be with securing the computers first, if they think there may be classified downloads on them but they are obviously trying to look proactive without really having a clear game plan in mind. Under those circumstances, I would hold off on reporting names.

From: Alan Willard
Sent: Tuesday, November 30, 2010 2:15 PM
To: Steve Needle
Subject: RE: Wikileaks Site Block ***Situational Awareness***

Two workstations from NTIS accessed the site yesterday. I cannot confirm that they downloaded anything.

The site is now blocked.

From: Steve Needle
Sent: Tuesday, November 30, 2010 2:14 PM
To: Alan Willard
Subject: RE: Wikileaks Site Block ***Situational Awareness***

Let's worry about it only after we have determined that NTIS computers accessed the site. Let me know if anyone did (but I don't need names).

From: Alan Willard
Sent: Tuesday, November 30, 2010 12:10 PM
To: Steve Needle
Cc: Bruce Borzino
Subject: FW: Wikileaks Site Block ***Situational Awareness***
Importance: High

Hi Steve;

Please see below and let me know what you think about the second part..." provide a listing of users..."

Thanks,
Alan

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: vnguyen@doc.gov
SIPRNet: vnguyen@doc.sgov.gov
Phone: (202) 482-6401
Blackberry: (202) 834-9123

Steve Needle

From: Alan Willard
Sent: Tuesday, November 30, 2010 2:15 PM
To: Steve Needle
Subject: RE: Wikileaks Site Block ***Situational Awareness***

Two workstations from NTIS accessed the site yesterday. I cannot confirm that they downloaded anything.

The site is now blocked.

From: Steve Needle
Sent: Tuesday, November 30, 2010 2:14 PM
To: Alan Willard
Subject: RE: Wikileaks Site Block ***Situational Awareness***

Let's worry about it only after we have determined that NTIS computers accessed the site. Let me know if anyone did (but I don't need names).

From: Alan Willard
Sent: Tuesday, November 30, 2010 12:10 PM
To: Steve Needle
Cc: Bruce Borzino
Subject: FW: Wikileaks Site Block ***Situational Awareness***
Importance: High

Hi Steve;

Please see below and let me know what you think about the second part..." provide a listing of users..."

Thanks,
Alan

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: vnguyen@doc.gov
SIPRNet: vnguyen@doc.sgov.gov
Phone: (202) 482-6401
Blackberry: (202) 834-9123

Steve Needle

From: Bob McClellan
Sent: Tuesday, November 30, 2010 12:43 PM
To: Alan Willard; Keith Sinner; Lee Halvorsen
Cc: Leigh Anne Levesque
Subject: RE: Wikileaks Site Block ***Situational Awareness***

Done.

Bob

From: Alan Willard
Sent: Tuesday, November 30, 2010 12:02 PM
To: Bob McClellan; Keith Sinner; Lee Halvorsen
Cc: Leigh Anne Levesque
Subject: FW: Wikileaks Site Block ***Situational Awareness***
Importance: High

Bob;

Please block access to the wikileaks.org website as soon as possible and let me know when it's done so that I can submit a report.

Also, please check to see if any NTIS PC's have accessed the wikileaks.org site since Friday 11/26 and let me know.

Thanks,
Alan

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: vnguyen@doc.gov
SIPRNet: vnguyen@doc.sgov.gov
Phone: (202) 482-6401
Blackberry: (202) 834-9123

Steve Needle

From: Alan Willard
Sent: Tuesday, November 30, 2010 12:10 PM
To: Steve Needle
Cc: Bruce Borzino
Subject: FW: Wikileaks Site Block ***Situational Awareness***
Importance: High

Hi Steve;

Please see below and let me know what you think about the second part..." provide a listing of users..."

Thanks,
Alan

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
SIPRNet: vnnguyen@doc.sgov.gov
Phone: (202) 482-6401
Blackberry: (202) 834-9123

Dolan, Brenda

From: Steve Needle [SNeedle@ntis.gov]
Sent: Tuesday, January 04, 2011 10:23 AM
To: Dolan, Brenda; Boyd, Harriette
Cc: Moton, Pat
Subject: CRRIF 11-0911 (NTIS 11-10)
Attachments: Wikileaks .pdf

Brenda/Harriet: I found this after I sent the package to Pat on this FOIA. Please add it to the file she sent. We have no objection to release.

Steve

Pardun, John

From: Counsel, General
Sent: Monday, December 06, 2010 11:08 AM
To: Broadcast, DOC
Subject: Follow-up Guidance on WikiLeaks

Last week, you received notice from the Department's Office of CIO and Office of Security reminding you that, even though the classified government documents released by Wikileaks have been posted online and discussed widely in the media, they remain classified and have to be treated as such by federal employees and contractors.

We received additional guidance from OMB on Friday (which you may have read about over the weekend) about obligations for treatment of classified information and the use of non-classified government information technology systems. OMB's guidance appears below.

Cameron F. Kerry
General Counsel
United States Department of Commerce
1401 Constitution Avenue, NW, Room 5870
Washington, DC 20230

tel: 202-482-4772
email: generalcounsel@doc.gov
web: www.ogc.doc.gov

- 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.

12/28/2010

- 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.

Pardun, John

From: Pardun, John
Sent: Thursday, December 02, 2010 4:13 PM
To: 'DOC-CIRT@doc.gov'
Cc: Turk, Rod; Blevins, Michael; 'vnguyen@doc.gov'
Subject: RE: Wikileaks Site Block ***Situational Awareness***

USPTO has complied with the below instructions for all users that accessed the WiliLeaks.or site as instructed.

The hard drives are at USPTO and are being appropriately stored by the USPTO CIRT team awaiting further guidance.

Thank you,

John Pardun, CISSP

Director, Cybersecurity Division
OCIO Office of Organizational Policy and Governance
US Patent and Trademark Office
Madison West (MDW), 5th Floor, Room 5D01
Office (571) 272-4349

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 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:

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
SIPRNet: 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
SIPRNet: vnguyen@doc.sgov.gov
Phone: (202) 482-6401
Blackberry: (202) 834-9123

Pardun, John

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 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.

1/12/2011

National Oceanic and Atmospheric Adm...



Rob Swisher <robert.swisher@noaa.gov>

Fwd: Wikileaks Site Block ***Situational Awareness***

2 messages

Larry Reed <Lawrence.Reed@noaa.gov>
To: Swisher Robert <Robert.Swisher@noaa.gov>

Wed, Jan 12, 2011 at 9:55 AM

per your request. 1 of 2

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

Subject: Wikileaks Site Block ***Situational Awareness***

Date: Tue, 30 Nov 2010 11:57:02 -0500

From: Nguyen, Vu <VNguyen@DOC.GOV>

Reply-To: members of the Federation of Department of Commerce CIRTs and
CIRCS <FEDCIRT@LIST.COMMERCE.GOV>

To: 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: 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

Larry Reed <Lawrence.Reed@noaa.gov>
To: swisher Robert <Robert.Swisher@noaa.gov>

Wed, Jan 12, 2011 at 9:59 AM

1/12/2011

National Oceanic and Atmospheric Adm...

per your request. 2 of 2.

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

Subject: Re: Wikileaks Site Block ***Situational Awareness***

Date: Tue, 30 Nov 2010 16:16:42 -0500

From: Nguyen, Vu <VNguyen@DOC.GOV>

Reply-To: members of the Federation of Department of Commerce CIRTs and

CIRCs <FEDCIRT@LIST.COMMERCE.GOV>

To: FEDCIRT@LIST.COMMERCE.GOV

Federation Team Members,

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:

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.

1/12/2011

National Oceanic and Atmospheric Adm...

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: 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
[Quoted text hidden]

1/12/2011

National Oceanic and Atmospheric Adm...



Rob Swisher <robert.swisher@noaa.gov>

Follow-up Guidance on WikiLeaks

1 message

Counsel, General <GeneralCounsel@doc.gov>

Mon, Dec 6, 2010 at 11:08 AM

Last week, you received notice from the Department's Office of CIO and Office of Security reminding you that, even though the classified government documents released by Wikileaks have been posted online and discussed widely in the media, they remain classified and have to be treated as such by federal employees and contractors.

We received additional guidance from OMB on Friday (which you may have read about over the weekend) about obligations for treatment of classified information and the use of non-classified government information technology systems. OMB's guidance appears below.

Cameron F. Kerry

General Counsel

United States Department of Commerce

1401 Constitution Avenue, NW, Room 5870

Washington, DC 20230

tel: 202-482-4772

email: generalcounsel@doc.gov

web: www.ogc.doc.gov

- 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

- 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.

1/12/2011

National Oceanic and Atmospheric Adm...



Rob Swisher <robert.swisher@noaa.gov>

A Message Regarding WikiLeaks

1 message

Dr. Jane Lubchenco <Announcement@noaa.gov>

Tue, Dec 7, 2010 at 2:45 PM

Message From the Under Secretary

December 7, 2010

As you may know by now, classified documents have been posted to the WikiLeaks website and the associated "mirror" websites. These documents may contain 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.

Utilizing NOAA issued equipment to view these sites not only introduces potentially classified information onto our unclassified networks and represents a spillage of classified data, but also requires the sanitization of affected equipment.

I want to reinforce the proper use of NOAA equipment and networks, and I am requesting your support in this effort. To that end, I'm resending (below) the full WikiLeaks policy directive issued by the Department of Commerce. Please take some time to review it if you haven't already done so.

If you have questions regarding this message or have accessed the WikiLeaks documents, please contact NOAA IT Security for assistance at itsec@noaa.gov.

Sincerely,

Dr. Jane

Join me on Facebook: www.facebook.com/noaa.lubchenco

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

From: Broadcast, DOC [<mailto:broadcast@doc.gov>]

Sent: Wednesday, December 01, 2010 10:57 AM

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

1/12/2011

National Oceanic and Atmospheric Adm...

This message was generated for the Under Secretary of Commerce
for Oceans and Atmosphere and NOAA Administrator by the NOAA
Information Technology Center/Financial and Administrative
Supporting Division

Katzman, Esther S.

From: Katzman, Esther S.
Sent: Wednesday, December 01, 2010 10:21 AM
To: Richter, Gale C.; Antonishek, John K.; Densock, Robert J.; Ting, Michael
Cc: Glenn, K. Robert; Enloe, Christian
Subject: FW: Wikileaks Site Block ***Situational Awareness***

FYI...I assume you all know about this already...but know some of you aren't on the OU secur list...Chris already forwarded it to the C&A team as well...

From: ou_secur@nist.gov [mailto:ou_secur@nist.gov] **On Behalf Of** Glenn, K. Robert
Sent: Wednesday, December 01, 2010 9:11 AM
To: Multiple recipients of list
Subject: FW: Wikileaks Site Block ***Situational Awareness***

OU ITSOs,

Based on the direction below, NIST blocked access to the wikileaks.org site yesterday afternoon. Based on initial network logs, we've identified 36 NIST computers (at both campuses) that accessed the site since Friday, November 26, 2010. We are analyzing that information and will validate it before sending it to DoC. We're working with DoC on clarifying some additional instructions and I'll relay what I can as we better understand the next steps that need to be taken.

Regards,

Rob G.

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 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: vnguyen@doc.gov
SIPRNet: vnguyen@doc.sgov.gov

• Phone: (202) 482-6401
Blackberry: (202) 834-9123

Antonishek, John K.

From: Glenn, K. Robert
Sent: Wednesday, December 01, 2010 2:29 PM
To: Antonishek, John K.
Cc: Glenn, K. Robert
Subject: Comments - wikileaks response memorandum
Attachments: wikileaks response memo 120110.doc

John, Comments or suggested edits?

Per Del, Pat and Kevin want the users to be able to continue using their computers; hence the change in that part of the message.

Rob G.

December 1, 2010

MEMORANDUM FOR THE RECORD

FROM: Rob Glenn, NIST IT Security Officer

Subject: NIST Plan on responding to Wikileaks incident instructions from the Department of Commerce (DoC)

On Tuesday, November 30, 2010, the DoC Office of the CIO (OCIO) directed all DoC Operating Units (OUs) as follows:

"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."

On Tuesday afternoon, the NIST Office of Information System Management (OISM) IT Security and Networking Division (ITSND) implemented the blocks as instructed and reported this status to DoC OCIO. ITSND also started analyzing network logs to determine computers and users that accessed Wikileaks.org websites since Friday, November 26, 2010. Logs identified 36 NIST computers that accessed these websites to varying degrees. Also, two servers that log NIST network traffic were identified that contained data exchanged between these NIST computers and the Wikileaks.org websites.

Later on Tuesday afternoon, DoC OCIO provided additional directions to all DoC OUs as follows:

"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:

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.”

Since NIST OISM has a highly skilled incident response team, including staff with appropriate clearances and experience in dealing with prior classified information spillages, NIST OISM intends to follow an alternative plan as follows:

- 1) Complete analysis to determine all users that accessed the Wikileaks.org sites. Report this list of users to DoC OCIO.
- 2) Notify users and their OU ITSOs that the users have been identified as having accessed Wikileaks documentation and as a result, may have unknowingly accessed classified information. 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 will also be reminded that they must continue to refrain from accessing any other Wikileaks documentation from any other websites.
- 3) 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:
 - 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) Identify and delete all data on the 2 servers that contain traffic between NIST computers and the Wikileaks.org websites. Erase all unused data sectors on the servers' hard drives.

This plan will completely eliminate all potential classified information stored on these computers, minimize the impact to users, and minimize the risks of losing NIST user data.

Subject: RE: Comments - wikileaks response memorandum
From: "Antonishek, John K." <john.antonishek@nist.gov>
Date: Wed, 1 Dec 2010 18:06:05 -0500
To: "Glenn, K. Robert" <robert.glenn@nist.gov>
CC: "Antonishek, John K." <john.antonishek@nist.gov>

Looks good to me. I'd indent the quotes, to make it easier to read (see attached).

-John

From: Glenn, K. Robert
Sent: Wednesday, December 01, 2010 2:29 PM
To: Antonishek, John K.
Cc: Glenn, K. Robert
Subject: Comments - wikileaks response memorandum

John, Comments or suggested edits?

Per Del, Pat and Kevin want the users to be able to continue using their computers; hence the change in that part of the message.

Rob G.

wikileaks response memo 120110 - ant.docx	Content-Description: wikileaks response memo 120110 - ant.docx Content-Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document Content-Encoding: base64
--	--

December 1, 2010

MEMORANDUM FOR THE RECORD

FROM: Rob Glenn, NIST IT Security Officer

Subject: NIST Plan on responding to Wikileaks incident instructions from the Department of Commerce (DoC)

On Tuesday, November 30, 2010, the DoC Office of the CIO (OCIO) directed all DoC Operating Units (OUs) as follows:

"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."

On Tuesday afternoon, the NIST Office of Information System Management (OISM) IT Security and Networking Division (ITSND) implemented the blocks as instructed and reported this status to DoC OCIO. ITSND also started analyzing network logs to determine computers and users that accessed Wikileaks.org websites since Friday, November 26, 2010. Logs identified 36 NIST computers that accessed these websites to varying degrees. Also, two servers that log NIST network traffic were identified that contained data exchanged between these NIST computers and the Wikileaks.org websites.

Later on Tuesday afternoon, DoC OCIO provided additional directions to all DoC OUs as follows:

"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:

Roger Clark

Antonishek, John K.

From: Glenn, K. Robert
Sent: Thursday, December 02, 2010 8:36 AM
To: Antonishek, John K.
Cc: Glenn, K. Robert
Subject: RE: Comments - wikileaks response memorandum

Thanks, John! I've added three more steps to our procedures. One to notify DoC OCIO that we will implement our own clean up procedures, one to notify OU Directors and OU ITSOs of the list of users, and one to notify DoC OCIO when clean up has been completed. I'll copy you on the updated version I send to Del, Susannah, and Kevin Kimball.

Rob G.

From: Antonishek, John K.
Sent: Wednesday, December 01, 2010 6:06 PM
To: Glenn, K. Robert
Cc: Antonishek, John K.
Subject: RE: Comments - wikileaks response memorandum

Looks good to me. I'd indent the quotes, to make it easier to read (see attached).

-John

From: Glenn, K. Robert
Sent: Wednesday, December 01, 2010 2:29 PM
To: Antonishek, John K.
Cc: Glenn, K. Robert
Subject: Comments - wikileaks response memorandum

John, Comments or suggested edits?

Per Del, Pat and Kevin want the users to be able to continue using their computers; hence the change in that part of the message.

Rob G.

Subject: FW: Wikileaks Site Block ***Situational Awareness***
From: "Glenn, K. Robert" <robert.glenn@nist.gov>
Date: Thu, 2 Dec 2010 09:35:43 -0500
To: "Zimmerman, Elizabeth" <elizabeth.zimmerman@nist.gov>
CC: "Glenn, K. Robert" <robert.glenn@nist.gov>

Beth, Here are the second set of instructions we received.

Rob G.

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 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:

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

Antonishek, John K.

From: Glenn, K. Robert
Sent: Thursday, December 02, 2010 9:43 AM
To: Kimball, Kevin A.; Brockett, Del; Schiller, Susannah B.; Zimmerman, Elizabeth
Cc: Antonishek, John K.; Glenn, K. Robert
Subject: WikiLeaks clean-up
Attachments: wikileaks response memo 120210.docx; CNSSI-1001.pdf

Del, Kevin, Beth, and Susannah, Attached is a draft memorandum which documents the highlights of what has occurred, specific details on DoC instructions (and how we responded), and our proposed plan on how to move forward. Let me know if you have any comments or suggestions. The next step would be to draft the email language for the users; which I hope to work on today.

I have also attached the official "National Instruction on Classified Information Spillage" as a reference so that it is understood what is formally required in case any of this is ever audited by the OIG, GAO, State, etc. The relevant section is Section V, steps 6, 8, 10, and 11. I believe the procedures outlined in the draft memorandum remains aligned with the formal instructions.

The one risk worth mentioning is that it is a bit of a stretch to use the continuity of operations/operational necessity consideration to justify permitting users to continue using their computers until sanitization is complete. If the risk is considered too high, then I would recommend either telling users that they cannot use their computer until it has been sanitized; remove the computer from the network until it has been sanitized; or (per DoC instructions and normal SOP for these cases) have the hard drives removed and let users know that as part of the sanitization we will work with them to return their data as part of the sanitization process. If this information had not been posted broadly and publicly, we would have implemented standard procedures (i.e. disconnect the computers, collect hard drives for large numbers of users or immediately sanitize if it involved only 1 or 2 computers) and not considered allowing users to continue using their computers.

Regards,

Rob G.

December 2, 2010

MEMORANDUM FOR THE RECORD

FROM: Rob Glenn, NIST IT Security Officer

Subject: NIST Plan on responding to Wikileaks incident instructions from the Department of Commerce (DoC)

On Tuesday, November 30, 2010, the DoC Office of the CIO (OCIO) directed all DoC Operating Units (OUs) as follows:

"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."

On Tuesday afternoon, the NIST Office of Information System Management (OISM) IT Security and Networking Division (ITSND) implemented the blocks as instructed and reported this status to DoC OCIO. ITSND also started analyzing network logs to determine computers and users that accessed Wikileaks.org websites since Friday, November 26, 2010. Logs identified 36 NIST computers that accessed these websites to varying degrees. Also, two servers that log NIST network traffic were identified that contained data exchanged between these NIST computers and the Wikileaks.org websites.

Later on Tuesday afternoon, DoC OCIO provided additional directions to all DoC OUs as follows:

"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:

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."

Since NIST OISM has a highly skilled incident response team, including staff with appropriate clearances and experience in dealing with prior classified information spillages, NIST OISM intends to follow an alternative plan as follows:

- 1) Complete analysis to determine all users that accessed the Wikileaks.org sites. Report this list of users to DoC OCIO.
- 2) Notify DoC OCIO that NIST will implement its own containment and clean up procedures and notify DoC OCIO when clean up has been completed.
- 3) Notify OU Directors and OU ITSOs of their users whose computers have accessed Wikileaks.org sites.
- 4) Notify users that their computer has been identified as having accessed Wikileaks documentation and as a result, may have unknowingly accessed classified information. 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 will also be reminded that they must continue to refrain from accessing any other Wikileaks documentation from any other websites. Specific email language to be sent to users is TBD.
- 5) 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.
- 6) For each computer to be sanitized:
 - 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.
- 7) Identify and delete all data on the 2 servers that contain traffic between NIST computers and the Wikileaks.org websites. Erase all unused data sectors on the servers' hard drives.
- 8) Notify DoC OCIO that clean up has been completed and that specific details are available as needed.

This plan will completely eliminate all potential classified information stored on these computers, minimize the impact to users, and minimize the risks of losing NIST user data.

DRAFT

Committee on National Security System

**CNSS Instruction No. 1001
February 2008**



National Instruction On Classified Information Spillage



Committee on National Security Systems

CNSS Instruction No. 1001

National Manager

FOREWORD

1. The Committee on National Security Systems Instruction (CNSSI) No. 1001, "National Instruction on Classified Information Spillage" implements the Committee on National Security Systems Policy No. 18, reference 4.a, and is effective upon receipt.
2. Additional copies of this instruction may be obtained from the Secretariat or the Committee on National Security Systems website – www.cnss.gov.

//s//

KEITH B. ALEXANDER
Lieutenant General, U.S. Army

NATIONAL INSTRUCTION ON CLASSIFIED INFORMATION SPILLAGE

CNSS Secretariat (1923)
National Security Agency
9800 Savage Road - STE 6716 - Ft Meade MD 20755-6716
Office: (410) 854-6805
Unclassified FAX: (410) 854-6814
cnss@radium.ncsc.mil

<u>TITLE</u>	<u>SECTION</u>
PURPOSE	I
SCOPE	II
REFERENCES	III
DEFINITIONS	IV
PROCEDURES	V
RESPONSIBILITIES	VI

SECTION I – PURPOSE

1. This instruction establishes the minimum actions required when responding to an information spillage¹ of classified national security information² onto an unclassified Information System (IS), or higher-level classified information onto a lower level classified IS or onto a system not accredited to that category³ (i.e. restrictive label) of information, to include non-government systems.

SECTION II – SCOPE

2. This instruction applies to the spillage of classified national security information on any IS, be it government, commercial, or private. In the case of private or commercial systems where there is no contractual requirement with the government, department/agency heads will ensure that an inquiry/investigation is conducted in accordance with references 3 b and c. In such cases, the actions established by this instruction will be implemented to the extent practical.

SECTION III – REFERENCES

3. References:

a. Committee on National Security Systems Policy No. 18, “National Policy on Classified Information Spillage,” June 2006.

¹ CNSSI No. 4009, reference 3.d, defines spillage.

² Executive Order 12958, reference 3.b, defines classified national security information.

³ CNSSI No. 4009, reference 3.d, defines category.

- b. Executive Order 12958, "Classified National Security Information," as amended, March 2003.
- c. 32 CFR Part 2001 "Classified National Security Information," (Information Security Oversight Office Directive No. 1), 22 September 2003.
- d. Committee on National Security Systems Instruction No. 4009, "National Information Assurance (IA) Glossary," June 2006.
- e. Federal Information Security Management Act (FISMA), Title III of Public Law 107-347 (116 Stat 2948), and the E-Government Act of 2002, Public Law 107-347 (116 Stat 2899).

SECTION IV – DEFINITIONS

- 4. Definitions in references 3.b, c, and d apply to this instruction.

SECTION V – PROCEDURES

- 5. When there is evidence of a possible spillage of classified national security information, hereinafter "*classified information*," an immediate notification shall be made to the information owner, the information assurance manager, the activity security manager, and the responsible Incident Response Center (IRC)⁴. Responsible personnel shall conduct an immediate preliminary inquiry to determine whether the classified information was subjected to loss, possible compromise, or unauthorized disclosure⁵.
- 6. If the preliminary inquiry indicates a spillage has occurred, immediate steps shall be taken to contain and prevent further spillage of classified information. In all steps undertaken to isolate and protect the classified information from unauthorized disclosure, continuity of operations should be maintained. Continuity of operations factors should include: classification level and category of the information, perishability of the information, possible impact to ongoing investigations, or operational necessity. Consideration should be given to law enforcement implications and preservation of evidence.
- 7. Upon determination that a spillage has occurred, a formal inquiry shall be conducted. A team shall be formed to investigate. At a minimum, the team shall include the Information Assurance Manager, Information System Security Manager or equivalent⁶, Activity Security Manager, information owner, responsible IRC, and law

⁴ FISMA, reference 3.e, defines incident response center.

⁵ Executive Order 12958, reference 4 b, defines unauthorized disclosure.

⁶ The cited specialty titles may be equivalent to other titles used throughout organizations.

enforcement authorities, as appropriate. The team will address, at a minimum, the following questions:

- a. When did the spillage occur?
 - b. What information was spilled?
 - c. What was the classification/category of the spilled information?
 - d. Was the classified information in question properly classified?
 - e. What steps were taken to contain the spillage?
 - f. What caused the spillage to occur?
 - g. Who was responsible for the spill?
 - h. What was the flow of information to reach its ultimate destination (e.g., specific web, mail, or file servers)?
 - i. Where is the information now stored?
 - j. What steps were taken to identify the person(s) responsible for the spillage?
 - k. What individuals had access to the information?
 - l. In what specific media did the classified information originate?
 - m. What IS(s) were affected and to what extent?
 - n. Will further inquiry increase the damage caused in the event of a compromise?
 - o. Is the information being handled as evidence?
8. The appropriate procedures for sanitizing or remediating the effects of a spill may include:
- a. Using the operating system to delete the spilled information.
 - b. Re-labeling the media containing the spilled information to the appropriate classification/category and transferring the media into an appropriate environment.

- c. Removing the classified information from the media by organization-approved technical means to render the information unrecoverable.

- d. Erasing operating system, program files, and all data files.

- e. Erasing all partition tables and drive formats.

- f. Erasing and sanitizing the media.

- g. Forfeiting the media.

9. Selection of the appropriate remediation procedure is dependent on several factors that may include:

- a. The difference between the classification and category of the spilled information and the classification and category approved for the system containing the spilled information.

- b. The requirements of the information owner regarding information sensitivity and risks from inadvertent disclosure.

- c. Financial considerations, including costs of media replacement and resources required for remediating the spill.

- d. Operation and mission impacts.

- e. Pre-existing agreements between the information owner's and the spiller's organization(s).

- f. Assessment of the effectiveness of the sanitization/remediation procedures.

10. Unless otherwise determined by the information owner, in cases where the spillage occurred within agency-controlled space, sanitization is not required until such time as the affected systems are removed from agency control. In such cases, immediate actions will be required to ensure that the spillage is isolated and contained, and that unauthorized access is precluded based on risk management decisions and operational considerations related to the loss of information services. Preclusion of unauthorized access may include software overwriting of affected data sectors in the interest of meeting operational needs. When the media is released from agency control, sanitization is required.

11. Once the extent of the spillage has been determined and the exact location(s) of the information on the system(s) are known, a final report must be completed and submitted to the information owner and must include a statement of recommended corrective action to prevent a recurrence. The information owner and the head or

designee of the department/agency where the incident occurred shall collaborate in the performance of a risk assessment to determine mitigation procedures, with input from the responsible IRC and other appropriate parties:

a. Such corrective actions include new procedures, technologies, security education, and other means to address technical and procedural deficiencies, or incidents of negligence and deliberate disregard.

b. When implementing the mitigation procedures, options should be taken to preserve continuity of operations.

c. If the conclusion of the inquiry is a loss, possible compromise or unauthorized disclosure of classified information, the degree of damage to national security shall be ascertained.

SECTION VI – RESPONSIBILITIES

12. The head of each department/agency shall:

a. Provide policy and direction for reporting and investigating spillages of classified information onto an unclassified IS, or higher-level classified information onto lower level classified IS or onto a system not accredited to that category of information, to include non-government systems.

b. Monitor investigations of spillages of classified information.

c. Review findings of initial inquiry and/or investigation of spillages of classified information.

d. Determine whether an additional internal investigation is appropriate, depending on the results of the initial inquiry and/or investigation. Consultation should take place with the department/agency having original classification authority for the information.

e. Determine whether the incident should be referred to the Department of Justice for investigation and/or criminal prosecution.

f. Notify the Director, Information Security Oversight Office as required by reference b.⁷

g. Request the initiation of comprehensive analyses and damage assessments when such disclosures affect intelligence or counterintelligence activities, capabilities, and techniques.

h. Ensure cooperation with the agency having original classification authority in their conduct of comprehensive damage assessments, analyses, and/or operations.

i. Designate, at their discretion, a responsible department/agency official for implementing the responsibilities listed above.

13. Responsible department/agency officials shall:

a. Notify the head of the department/agency or designee about any spillage of classified information, and provide the information listed in Section V, paragraphs 7 and 8 in accordance with internal guidance or procedures.

b. Serve as the principal point of contact on counterintelligence and security investigative matters related to the spillage that involve other government organizations.

c. Determine whether further investigation is appropriate when the initial inquiry or investigation does not identify the person responsible for or cause of a spillage.

d. Report the investigative results and any corrective and/or disciplinary action taken to the department/agency head.

e. Refer the incident to the appropriate counterintelligence organization, when there are indications that show a foreign intelligence service or an international terrorist group or organization may be involved.

14. Department/agency security personnel, Information Technology/Information Assurance personnel, and others shall:

a. Ensure that all known or suspected instances of spillages of classified information are promptly reported and render full cooperation in any investigation.

b. Ensure that all known or suspected instances of spillages of classified information are promptly investigated pursuant to their areas of responsibilities.

⁷ Section 5.5. (e) (2) of Executive Order 12958, reference b, as amended, states, "notify the Director of the Information Security Oversight Office when a violation under paragraph (b) (1), (2), or (3) of this section occurs."

c. Ensure appropriate actions are taken to isolate and contain the spillage, as well as to preclude unauthorized access, while using risk management principles to maintain continuity of operations.

d. Ensure notification of the spillage to the responsible IRC.

15. Users shall report all known or suspected instances of spillages of classified information per department/agency guidance and render full cooperation in any investigation.

Brockett, Del

From: Glenn, K. Robert
Sent: Thursday, December 02, 2010 10:04 AM
To: Glenn, K. Robert; Kimball, Kevin A.; Brockett, Del; Schiller, Susannah B.; Zimmerman, Elizabeth
Cc: Antonishek, John K.; Glenn, K. Robert
Subject: RE: WikiLeaks clean-up

As a follow-up. Roger Clark just called and asked on the status of getting him the list of names. He specifically mentioned that OSY is pushing for the list of names so they can schedule an inadvertent disclosure briefing for each user. I told Roger that we're still working on identifying a couple of the users and should be able to get him the list today.

Rob G.

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

From: Glenn, K. Robert
Sent: Thursday, December 02, 2010 9:43 AM
To: Kimball, Kevin A.; Brockett, Del; Schiller, Susannah B.; Zimmerman, Elizabeth
Cc: Antonishek, John K.; Glenn, K. Robert
Subject: Wikileaks clean-up

Del, Kevin, Beth, and Susannah, Attached is a draft memorandum which documents the highlights of what has occurred, specific details on DoC instructions (and how we responded), and our proposed plan on how to move forward. Let me know if you have any comments or suggestions. The next step would be to draft the email language for the users; which I hope to work on today.

I have also attached the official "National Instruction on Classified Information Spillage" as a reference so that it is understood what is formally required in case any of this is ever audited by the OIG, GAO, State, etc. The relevant section is Section V, steps 6, 8, 10, and 11. I believe the procedures outlined in the draft memorandum remains aligned with the formal instructions.

The one risk worth mentioning is that it is a bit of a stretch to use the continuity of operations/operational necessity consideration to justify permitting users to continue using their computers until sanitization is complete. If the risk is considered too high, then I would recommend either telling users that they cannot use their computer until it has been sanitized; remove the computer from the network until it has been sanitized; or (per DoC instructions and normal SOP for these cases) have the hard drives removed and let users know that as part of the sanitization we will work with them to return their data as part of the sanitization process. If this information had not been posted broadly and publicly, we would have implemented standard procedures (i.e. disconnect the computers, collect hard drives for large numbers of users or immediately sanitize if it involved only 1 or 2 computers) and not considered allowing users to continue using their computers.

Regards,

Rob G.

Schiller, Susannah B.

From: Schiller, Susannah B.
Sent: Thursday, December 02, 2010 10:30 AM
To: Glenn, K. Robert; Brockett, Del; Antonishek, John K.; Kimball, Kevin A.; Zimmerman, Elizabeth
Subject: FW: WikiLeaks clean-up
Attachments: wikileaks response memo 120210.docx

I edited with track changes on -- a couple of questions, and a few more picky things since this memo to the file could easily be referenced later.

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

From: Glenn, K. Robert
Sent: Thursday, December 02, 2010 9:43 AM
To: Kimball, Kevin A.; Brockett, Del; Schiller, Susannah B.; Zimmerman, Elizabeth
Cc: Antonishek, John K.; Glenn, K. Robert
Subject: WikiLeaks clean-up

Del, Kevin, Beth, and Susannah, Attached is a draft memorandum which documents the highlights of what has occurred, specific details on DoC instructions (and how we responded), and our proposed plan on how to move forward. Let me know if you have any comments or suggestions. The next step would be to draft the email language for the users; which I hope to work on today.

I have also attached the official "National Instruction on Classified Information Spillage" as a reference so that it is understood what is formally required in case any of this is ever audited by the OIG, GAO, State, etc. The relevant section is Section V, steps 6, 8, 10, and 11. I believe the procedures outlined in the draft memorandum remains aligned with the formal instructions.

The one risk worth mentioning is that it is a bit of a stretch to use the continuity of operations/operational necessity consideration to justify permitting users to continue using their computers until sanitization is complete. If the risk is considered too high, then I would recommend either telling users that they cannot use their computer until it has been sanitized; remove the computer from the network until it has been sanitized; or (per DoC instructions and normal SOP for these cases) have the hard drives removed and let users know that as part of the sanitization we will work with them to return their data as part of the sanitization process. If this information had not been posted broadly and publicly, we would have implemented standard procedures (i.e. disconnect the computers, collect hard drives for large numbers of users or immediately sanitize if it involved only 1 or 2 computers) and not considered allowing users to continue using their computers.

Regards,

Rob G.

December 2, 2010

MEMORANDUM FOR THE RECORD

FROM: Rob Glenn, NIST IT Security Officer

Subject: NIST Plan ~~on~~ for responding to Wikileaks incident instructions from the Department of Commerce (DoC)

On Tuesday, November 30, 2010, the DoC Office of the CIO (OCIO) directed all DoC Operating Units (OUs) as follows:

"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."

On Tuesday afternoon, the NIST Office of Information System Management (OISM) IT Security and Networking Division (ITSND) implemented the blocks as instructed and reported this status to ~~DoC-CIRT~~ OCIO. ITSND also started analyzing network logs to determine which computers and users ~~that had~~ accessed Wikileaks.org websites since Friday, November 26, 2010. Logs identified 36 NIST computers ~~that had~~ accessed these websites to varying degrees. Also, two servers that log NIST network traffic were identified that contained data exchanged between these NIST computers and the Wikileaks.org websites.

Comment [SBS1]: This is what the instructions said to do – I realize it's part of OCIO, might as well be specific.

Later on Tuesday afternoon, DoC OCIO provided additional directions to all DoC OUs as follows:

"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:

Roger Clark

This plan will completely eliminate all potential classified information stored on these computers, minimize the impact to users, and minimize the risks of losing NIST user data.

Schiller, Susannah B.

From: Romine, Charles H.
Sent: Thursday, December 02, 2010 1:07 PM
To: Glenn, K. Robert; Kimball, Kevin A.; Schiller, Susannah B.; Brockett, Del; Romine, Charles H.
Cc: Schmidt, Carolyn M.
Subject: Re: WikiLeaks clean-up
Attachments: Wikileaks email to staff.docx

This is good — a few suggested edits are attached, in Word so I could use track changes. Also, sanitization (which sounds very much like wiping the entire disk) sounds alarming, particularly when the explanation sounds like it includes removing backups. Perhaps we should insert a statement that only the classified information, if any, will be removed?

Chuck

--

Charles H. Romine, Associate Director for Program Implementation
Information Technology Laboratory, NIST
301-975-3039, cromine@nist.gov

From: "Glenn, K. Robert" <robert.glenn@nist.gov>
Date: Thu, 2 Dec 2010 12:07:12 -0500
To: Kevin Kimball <kevin.kimball@nist.gov>, Susannah Schiller <susannah.schiller@nist.gov>, "Brockett, Del" <del.brockett@nist.gov>, Charles Romine <charles.romine@nist.gov>
Cc: "Schmidt, Carolyn M." <carolyn.schmidt@nist.gov>, "Glenn, K. Robert" <robert.glenn@nist.gov>
Subject: RE: WikiLeaks clean-up

Below is a draft user message to be discussed at this afternoon's meeting. The idea is that a single message would be sent and blind copied to each of the 36 users.

Carol - thank you very much for your help with this.

Rob G.

=====

Subject: WikiLeaks Incident

DOC has confirmed that WikiLeaks was accessed from your computer. Hence, you may have unknowingly accessed classified information. Because access occurred prior to receiving guidance from DOC, this is viewed as an unintentional incident in terms of behavior. However, your computer must be treated as though there is classified data resident (i.e., classified information spillage). Therefore, your 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 will contact you to schedule sanitization of your computer. Please do not access, read, forward, or otherwise move any WikiLeaks documentation that you may have downloaded to your computer. Sanitization will include removal of the information in your browser cache/history, temporary files, backups, etc., and verification made that the information was not forwarded via other methods such as email, instant messaging, etc. 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 follow up to schedule an inadvertent disclosure briefing with you.

DOC has confirmed that WikiLeaks was accessed from ~~your~~ a computer registered to you. Hence, you or another user of the computer may have unknowingly accessed classified information. Because access occurred prior to receiving guidance from DOC, this is viewed as an unintentional incident ~~in terms of behavior~~. However, NIST is required to treat your the computer must be treated as though there is classified data resident (i.e., classified information spillage). Therefore, ~~your 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 will contact you to schedule sanitization of ~~your the~~ computer. Please do not access, read, forward, or otherwise move any WikiLeaks documents ~~that you may have been downloaded to your computer~~. 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, etc., and verification ~~made that~~ the information was not forwarded via other methods such as email, instant messaging, etc. 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 follow up to schedule an inadvertent disclosure briefing ~~with you~~.

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 direct any questions to the NIST IT Assistance Center (iTAC) at 301-975-5375 (Gaithersburg), or 303-497-5375 (Boulder).

Comment [CHR1]: Has iTAC been provided guidance on how to handle these questions? Rules governing the handling of classified information are not widely understood and we can't risk providing info that hasn't been thoroughly vetted. Given the relatively small number of incidents and the even smaller likelihood of large numbers of calls, perhaps a single pt of contact rather than iTAC is better here.

Schiller, Susannah B.

From: Glenn, K. Robert
Sent: Thursday, December 02, 2010 1:48 PM
To: Romine, Charles H.; Kimball, Kevin A.; Schiller, Susannah B.; Brockett, Del
Cc: Schmidt, Carolyn M.; Glenn, K. Robert
Subject: RE: WikiLeaks clean-up
Attachments: Wikileaks email to staff v3.docx

Chuck, Thank you very much for the feedback.

Attached is an updated version that should address your concerns below (and incorporates your edits), keeping in mind that we will likely delete more than just classified information since no one has explained to us what is and is not classified in this case, and the sanitization will include cleaning of the browser cache and history, and may include shredding cds and dvds that include WikiLeaks and other information (i.e. if the information cannot be isolated before it has to be sanitized). Also, for messages like this, it is our standard process to request feedback from Jennie Covahey (PBA), which have now also been incorporated. Also, based on her feedback, this email would include a copy of the NIST allstaff (which included the DoC broadcast) sent out yesterday.

Regarding the iTAC comment, iTAC has already been instructed to forward all related requests and questions directly to my office, following standard service management practices, where either I or one of my staff will follow-up timely.

Rob G.

From: Romine, Charles H.
Sent: Thursday, December 02, 2010 1:07 PM
To: Glenn, K. Robert; Kimball, Kevin A.; Schiller, Susannah B.; Brockett, Del; Romine, Charles H.
Cc: Schmidt, Carolyn M.
Subject: Re: WikiLeaks clean-up

This is good — a few suggested edits are attached, in Word so I could use track changes. Also, sanitization (which sounds very much like wiping the entire disk) sounds alarming, particularly when the explanation sounds like it includes removing backups. Perhaps we should insert a statement that only the classified information, if any, will be removed?

Chuck

--

Charles H. Romine, Associate Director for Program Implementation
Information Technology Laboratory, NIST
301-975-3039, cromine@nist.gov

From: "Glenn, K. Robert" <robert.glenn@nist.gov>
Date: Thu, 2 Dec 2010 12:07:12 -0500
To: Kevin Kimball <kevin.kimball@nist.gov>, Susannah Schiller <susannah.schiller@nist.gov>, "Brockett, Del" <del.brockett@nist.gov>, Charles Romine <charles.romine@nist.gov>
Cc: "Schmidt, Carolyn M." <carolyn.schmidt@nist.gov>, "Glenn, K. Robert" <robert.glenn@nist.gov>
Subject: RE: WikiLeaks clean-up

Below is a draft user message to be discussed at this afternoon's meeting. The idea is that a single message would be sent and blind copied to each of the 36 users.

if you have any comments or suggestions. The next step would be to draft the email language for the users; which I hope to work on today.

I have also attached the official "National Instruction on Classified Information Spillage" as a reference so that it is understood what is formally required in case any of this is ever audited by the OIG, GAO, State, etc. The relevant section is Section V, steps 6, 8, 10, and 11. I believe the procedures outlined in the draft memorandum remains aligned with the formal instructions.

The one risk worth mentioning is that it is a bit of a stretch to use the continuity of operations/operational necessity consideration to justify permitting users to continue using their computers until sanitization is complete. If the risk is considered too high, then I would recommend either telling users that they cannot use their computer until it has been sanitized; remove the computer from the network until it has been sanitized; or (per DoC instructions and normal SOP for these cases) have the hard drives removed and let users know that as part of the sanitization we will work with them to return their data as part of the sanitization process. If this information had not been posted broadly and publicly, we would have implemented standard procedures (i.e. disconnect the computers, collect hard drives for large numbers of users or immediately sanitize if it involved only 1 or 2 computers) and not considered allowing users to continue using their computers.

Regards,

Rob G.

DOC has confirmed that WikiLeaks was accessed from ~~your a computer registered to you, which may mean.~~ Hence, ~~you or another user of the computer~~ may have ~~classified information was unknowingly accessed, classified information.~~ Because access occurred prior to receiving guidance from DOC (~~see below~~), this is viewed as an unintentional incident ~~in terms of behavior.~~ However, NIST is required to treat your the computer must be treated as though there is classified data resident (i.e., classified information spillage) and. Therefore, ~~your 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 will contact you to schedule sanitization of ~~your the~~ computer. Please do not access, read, forward, or otherwise move any WikiLeaks documents ~~that you may have been downloaded to your computer.~~ 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 ~~made 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. 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 follow up to schedule an inadvertent disclosure briefing ~~with you.~~

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 direct any questions to the NIST IT Assistance Center (iTAC) at 301-975-5375 (Gaithersburg), or 303-497-5375 (Boulder).

Comment [CHR1]: Has iTAC been provided guidance on how to handle these questions? Rules governing the handling of classified information are not widely understood and we can't risk providing info that hasn't been thoroughly vetted. Given the relatively small number of incidents and the even smaller likelihood of large numbers of calls, perhaps a single pt of contact rather than iTAC is better here.

Schiller, Susannah B.

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"
Attachments: Wikileaks email to staff v4.docx

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?

Schmidt, Carolyn M.

From: Schmidt, Carolyn M.
Sent: Thursday, December 02, 2010 1:34 PM
To: Covahey, Virginia
Cc: Glenn, K. Robert
Subject: RE: draft incident msg

Thanks so much, Jennie. We've integrated your changes along with those received from Chuck Romine. Rob has a meeting with Chuck and Kevin Kimball to go through this and subsequent actions this afternoon. Appreciate your time. Feel better. -C

From: Covahey, Virginia
Sent: Thursday, December 02, 2010 1:25 PM
To: Schmidt, Carolyn M.
Cc: Glenn, K. Robert
Subject: RE: draft incident msg

You might want to reference the earlier note from DOC in case people didn't read it – maybe include a link to the email? A few other tweaks to remove a "hence" and "therefore" ☺

Subject: WikiLeaks Incident

DOC has confirmed that WikiLeaks was accessed from your computer, which may mean you have unknowingly accessed classified information. Because access occurred prior to receiving guidance from DOC (include link to DOC email here?), this is viewed as an unintentional incident in terms of behavior. However, your computer must be treated as though there is classified data resident (i.e., classified information spillage), and your 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 will contact you to schedule sanitization of your computer. Please do not access, read, forward, or otherwise move any WikiLeaks documentation that you may have downloaded to your computer. Sanitization will include removal of the information in your browser cache/history, temporary files, backups, etc., and verification made that the information was not forwarded via other methods such as email, instant messaging, etc. Given the number of incidents within NIST, we ask for your patience in scheduling sanitization, and recovering your work environment.

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 direct any questions to the NIST IT Assistance Center (iTAC) at 301-975-5375 (Gaithersburg), or 303-497-5375 (Boulder).

From: Schmidt, Carolyn M.
Sent: Thursday, December 02, 2010 11:21 AM
To: Covahey, Virginia
Cc: Glenn, K. Robert
Subject: draft incident msg

Hi Jennie,

Below is a draft message intended for a small populace of NIST staff. We don't want to panic the users, and while we don't explicitly state it (nor do I think we want to), they may continue to use their computers until we can sanitize their computers. Please reply to all with any comments as soon as you can. There is an urgency to get this out to the affected users. I ***always*** appreciate your perspective.

Hope you feel better!

Carol

Subject: WikiLeaks Incident

DOC has confirmed that WikiLeaks was accessed from your computer. Hence, you may have unknowingly accessed classified information. Because access occurred prior to receiving guidance from DOC, this is viewed as an unintentional incident in terms of behavior. However, your computer must be treated as though there is classified data resident (i.e., classified information spillage). Therefore, your 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 will contact you to schedule sanitization of your computer. Please do not access, read, forward, or otherwise move any WikiLeaks documentation that you may have downloaded to your computer. Sanitization will include removal of the information in your browser cache/history, temporary files, backups, etc., and verification made that the information was not forwarded via other methods such as email, instant messaging, etc. Given the number of incidents within NIST, we ask for your patience in scheduling sanitization, and recovering your work environment.

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 direct any questions to the NIST IT Assistance Center (iTAC) at 301-975-5375 (Gaithersburg), or 303-497-5375 (Boulder).

Schiller, Susannah B.

From: Schiller, Susannah B.
Sent: Thursday, December 02, 2010 4:54 PM
To: Diduch, Lukas
Subject: Wikileaks

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?

Susannah B. Schiller
Deputy CIO
National Institute of Standards and Technology
100 Bureau Dr.
Mail Stop 1800
Gaithersburg, MD 20899-1800
301-975-6500

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: Bruno, Thomas J. Phone: 303-497-5158
Requester Email: thomas.bruno@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

Subject: RE: New wikileaks block
From: "Glenn, K. Robert" <robert.glenn@nist.gov>
Date: Fri, 3 Dec 2010 10:20:58 -0500
To: "Klosowski, Przemek" <przemek.klosowski@nist.gov>
CC: "Glenn, K. Robert" <robert.glenn@nist.gov>

Przemek,

For this, I need SIIRT to do the work to ensure everything is well documented and the clean up is consistent across NIST. Also, SIIRT has the clearances required to access the data if necessary.

BTW, I'm having a problem getting to one of your users; I'm not even getting voice mail, it just keeps ringing. I'm hoping that for those that are not at their phone today, I can leave voice mail and send them an email, but in this particular case, since I can't get his voicemail, I may need your help getting in touch with him. I'll let you know after lunch if I need your help.

Rob G.

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

From: Przemek Klosowski [<mailto:przemek.klosowski@nist.gov>]
Sent: Friday, December 03, 2010 10:09 AM
To: Glenn, K. Robert
Subject: Re: New wikileaks block

Rob,

I see that 2 NCNR computers accessed the wikileak site. I have a question about your instructions: who is supposed to do the cleanup: SIIRT or our support group? It seems simple enough so we could do it unless you wanted a standard process and preferred SIIRT to do it.

I understand that you're in the process of notifying the user and I will hear from you shortly.

P

Katzman, Esther S.

From: Katzman, Esther S.
Sent: Friday, December 03, 2010 11:06 AM
To: Richter, Gale C.; Enloe, Christian; Densock, Robert J.; Ting, Michael; Waltermire, Karen; Schmidt, Carolyn M.; ant@nist.gov
Cc: Glenn, K. Robert
Subject: FW: Guidance regarding WikiLeaks

I'm sure most of you are already aware of this status, but please inform your staff of the details. Thx, E

From: ou_secur@nist.gov [ou_secur@nist.gov] On Behalf Of Glenn, K. Robert [robert.glenn@nist.gov]
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.

McIntyre, Jeffrey J.

From: Hurst V, Alfred Coulter
Sent: Friday, December 03, 2010 2:15 PM
To: siirt
Subject: Template document
Attachments: WikiLeaks Template Document.docx

Template document

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/>

Brockett, Del

From: Brockett, Del
Sent: Friday, December 03, 2010 2:31 PM
To: 'MBryant@doc.gov'
Subject: Complete list from NIST
Attachments: Complete list of NIST Users - wikileaks.xlsx

Mike,

We now have a complete list of all identified NIST users. I am providing as attached.

Please let me know if you have any questions.

Thanks,

Del

*Delwin Brockett
CIO
National Institute of Standards and Technology
www.nist.gov
100 Bureau Dr. Mail Stop 1800
Gaithersburg, MD 20899-1800
301-975-6500*

Brockett, Del

From: Glenn, K. Robert
Sent: Tuesday, December 07, 2010 1:47 PM
To: Schiller, Susannah B.; Brockett, Del
Cc: Glenn, K. Robert
Subject: FW: List of Names
Attachments: NIST Users - WikiLeaks 120710.xlsx

FYI – updated list of names.

Rob G.

From: Glenn, K. Robert
Sent: Tuesday, December 07, 2010 1:43 PM
To: Clark, Roger
Cc: Glenn, K. Robert
Subject: RE: List of Names

Roger,

Attached is an updated list based on follow-up discussions with some of the users. Note in particular that we found that the computer that we believed was being used by Thomas Bruno, was actually in use by a student of his that is working on final exams and may not be reachable until after break.

Regards,

Rob G.

Hurst V, Alfred Coulter

From: Hurst V, Alfred Coulter
Sent: Wednesday, December 08, 2010 11:53 AM
To: Beltz, John
Subject: Template
Attachments: WikiLeaks Template Document.docx

Document attached

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/>

Loebach, Matthew T.

From: Antonishek, John K.
Sent: Friday, December 17, 2010 10:02 AM
To: Kustaborder, David P.; siirt
Subject: Re: Linux/wiki

Yes, I'm okay with this plan.

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

From: David Kustaborder <kusty@nist.gov>
To: siirt
Sent: Fri Dec 17 09:33:22 2010
Subject: Linux/wiki

John,

We had a problem with one of the linux machines yesterday trying to clean up the wikileaks stuff.

Specs:

Mac hardware running rEFIt (boot menu toolkit for intel macs)
OS's: Window, OSX, ubuntu

Ubuntu was being used when wikileaks was accessed.

We couldn't boot to thumb drive or numerous live linux solutions. (the user said they have had problems with this machine in the past)

My plan (I did run this by Rob, he is fine with it)

I plan on just shredding the mozilla cache directory.

Command I plan on using.

```
cd ~/.mozilla/firefox/[whatever dir]/Cache/
```

```
find . -type f -exec shred -z -u {} \;
```

-z (write zeroes on final pass)

-u (truncate and remove file after overwriting)

Are you ok with this?

Re wikiclean 12-21-140pm.txt
From: Robert Sorensen [rsoren@boulder.nist.gov]
Sent: Tuesday, December 21, 2010 1:43 PM
To: Becker, Dan
Cc: Beltz, John; Sorensen, Robert
Subject: Re: wikiclean

Dan,

We finally got the instructions we need. I'll be in tomorrow as well.
Let me know.

-Robert

> Sounds good, just let me know.

>

> On 12/17/10 8:08 AM, Beltz, John wrote:

>> Hi Dan. That does make a difference. The SIRT team must have missed that
fact in there research. We are awaiting the official instructions for
cleaning MACs, so it may be a few days.

>>

>> I will be working in Gaithersburg next week so Robert Sorensen will contact
you when we have more information.

>>

>> Thanks,

>> John

>>

>>

>> From: Dan Becker [beckerd@boulder.nist.gov]

>> Sent: Thursday, December 16, 2010 3:18 PM

>> To: Beltz, John

>> Subject: wikiclean

>>

>> John,

>>

>> Since we keep playing phone tag, should we just set a time via email?
>> Would tomorrow morning at 8:30 AM work for you?

>>

>> One thing I should point out - I have a mac, not sure if that makes a
>> difference.

>>

>> Dan

>>

>> --

>> Dan Becker

>> 303/497-6824

Loebach, Matthew T.

From: Kustaborder, David P.
Sent: Tuesday, December 28, 2010 8:14 AM
To: Loebach, Matthew T.
Subject: FW: De-sanitization

Thanks

t
From: Heller, Gregory M.
Sent: Tuesday, December 21, 2010 6:16 PM
To: Kustaborder, David P.
Subject: RE: De-sanitization

Tuesday morning should work out call x6292 to reach me.
Thanks

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

From: David Kustaborder [mailto:kusty@nist.gov]
Sent: Tuesday, December 21, 2010 1:08 PM
To: Heller, Gregory M.
Subject: Re: De-sanitization

Thanks for the response. How is Tuesday morning?

I'll give you a call next week to confirm.

On 12/20/2010 05:52 PM, Heller, Gregory M. wrote:

> I will be here 3pm-11pm until the 24th, then next week 7am-3pm.
> Thanks

>

>

> -----Original Message-----

> **From:** David Kustaborder [mailto:kusty@nist.gov]
> **Sent:** Wednesday, December 15, 2010 3:26 PM
> **To:** Heller, Gregory M.
> **Subject:** De-sanitization

>

> Greg,

>

> I wanted to schedule a time that I could come by to work on cleaning
> up your computer due to accessing wikileaks.org.

>

> I usually get to work at around 5:00-5:30 am. If you could give me a
> call in the morning to determine what is the best time.

>

>

> Thanks,

>

> David Kustaborder

> OISM

>

Dolan, Brenda

From: Steve Needle [SNeedle@ntis.gov]
Sent: Tuesday, January 04, 2011 10:23 AM
To: Dolan, Brenda; Boyd, Harriette
Cc: Moton, Pat
Subject: CRRIF 11-0911 (NTIS 11-10)
Attachments: Wikileaks .pdf

Brenda/Harriet: I found this after I sent the package to Pat on this FOIA. Please add it to the file she sent. We have no objection to release.

Steve

Steve Needle

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, GSLC
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

From: William W. Bradd
To: Yu Nguyen
Subject: info
Date: 12/01/2010 08:50 AM

FYI --

wikileaks.org - 184.72.37.90 (ec2-184-72-37-90.us-west-1.compute.amazonaws.com)
www.wikileaks.org- 184.72.37.90 (ec2-184-72-37-90.us-west-1.compute.amazonaws.com)
cablegate.wikileaks.org - 204.236.131.131 (ec2-204-236-131-131.us-west-1.compute.amazonaws.com)

--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

From: William W. Bradd
To: Kenneth Harrison
Cc: Scott D. Williams; Timothy P. Ruland
Subject: WL blocking
Date: 12/01/2010 08:52 AM

Kenney,

Need to ensure the sites below are blocked. Know we have the first one, but want to ensure we have the other covered as well.

Thanks.

wikileaks.org - 184.72.37.90 (ec2-184-72-37-90.us-west-1.compute.amazonaws.com)
www.wikileaks.org - 184.72.37.90 (ec2-184-72-37-90.us-west-1.compute.amazonaws.com)
cablegate.wikileaks.org - 204.236.131.131 (ec2-204-236-131-131.us-west-1.compute.amazonaws.com)

--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

From: William W Bradd
To: Vu Nguyen
Subject: Fw: Guidance regarding WikiLeaks
Date: 12/01/2010 12:52 PM

Vu,

The broadcast is instructing employee's to contact the DOC CIRT, rather than their OU's CIRTs. This will make it hard for us to respond in a timely manor.

--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 12:51 PM -----

From: DOC Broadcast System
To:
Date: 12/01/2010 11:00 AM
Subject: Guidance regarding WikiLeaks
Sent Administrator
by:

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.

From: William W Bradd
To: Vu Nguyen
Subject: Fw: Wikileaks
Date: 12/03/2010 12:14 PM

FYI

--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 12/03/2010 12:12 PM -----

From: William W Bradd/ITSO/HQ/BOC
To: "Kenneth Harrison" <kenneth.r.harrison@census.gov>
Cc: Timothy P Ruland/ITSO/HQ/BOC@BOC, Scott D Williams/TCO/HQ/BOC@BOC
Date: 12/03/2010 10:05 AM
Subject: Wikileaks

Kenney,

With all that is going on wikileaks has started to move around and is available via alternative addresses.

Here are some additional blocks we need to address:

h-46-59-1-2.na.cust.bahnhof.se
ns201695.ovh.net
warlogs.owni.fr
911.wikileaks.org
calateralmurder.com
cauce.us
cgisecurity.de
chat.wikileaks.org
wikileakscom.org
citizen-q-usa.biz
citizen-q-usa.com
citizen-q-usa.info
citizen-q-usa.net
citizen-q-usa.org
citizen-q-usa.us
citizenq-usa.biz
citizenq-usa.com

citizenq-usa.info
citizenq-usa.net
citizenq-usa.org
citizenq-usa.us
citizenqusa.biz
citizenqusa.com
citizenqusa.info
citizenqusa.net
citizenqusa.org
citizenqusa.us
colatrilmurder.com
colateralmurder.com
collateralmurder.com
collateralmurder.org
digitalpublications.com
inbred.org
lasttry.org
ljsf.org
mail.home.e.co.za
mail.ljsf.org
mail.new.spacetechnology.net
mail.special.k.vu
mail.sunshinepress.org
mail.wikileaks.ch
socialsts-never-understand-much-including-dns.mo00.com
wikileaks.ch
wikileaks.de
wikileaks.eu
wikileaks.fi
wikileaks.nl
wikileaks.pl
www.cauce.us
www.collateralmurder.com
www.wikileaks.de
www.wikileaks.fi
213.251.145.96

--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

From: Jeffrey Wiley
To: Kenneth R Harrison
Cc: Benjamin A Padilla; TCO SSB Alerts List; William Bradd
Subject: Re: Incident INC000000131156 has been assigned to you. Priority: Medium. Description: PROXY CACHING
Date: 12/14/2010 08:03 AM

Thanks Kenny,

This is good and makes sense. However, when was the block initiated? I think that the directive to block the sites came after 26 Nov. So I guess the main question is: in the window of time that lapsed before it was blocked was anything cached? The date the directive came out was 30 Nov, so between 26-30 Nov. Let me know if this changes anything. Thanks for your help.

Cheers,

Jeff Wiley

Incident Response and Forensics Team
U.S. Census Bureau
Office: 301-763-0381

▼ Kenneth R Harrison---12/13/2010 05:13:29 PM---Jeff, The Wikkileaks sites are currently blocked in IronPort. If IronPort blocks the site, it does

From: Kenneth R Harrison/TCO/HQ/BOC
To: Jeffrey Wiley/ITSO/HQ/BOC@BOC
Cc: William Bradd <william.w.bradd@census.gov>, Benjamin A Padilla/ITSO/HQ/BOC@BOC, TCO SSB Alerts List
Date: 12/13/2010 05:13 PM
Subject: Re: Incident INC000000131156 has been assigned to you. Priority: Medium. Description: PROXY CACHING

Jeff,

The Wikkileaks sites are currently blocked in IronPort. If IronPort blocks the site, it does the cache the URLs.

Does this help?

Kenneth R Harrison
Chief, Census TCO Security Systems Branch
Desk: (301) 763-5561
Room: Suitland MD SFC 4K137
Paper Mail to:
Census, TCO SSB
SFC 4K137
Washington DC 20233

▼ IT REMEDY ITSM ---12/13/2010 04:17:23 PM---Incident INC000000131156 has been assigned to you. Service Type: User Service Request

From: IT REMEDY ITSM <itsm@remedy.it.census.gov>
To: kenneth.r.harrison@census.gov
Date: 12/13/2010 04:17 PM
Subject: Incident INC000000131156 has been assigned to you. Priority: Medium. Description: PROXY CACHING

Incident INC000000131156 has been assigned to you.
Service Type: User Service Request
Priority: Medium
Name: JEFFREY WILEY JR
JBond ID: wiley019
VIP: No
Organization: ITSO(28)
Department: INCIDENT RESPONSE&FORENSICS INVES
Summary: PROXY CACHING
Notes: Please review this list and let us know if any of these URLs or IP addresses have been cached by the proxy. The timeframe is between 26 Nov 2010 to the date that the search is executed. The following is the list:

wikileaks.org - 184.72.37.90 (ec2-184-72-37-90.us-west-1.compute.amazonaws.com)
www[dot]wikileaks[dot]org - 184.72.37.90 (ec2-184-72-37-90.us-west-1.compute.amazonaws.com)
cablegate.wikileaks.org - 204.236.131.131 (ec2-204-236-131-131.us-west-1.compute.amazonaws.com)
wikileaks.ch
h-46-59-1-2.na.cust.bahnhof.se
ns201695.ovh.net
warlogs.owni.fr
911.wikileaks.org
calateralmurder.com
cauce.us
cgisecurity.de
chat.wikileaks.org
wikileakscom.org
citizen-q-usa.biz
citizen-q-usa.com
citizen-q-usa.info
citizen-q-usa.net
citizen-q-usa.org
citizen-q-usa.us
citizenq-usa.biz
citizenq-usa.com
citizenq-usa.info
citizenq-usa.net
citizenq-usa.org
citizenq-usa.us
citizenqusa.biz
citizenqusa.com
citizenqusa.info
citizenqusa.net
citizenqusa.org
citizenqusa.us
colateralmurder.com
collateralmurder.com
collateralmurder.org
digitalpublications.com
inbred.org
lasttry.org
ljsf.org

mail.home.e.co.za
mail.ljsf.org
mail.new.spacetechnology.net
mail.special.k.vu
mail.sunshinepress.org
mail.wikileaks.ch
socialsts-never-understand-much-including-dns.mooo.com
wikileaks.ch
wikileaks.de
wikileaks.eu
wikileaks.fi
wikileaks.nl
wikileaks.pl
www[dot]cauce[dot]us
www[dot]collateralmurder[dot]com
www[dot]wikileaks[dot]de
www[dot]wikileaks[dot]fi
213.251.145.96

[attachment "ARNotification 578 NTS000005419509.ARTask" deleted
by Kenneth R Harrison/TCO/HQ/BOC]

Clark, Roger

From: Casias, Lisa
Sent: Wednesday, December 01, 2010 11:24 AM
To: Clark, Roger
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 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.

Clark, Roger

From: Batluck, Jonathan
Sent: Wednesday, December 01, 2010 7:27 AM
To: Clark, Roger
Cc: Nguyen, Vu
Subject: RE: Wikileaks Site Block ***Situational Awareness***

Great, thank you!

From: Clark, Roger
Sent: Wednesday, December 01, 2010 7:21 AM
To: Batluck, Jonathan
Cc: Nguyen, Vu
Subject: Re: Wikileaks Site Block ***Situational Awareness***

No only these that viewed content. Thanks for asking.

From: Batluck, Jonathan
To: Clark, Roger
Cc: Nguyen, Vu
Sent: Wed Dec 01 07:13:36 2010
Subject: FW: Wikileaks Site Block ***Situational Awareness***

Roger,

I went to wikileaks.org yesterday on my OSNET machine when working with Abner yesterday morning to implement the block. I believe that Doug Corey in the NOC and Abner also went there. I know that I personally did not view any of the content on the site. We were testing to see if the site block was successful or not.

Do we need to follow the same directions as below? Please advise.

Regards,

Jon

From: Blackwood, Wayne
Sent: Tuesday, November 30, 2010 4:36 PM
To: Ky, Wes; Harper, Pam; Fitzgerald, Erin
Cc: Sutch, Dennis; Whittington, Ron; Glover, Antwan; Batluck, Jonathan; Razavi, Shawn; Rogers, William
Subject: FW: Wikileaks Site Block ***Situational Awareness***

FYI

From: members of the Federation of Department of Commerce CIRTs and CIRCs <FEDCIRT@LIST.COMMERCE.GOV>
To: FEDCIRT@LIST.COMMERCE.GOV <FEDCIRT@LIST.COMMERCE.GOV>
Sent: Tue Nov 30 16:16:42 2010
Subject: Re: Wikileaks Site Block ***Situational Awareness***

Federation Team Members,

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:

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

SIPRNet: 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
SIPRNet: vnguyen@doc.sgov.gov
Phone: (202) 482-6401
Blackberry: (202) 834-9123

Clark, Roger

From: Eatmon, Jim
Sent: Wednesday, December 01, 2010 6:43 AM
To: Scalsky, Terry
Subject: FW: Wikileaks Site Block ***Situational Awareness***

Importance: High

This is rich.....

From: Whittington, Ron
Sent: Tuesday, November 30, 2010 8:14 PM
To: Rogers, William; Eatmon, Jim
Cc: Harper, Pam; Blackwood, Wayne
Subject: Fw: Wikileaks Site Block ***Situational Awareness***
Importance: High

Bill/Jim

Will we have the shelf stock to accomplish this work?

Ronald L. Whittington
Office of IT Services
Office of the Chief Information Officer
Office of the Secretary
U.S. Department of Commerce
Phone: 202 482-2373
Cell: 571 242-5382
Fax: 202 501-6073
RWhittington@doc.gov

From: Blackwood, Wayne
To: Ky, Wes; Harper, Pam; Fitzgerald, Erin
Cc: Sutch, Dennis; Whittington, Ron; Glover, Antwan; Batluck, Jonathan; Razavi, Shawn; Rogers, William
Sent: Tue Nov 30 16:36:04 2010
Subject: FW: Wikileaks Site Block ***Situational Awareness***

FYI

From: members of the Federation of Department of Commerce CIRTs and CIRCs <FEDCIRT@LIST.COMMERCE.GOV>
To: FEDCIRT@LIST.COMMERCE.GOV <FEDCIRT@LIST.COMMERCE.GOV>
Sent: Tue Nov 30 16:16:42 2010
Subject: Re: Wikileaks Site Block ***Situational Awareness***

Federation Team Members,

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

SIPRNet: vnguven@doc.sgov.gov

Phone: (202) 482-6401

Blackberry: (202) 834-9123

Clark, Roger

From: Clark, Roger
Sent: Wednesday, December 01, 2010 9:58 AM
To: Blackwood, Wayne
Cc: Neal, Earl; Westerback, Lisa; Szykman, Simon; Broadbent, Alfred
Subject: Broadcast Message

Importance: High

Wayne,

The following text has been approved by OSY, OCIO, and OGC. Please send to ALL Commerce Employees and Contractors as soon as possible. Thanks

To: All Commerce Employees and Contractors

Subject: Guidance regarding WikiLeaks

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.

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

Clark, Roger

From: Clark, Roger
Sent: Wednesday, December 01, 2010 10:00 AM
To: Glenn, K. Robert
Subject: FW: Broadcast Message

Importance: High

Here is an advance copy of the broadcast message.

From: Clark, Roger
Sent: Wednesday, December 01, 2010 9:58 AM
To: Blackwood, Wayne
Cc: Neal, Earl; Westerback, Lisa; Szykman, Simon; Broadbent, Alfred
Subject: Broadcast Message
Importance: High

Wayne,

The following text has been approved by OSY, OCIO, and OGC. Please send to ALL Commerce Employees and Contractors as soon as possible. Thanks

To: All Commerce Employees and Contractors

Subject: Guidance regarding WikiLeaks

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.

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

Clark, Roger

From: Clark, Roger
Sent: Wednesday, December 01, 2010 10:02 AM
To: Blackwood, Wayne
Subject: Re: Broadcast Message

Thanks wayne

From: Blackwood, Wayne
To: Slusarczyk, Theodore; Clark, Roger
Cc: Harper, Pam
Sent: Wed Dec 01 10:01:01 2010
Subject: Fw: Broadcast Message

Ted,

Please format and send immediately.

Thanks.

From: Clark, Roger
To: Blackwood, Wayne
Cc: Neal, Earl; Westerback, Lisa; Szykman, Simon; Broadbent, Alfred
Sent: Wed Dec 01 09:58:26 2010
Subject: Broadcast Message

Wayne,

The following text has been approved by OSY, OCIO, and OGC. Please send to ALL Commerce Employees and Contractors as soon as possible. Thanks

To: All Commerce Employees and Contractors

Subject: Guidance regarding WikiLeaks

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.

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

Clark, Roger

From: Batluck, Jonathan
Sent: Wednesday, December 01, 2010 7:14 AM
To: Clark, Roger
Cc: Nguyen, Vu
Subject: FW: Wikileaks Site Block ***Situational Awareness***

Importance: High

Roger,

I went to wikileaks.org yesterday on my OSNET machine when working with Abner yesterday morning to implement the block. I believe that Doug Corey in the NOC and Abner also went there. I know that I personally did not view any of the content on the site. We were testing to see if the site block was successful or not.

Do we need to follow the same directions as below? Please advise.

Regards,

Jon

From: Blackwood, Wayne
Sent: Tuesday, November 30, 2010 4:36 PM
To: Ky, Wes; Harper, Pam; Fitzgerald, Erin
Cc: Sutch, Dennis; Whittington, Ron; Glover, Antwan; Batluck, Jonathan; Razavi, Shawn; Rogers, William
Subject: FW: Wikileaks Site Block ***Situational Awareness***

FYI

From: members of the Federation of Department of Commerce CIRTs and CIRCs <FEDCIRT@LIST.COMMERCE.GOV>
To: FEDCIRT@LIST.COMMERCE.GOV <FEDCIRT@LIST.COMMERCE.GOV>
Sent: Tue Nov 30 16:16:42 2010
Subject: Re: Wikileaks Site Block ***Situational Awareness***

Federation Team Members,

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:

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

SIPRNet: 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

SIPRNet: vnguyen@doc.sgov.gov

Phone: (202) 482-6401

Blackberry: (202) 834-9123

Clark, Roger

From: Clark, Roger
Sent: Wednesday, December 01, 2010 10:37 AM
To: Slusarczyk, Theodore; Blackwood, Wayne
Cc: Harper, Pam; bcast-submit
Subject: RE: Broadcast Message - typo

Can you correct or do I need to resubmit?

From: Slusarczyk, Theodore
Sent: Wednesday, December 01, 2010 10:36 AM
To: Blackwood, Wayne; Clark, Roger
Cc: Harper, Pam; bcast-submit
Subject: Re: Broadcast Message - typo

WikiLeads appears once in this msg.

From: Blackwood, Wayne
To: Slusarczyk, Theodore; Clark, Roger
Cc: Harper, Pam
Sent: Wed Dec 01 10:01:01 2010
Subject: Fw: Broadcast Message

Ted,

Please format and send immediately.

Thanks.

From: Clark, Roger
To: Blackwood, Wayne
Cc: Neal, Earl; Westerback, Lisa; Szykman, Simon; Broadbent, Alfred
Sent: Wed Dec 01 09:58:26 2010
Subject: Broadcast Message

Wayne,

The following text has been approved by OSY, OCIO, and OGC. Please send to ALL Commerce Employees and Contractors as soon as possible. Thanks

To: All Commerce Employees and Contractors

Subject: Guidance regarding WikiLeaks

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.

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: roclark@doc.gov

Clark, Roger

From: Clark, Roger
Sent: Wednesday, December 01, 2010 10:39 AM
To: Eatmon, Jim; Nicoll, John
Subject: FW: Broadcast Message - typo

Please see below

From: Slusarczyk, Theodore
Sent: Wednesday, December 01, 2010 10:39 AM
To: Clark, Roger
Subject: Re: Broadcast Message - typo

You don't need to do anything. Whoever sends it out will correct it. You could give Jim or John a call if you want to be extra sure.

From: Clark, Roger
To: Slusarczyk, Theodore; Blackwood, Wayne
Cc: Harper, Pam; bcast-submit
Sent: Wed Dec 01 10:36:53 2010
Subject: RE: Broadcast Message - typo

Can you correct or do I need to resubmit?

From: Slusarczyk, Theodore
Sent: Wednesday, December 01, 2010 10:36 AM
To: Blackwood, Wayne; Clark, Roger
Cc: Harper, Pam; bcast-submit
Subject: Re: Broadcast Message - typo

WikiLeads appears once in this msg.

From: Blackwood, Wayne
To: Slusarczyk, Theodore; Clark, Roger
Cc: Harper, Pam
Sent: Wed Dec 01 10:01:01 2010
Subject: Fw: Broadcast Message

Ted,

Please format and send immediately.

Thanks.

From: Clark, Roger
To: Blackwood, Wayne
Cc: Neal, Earl; Westerbach, Lisa; Szykman, Simon; Broadbent, Alfred
Sent: Wed Dec 01 09:58:26 2010
Subject: Broadcast Message

Wayne,

The following text has been approved by OSY, OCIO, and OGC. Please send to ALL Commerce Employees and Contractors as soon as possible. Thanks

To: All Commerce Employees and Contractors

Subject: Guidance regarding WikiLeaks

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.

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

Clark, Roger

From: Blackwood, Wayne
Sent: Wednesday, December 01, 2010 10:01 AM
To: Slusarczyk, Theodore; Clark, Roger
Cc: Harper, Pam
Subject: Fw: Broadcast Message

Importance: High

Ted,

Please format and send immediately.

Thanks.

From: Clark, Roger
To: Blackwood, Wayne
Cc: Neal, Earl; Westerbach, Lisa; Szykman, Simon; Broadbent, Alfred
Sent: Wed Dec 01 09:58:26 2010
Subject: Broadcast Message

Wayne,

The following text has been approved by OSY, OCIO, and OGC. Please send to ALL Commerce Employees and Contractors as soon as possible. Thanks

To: All Commerce Employees and Contractors

Subject: Guidance regarding WikiLeaks

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.

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

Clark, Roger

From: Slusarczyk, Theodore
Sent: Wednesday, December 01, 2010 10:36 AM
To: Blackwood, Wayne; Clark, Roger
Cc: Harper, Pam; bcast-submit
Subject: Re: Broadcast Message - typo

WikiLeads appears once in this msg.

From: Blackwood, Wayne
To: Slusarczyk, Theodore; Clark, Roger
Cc: Harper, Pam
Sent: Wed Dec 01 10:01:01 2010
Subject: Fw: Broadcast Message

Ted,

Please format and send immediately.

Thanks.

From: Clark, Roger
To: Blackwood, Wayne
Cc: Neal, Earl; Westerbach, Lisa; Szykman, Simon; Broadbent, Alfred
Sent: Wed Dec 01 09:58:26 2010
Subject: Broadcast Message

Wayne,

The following text has been approved by OSY, OCIO, and OGC. Please send to ALL Commerce Employees and Contractors as soon as possible. Thanks

To: All Commerce Employees and Contractors

Subject: Guidance regarding WikiLeaks

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 WikiLeads 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.

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

Clark, Roger

From: william.w.bradd@census.gov
Sent: Wednesday, December 01, 2010 12:53 PM
To: Nguyen, Vu
Subject: Fw: Guidance regarding WikiLeaks

Vu,

The broadcast is instructing employee's to contact the DOC CIRT, rather than their OU's CIRTs. This will make it hard for us to respond in a timely manor.

--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 12:51 PM -----

From: DOC Broadcast System
To:
Date: 12/01/2010 11:00 AM
Subject: Guidance regarding WikiLeaks
Sent by: Administrator

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.

Clark, Roger

From: Lawless, George
Sent: Wednesday, December 01, 2010 1:15 PM
To: Peyman Goldoust
Cc: Anna Chai; Melonique Hayden
Subject: FW: Guidance regarding WikiLeaks

This e-mail is an excellent example of policy guidance on this specific issue and should be considered by outside contractors doing business with any Federal Government equipment as well. Just FYI

Regards,

George Lawless
Subject Matter Expert II - IT Security Policy Team GNS, Inc. Contractor Supporting
DOC/OCIO/OITSIT
1401 Constitution Avenue, NW (Room H6895) Washington, DC 20230
Phone: 202-482-6449
Fax: 202-482-1137

-----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 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.

Clark, Roger

From: Byrd, Teresa
Sent: Thursday, December 02, 2010 3:36 PM
To: Kramer, Shira
Subject: RE: Wash Post inquiry on DOC wikileaks guidance

Hi Shira,

Just checking to see if you were able to see if Simon responded. Thanks.\

t

Teresa A. Byrd

Secretary
Office of the Chief Information Officer
Phone: 202-482-4797
Fax: 201-501-1180
tbyrd@doc.gov

From: Kramer, Shira
Sent: Thursday, December 02, 2010 1:33 PM
To: Byrd, Teresa
Subject: RE: Wash Post inquiry on DOC wikileaks guidance

Thank you. Please keep in mind that press works on tight deadlines.

Shira Kramer

Deputy Press Secretary
Office of Public Affairs
U.S. Department of Commerce
skramer@doc.gov

From: Byrd, Teresa
Sent: Thursday, December 02, 2010 1:03 PM
To: Kramer, Shira; Millard, Mary Ann
Subject: RE: Wash Post inquiry on DOC wikileaks guidance

Thank you, I will bring it to Simon's attention.

Teresa A. Byrd

Secretary
Office of the Chief Information Officer
Phone: 202-482-4797
Fax: 201-501-1180
tbyrd@doc.gov

From: Kramer, Shira
Sent: Thursday, December 02, 2010 12:49 PM
To: Byrd, Teresa; Millard, Mary Ann
Subject: FW: Wash Post inquiry on DOC wikileaks guidance

In Joselyn's absence, adding you to this request for assistance.

Thanks,

Shira Kramer
Deputy Press Secretary
Office of Public Affairs
U.S. Department of Commerce
skramer@doc.gov

From: Kramer, Shira
Sent: Thursday, December 02, 2010 12:48 PM
To: Nguyen, Vu; Szykman, Simon
Cc: Bingham, Joselyn
Subject: Wash Post inquiry on DOC wikileaks guidance

Team CIO,

See the reporter inquiry we received from the Washington Post below regarding the DOC Broadcast guidance that was sent out yesterday on wikileaks.

I believe the answer is that "accessing" means we can't go to the site at all and "sanitation" means replacing the computer hard drive, but please confirm.

Thanks so much,

Shira Kramer
Deputy Press Secretary
Office of Public Affairs
U.S. Department of Commerce
skramer@doc.gov

From: Al Kamen [<mailto:kamena@washpost.com>]
Sent: Thursday, December 02, 2010 12:30 PM
To: Shah, Parita
Subject: Need some guidance

Commerce IT folks, pursuant to Obama's 12/29/09 Exec. order, cautioned employees not to look at the WikiLeaks stuff on their computers. There's a line I don't quite understand that says:
"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."

Does "accessing" in this case mean downloading or does it mean just looking at the stuff on your govt. computer.

Also, "sanitization" means? Wiping out your hard drive or something?

Clark, Roger

From: Title of BCast-Submit LISTSERV list [BCAST-SUBMIT@LIST.COMMERCE.GOV] on behalf of Eatmon, Jim [JEatmon@DOC.GOV]
Sent: Wednesday, December 01, 2010 10:51 AM
To: BCAST-SUBMIT_at_LIST.COMMERCE.GOV
Subject: FW: Broadcast Message - typo

From: Title of BCast-Submit LISTSERV list [<mailto:BCAST-SUBMIT@LIST.COMMERCE.GOV>] **On Behalf Of** Clark, Roger
Sent: Wednesday, December 01, 2010 10:37 AM
To: BCAST-SUBMIT_at_LIST.COMMERCE.GOV
Subject: Re: Broadcast Message - typo

Can you correct or do I need to resubmit?

From: Slusarczyk, Theodore
Sent: Wednesday, December 01, 2010 10:36 AM
To: Blackwood, Wayne; Clark, Roger
Cc: Harper, Pam; bcast-submit
Subject: Re: Broadcast Message - typo

WikiLeads appears once in this msg.

From: Blackwood, Wayne
To: Slusarczyk, Theodore; Clark, Roger
Cc: Harper, Pam
Sent: Wed Dec 01 10:01:01 2010
Subject: Fw: Broadcast Message

Ted,

Please format and send immediately.

Thanks.

From: Clark, Roger
To: Blackwood, Wayne
Cc: Neal, Earl; Westerback, Lisa; Szykman, Simon; Broadbent, Alfred
Sent: Wed Dec 01 09:58:26 2010
Subject: Broadcast Message

Wayne,

The following text has been approved by OSY, OCIO, and OGC. Please send to ALL Commerce Employees and Contractors as soon as possible. Thanks

To: All Commerce Employees and Contractors

Subject: Guidance regarding WikiLeaks

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.

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

Clark, Roger

From: Scalsky, Terry
Sent: Wednesday, December 01, 2010 6:45 AM
To: Eatmon, Jim
Subject: RE: Wikileaks Site Block ***Situational Awareness***

Arrgggg! Now you know what I was doing yesterday. I tried to argue him out of it. STUPID STUPID STUPID. Are we going to use the MIB mind ray on everyone who has watched fox or read the Times? Roger couldn't tell me HOW he was going to determine if anyone downloaded any of the files.

I just read the rest of the instructions. IS HE OUT OF HIS MIND!!!!!!!!!! OMG – this is going to be a very bad day if there were any OS users on that list.

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)

From: Eatmon, Jim
Sent: Wednesday, December 01, 2010 6:43 AM
To: Scalsky, Terry
Subject: FW: Wikileaks Site Block ***Situational Awareness***
Importance: High

This is rich.....

From: Whittington, Ron
Sent: Tuesday, November 30, 2010 8:14 PM
To: Rogers, William; Eatmon, Jim
Cc: Harper, Pam; Blackwood, Wayne
Subject: Fw: Wikileaks Site Block ***Situational Awareness***
Importance: High

Bill/Jim

Will we have the shelf stock to accomplish this work?

Ronald L. Whittington
Office of IT Services
Office of the Chief Information Officer
Office of the Secretary
U.S. Department of Commerce
Phone: 202 482-2373
Cell: 571 242-5382
Fax: 202 501-6073
RWhittington@doc.gov

From: Blackwood, Wayne
To: Ky, Wes; Harper, Pam; Fitzgerald, Erin
Cc: Sutch, Dennis; Whittington, Ron; Glover, Antwan; Batluck, Jonathan; Razavi, Shawn; Rogers, William
Sent: Tue Nov 30 16:36:04 2010
Subject: FW: Wikileaks Site Block ***Situational Awareness***

FYI

From: members of the Federation of Department of Commerce CIRTs and CIRCs <FEDCIRT@LIST.COMMERCE.GOV>
To: FEDCIRT@LIST.COMMERCE.GOV <FEDCIRT@LIST.COMMERCE.GOV>
Sent: Tue Nov 30 16:16:42 2010
Subject: Re: Wikileaks Site Block ***Situational Awareness***

Federation Team Members,

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:

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
SIPRNet: 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

SIPRNet: vnguyen@doc.sgov.gov

Phone: (202) 482-6401

Blackberry: (202) 834-9123

Clark, Roger

From: Razavi, Shawn
Sent: Wednesday, December 01, 2010 9:21 AM
To: Batluck, Jonathan
Subject: RE: Wikileaks Site Block ***Situational Awareness***

You are still an infidel!

From: Batluck, Jonathan
Sent: Wednesday, December 01, 2010 7:31 AM
To: Batluck, Jonathan; Rogers, William; Blackwood, Wayne; Ky, Wes
Cc: Glover, Antwan; Razavi, Shawn; Corey, Douglas
Subject: RE: Wikileaks Site Block ***Situational Awareness***

I emailed Roger this morning and he says that we are OK if we did not view content. I have reactivated my OSNET machine.

Jonathan Batluck
OCIO - HCHB Network & Telecommunications U.S. Dept. of Commerce
202.482.5556
jbatluck@doc.gov

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

From: Batluck, Jonathan
Sent: Tuesday, November 30, 2010 6:04 PM
To: Rogers, William; Blackwood, Wayne; Ky, Wes
Cc: Glover, Antwan; Razavi, Shawn; Corey, Douglas
Subject: RE: Wikileaks Site Block ***Situational Awareness***

Wayne, Bill, Wes:

I went to wikileaks.org this morning to ensure that the block requested by the SOC was working. I did not view any "leaks" of any nature, I went to the main page and to one page off the main page. In addition, I know that Doug Corey went to the site for testing purposes this morning.

Per this email, I have asked that Shawn unplug my workstation from the network as the first step.

Regards,

Jon

From: Rogers, William
Sent: Tuesday, November 30, 2010 4:38 PM
To: Blackwood, Wayne; Ky, Wes; Harper, Pam; Fitzgerald, Erin
Cc: Sutch, Dennis; Whittington, Ron; Glover, Antwan; Batluck, Jonathan; Razavi, Shawn
Subject: Re: Wikileaks Site Block ***Situational Awareness***

Amy came by and the hardware team went with her to remove the drives identified.

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: Razavi, Shawn
Sent: Wednesday, December 01, 2010 9:21 AM
To: Batluck, Jonathan
Subject: RE: Wikileaks Site Block ***Situational Awareness***

You are still an infidel!

From: Batluck, Jonathan
Sent: Wednesday, December 01, 2010 7:31 AM
To: Batluck, Jonathan; Rogers, William; Blackwood, Wayne; Ky, Wes
Cc: Glover, Antwan; Razavi, Shawn; Corey, Douglas
Subject: RE: Wikileaks Site Block ***Situational Awareness***

I emailed Roger this morning and he says that we are OK if we did not view content. I have reactivated my OSNET machine.

Jonathan Batluck
OCIO - HCHB Network & Telecommunications U.S. Dept. of Commerce
202.482.5556
jbatluck@doc.gov

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

From: Batluck, Jonathan
Sent: Tuesday, November 30, 2010 6:04 PM
To: Rogers, William; Blackwood, Wayne; Ky, Wes
Cc: Glover, Antwan; Razavi, Shawn; Corey, Douglas
Subject: RE: Wikileaks Site Block ***Situational Awareness***

Wayne, Bill, Wes:

I went to wikileaks.org this morning to ensure that the block requested by the SOC was working. I did not view any "leaks" of any nature, I went to the main page and to one page off the main page. In addition, I know that Doug Corey went to the site for testing purposes this morning.

Per this email, I have asked that Shawn unplug my workstation from the network as the first step.

Regards,

Jon

From: Rogers, William
Sent: Tuesday, November 30, 2010 4:38 PM
To: Blackwood, Wayne; Ky, Wes; Harper, Pam; Fitzgerald, Erin
Cc: Sutch, Dennis; Whittington, Ron; Glover, Antwan; Batluck, Jonathan; Razavi, Shawn
Subject: Re: Wikileaks Site Block ***Situational Awareness***

Amy came by and the hardware team went with her to remove the drives identified.

Bill Rogers
IT Customer Service Center
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: Blackwood, Wayne
To: Ky, Wes; Harper, Pam; Fitzgerald, Erin
Cc: Sutch, Dennis; Whittington, Ron; Glover, Antwan; Batluck, Jonathan; Razavi, Shawn; Rogers, William
Sent: Tue Nov 30 16:36:04 2010
Subject: FW: Wikileaks Site Block ***Situational Awareness***

FYI

From: members of the Federation of Department of Commerce CIRTs and CIRCs
<FEDCIRT@LIST.COMMERCE.GOV>
To: FEDCIRT@LIST.COMMERCE.GOV <FEDCIRT@LIST.COMMERCE.GOV>
Sent: Tue Nov 30 16:16:42 2010
Subject: Re: Wikileaks Site Block ***Situational Awareness*** Federation Team Members,

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:

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: Batluck, Jonathan
Sent: Wednesday, December 01, 2010 7:31 AM
To: Batluck, Jonathan; Rogers, William; Blackwood, Wayne; Ky, Wes
Cc: Glover, Antwan; Razavi, Shawn; Corey, Douglas
Subject: RE: Wikileaks Site Block ***Situational Awareness***

I emailed Roger this morning and he says that we are OK if we did not view content. I have reactivated my OSNET machine.

Jonathan Batluck
OCIO - HCHB Network & Telecommunications U.S. Dept. of Commerce
202.482.5556
jbatluck@doc.gov

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

From: Batluck, Jonathan
Sent: Tuesday, November 30, 2010 6:04 PM
To: Rogers, William; Blackwood, Wayne; Ky, Wes
Cc: Glover, Antwan; Razavi, Shawn; Corey, Douglas
Subject: RE: Wikileaks Site Block ***Situational Awareness***

Wayne, Bill, Wes:

I went to wikileaks.org this morning to ensure that the block requested by the SOC was working. I did not view any "leaks" of any nature, I went to the main page and to one page off the main page. In addition, I know that Doug Corey went to the site for testing purposes this morning.

Per this email, I have asked that Shawn unplug my workstation from the network as the first step.

Regards,

Jon

From: Rogers, William
Sent: Tuesday, November 30, 2010 4:38 PM
To: Blackwood, Wayne; Ky, Wes; Harper, Pam; Fitzgerald, Erin
Cc: Sutch, Dennis; Whittington, Ron; Glover, Antwan; Batluck, Jonathan; Razavi, Shawn
Subject: Re: Wikileaks Site Block ***Situational Awareness***

Amy came by and the hardware team went with her to remove the drives identified.

Bill Rogers
IT Customer Service Center
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: Blackwood, Wayne
To: Ky, Wes; Harper, Pam; Fitzgerald, Erin
Cc: Sutch, Dennis; Whittington, Ron; Glover, Antwan; Batluck, Jonathan; Razavi, Shawn; Rogers, William
Sent: Tue Nov 30 16:36:04 2010
Subject: FW: Wikileaks Site Block ***Situational Awareness***

FYI

From: members of the Federation of Department of Commerce CIRTs and CIRCs
<FEDCIRT@LIST.COMMERCE.GOV>
To: FEDCIRT@LIST.COMMERCE.GOV <FEDCIRT@LIST.COMMERCE.GOV>
Sent: Tue Nov 30 16:16:42 2010
Subject: Re: Wikileaks Site Block ***Situational Awareness*** Federation Team Members,

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:

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: Plummer, Christopher
Sent: Friday, December 10, 2010 1:47 PM
To: Plummer, Christopher
Cc: DOC-CIRT
Subject: RE: Incident 30241 - New Group Assignment Notification

Roger,

It looks like helpdesk created a new ticket for this incident today. I guess the user called in again looking for her files. I called helpdesk and had them connect the two tickets.

Do you have an update on the status of her files?

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

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

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

-----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: Sequoyah Stamps
Office: HCHB

Category: Employee Access

Description: Sequoyah's 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 Sequoyah"

Please review the assignment and follow up accordingly.

Thank you.

Clark, Roger

From: Kramer, Shira
Sent: Thursday, December 02, 2010 12:48 PM
To: Nguyen, Vu; Szykman, Simon
Cc: Bingham, Joselyn
Subject: Wash Post inquiry on DOC wikileaks guidance

Team CIO,

See the reporter inquiry we received from the Washington Post below regarding the DOC Broadcast guidance that was sent out yesterday on wikileaks.

I believe the answer is that "accessing" means we can't go to the site at all and "sanitation" means replacing the computer hard drive, but please confirm.

Thanks so much,

Shira Kramer
Deputy Press Secretary
Office of Public Affairs
U.S. Department of Commerce
skramer@doc.gov

From: Al Kamen [<mailto:kamena@washpost.com>]
Sent: Thursday, December 02, 2010 12:30 PM
To: Shah, Parita
Subject: Need some guidance

Commerce IT folks, pursuant to Obama's 12/29/09 Exec. order, cautioned employees not to look at the WikiLeaks stuff on their computers. There's a line I don't quite understand that says:
"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."

Does "accessing" in this case mean downloading or does it mean just looking at the stuff on your govt. computer.

Also, "sanitization" means? Wiping out your hard drive or something?

Clark, Roger

From: jason.templeman@census.gov
Sent: Wednesday, December 01, 2010 3:36 PM
To: DOC-CIRT
Subject: WikiLeaks

Hello,

Does reading news articles on CNN or MSNBC related to the release necessitate computer sanitization?

Thank you,
Jason Templeman

Clark, Roger

From: Anthony, Darren
Sent: Wednesday, December 01, 2010 2:57 PM
To: Helzer, Anne
Subject: FW: Guidance regarding WikiLeaks

-----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 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.

Clark, Roger

From: Clark, Roger
Sent: Wednesday, December 01, 2010 9:58 AM
To: Blackwood, Wayne
Cc: Neal, Earl; Westerback, Lisa; Szykman, Simon; Broadbent, Alfred
Subject: Broadcast Message

Importance: High

Wayne,

The following text has been approved by OSY, OCIO, and OGC. Please send to ALL Commerce Employees and Contractors as soon as possible. Thanks

To: All Commerce Employees and Contractors

Subject: Guidance regarding WikiLeaks

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.

v/r
Roger Clark
Senior Advisor
National & Cyber Security
Office of the Chief Information Officer
U.S. Department of Commerce
Phone: (202) 482-0121

Clark, Roger

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 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.

Clark, Roger

From: Szykman, Simon
Sent: Thursday, December 02, 2010 2:26 PM
To: Kramer, Shira
Cc: Szykman, Simon
Subject: RE: Wash Post inquiry on DOC wikileaks guidance

Shira,

Answers to Mr. Kamen's questions appear below. I generally don't get technical with reporters, but in this case the technical explanation is important because it explains why even accessing documents and web pages without explicitly saving them to your machine can be problematic.

Does "accessing" in this case mean downloading or does it mean just looking at the stuff on your govt. computer.

A user downloading and saving data to a computer is an issue for obvious reasons, but in this case accessing does mean "just looking at stuff". The reason why simply accessing information is just problematic as a user who saves files to a computer is slightly technical. Many kinds of applications, including web browsers, automatically save data that is accessed/viewed even when a user takes no action to save a file or web page to their machine. This automatic background saving, called caching, is done to speed up access to the same information should it be accessed again in the future. As described in this Microsoft technical note, a web browser can cache a variety of items accessed online, including web pages and images: <http://www.microsoft.com/windows/ie/ie6/using/howto/customizing/clearcache.msp> (While that note applies to Internet Explorer 6, this caching functionality is generally inherent in web browsers as well as many other kinds of applications.) In addition to web pages and images, stand-alone files (e.g., a Word document) that are accessed online, even though they are not themselves web pages, can likewise get saved in a similar way. In all of these cases, this saving happens in the background without the user taking any action of their own to save files to their computer, which is why just users just viewing content is a concern.

Also, "sanitization" means? Wiping out your hard drive or something?

Yes, but to certain established standards. Using a typical hard disk drive formatting utility available on most computers, for example, does not adequately wipe the information that is stored on the drive and would not be sufficient.

- Simon

--

Chief Information Officer
U.S. Department of Commerce

Clark, Roger

From: Scalsky, Terry
Sent: Thursday, December 09, 2010 11:43 AM
To: Desir, Abner; Kim, Jun
Subject: 11 meeting

The whole WAP thing was covered at the meeting. Ron wants a scan done on the suspect stuff. Dale is convinced the laptop is compromised and some outside party is trying to exfiltrate data so the laptop even if it is GFE, is compromised. Me personally not so sure. Without following the traffic flow I couldn't say. Do we have the info and what do you think of Dale's thoughts? Of course Ron wants EVERY laptop now scanned for wikileaks. Let's hope that idea dies.

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)

Clark, Roger

From: Szykman, Simon
Sent: Friday, December 03, 2010 11:45 AM
To: Szykman, Simon; Clark, Roger; Neal, Earl
Cc: Westerback, Lisa; Dornell, Izella
Subject: RE: DOC and Wikileaks in the press

All,

I was glad to see this follow-up to yesterdays somewhat negative slant on the DOC Wikileaks guidance memo:
<http://www.theatlantic.com/national/archive/2010/12/more-about-secret-info-on-the-front-page/67423/>
The new article provides some more supportive perspectives on the reason for taking this kind of action.

- Simon

--

Chief Information Officer
U.S. Department of Commerce

Clark, Roger

From: Szykman, Simon
Sent: Thursday, December 02, 2010 2:53 PM
To: Clark, Roger; Neal, Earl
Cc: Westerback, Lisa; Dornell, Izella
Subject: DOC and Wikileaks in the press

FYI: <http://www.theatlantic.com/national/archive/2010/12/why-not-just-stamp-secret-across-the-front-page-of-the-ny-times/67310/>

And based on a separate inquiry, there may be some coverage in the Post as well.

- Simon

--

Chief Information Officer
U.S. Department of Commerce

Clark, Roger

From: Neal, Earl
Sent: Friday, December 03, 2010 1:39 PM
To: Szykman, Simon; Clark, Roger; Hurr, Tim
Subject: Re: DOC and Wikileaks in the press

Finally something positive and factual.
Earl Neal

From: Szykman, Simon
To: Szykman, Simon; Clark, Roger; Neal, Earl
Cc: Westerback, Lisa; Dornell, Izella
Sent: Fri Dec 03 11:45:18 2010
Subject: RE: DOC and Wikileaks in the press

All,

I was glad to see this follow-up to yesterdays somewhat negative slant on the DOC Wikileaks guidance memo:
<http://www.theatlantic.com/national/archive/2010/12/more-about-secret-info-on-the-front-page/67423/>
The new article provides some more supportive perspectives on the reason for taking this kind of action.

- Simon

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

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 "ABukhari" 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

202-482-5010

Clark, Roger

From: Clark, Roger
Sent: Wednesday, December 01, 2010 1:05 PM
To: MZAHIR@DOCFCU.ORG
Subject: FW: Guidance regarding WikiLeaks

Here is the broadcast that we discussed.

-----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 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.

Clark, Roger

From: Plummer, Christopher
Sent: Wednesday, December 01, 2010 3:55 PM
To: Clark, Roger
Cc: Templeman, Jason
Subject: FW: WikiLeaks

Roger,

This is another Wikileaks email from the DOC-CIRT general email.

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

From: jason.templeman@census.gov [<mailto:jason.templeman@census.gov>]
Sent: Wednesday, December 01, 2010 3:36 PM
To: DOC-CIRT
Subject: WikiLeaks

Hello,

Does reading news articles on CNN or MSNBC related to the release necessitate computer sanitization?

Thank you,
Jason Templeman

Clark, Roger

From: Jenkins, Brenda
Sent: Wednesday, December 01, 2010 9:04 AM
To: Sutch, Dennis
Subject: Re: Wikileaks Site Block ***Situational Awareness***

Not I. Thank goodness!
Brenda Jenkins
Webmaster/Developer
U.S. Department of Commerce
Office of the Secretary/CIO
202.482.0247
Email: bjenkins@doc.gov

From: Sutch, Dennis
To: Wood, Tim; Jenkins, Brenda; Gautsch, Daniel; Severe, William
Sent: Tue Nov 30 16:39:24 2010
Subject: FW: Wikileaks Site Block ***Situational Awareness***

FYI... Let's hope none of us have accessed WikiLeaks.org website in the last few days, otherwise we're going to be missing some workstations.

--
Dennis Sutch
OITS/OCIO/U.S. Dept. of Commerce
202-730-9453 (mobile)
202-482-2564 (office)

From: Blackwood, Wayne
Sent: Tuesday, November 30, 2010 4:36 PM
To: Ky, Wes; Harper, Pam; Fitzgerald, Erin
Cc: Sutch, Dennis; Whittington, Ron; Glover, Antwan; Batluck, Jonathan; Razavi, Shawn; Rogers, William
Subject: FW: Wikileaks Site Block ***Situational Awareness***
Importance: High

FYI

From: members of the Federation of Department of Commerce CIRTs and CIRCs <FEDCIRT@LIST.COMMERCE.GOV>
To: FEDCIRT@LIST.COMMERCE.GOV <FEDCIRT@LIST.COMMERCE.GOV>
Sent: Tue Nov 30 16:16:42 2010
Subject: Re: Wikileaks Site Block ***Situational Awareness***

Federation Team Members,

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:

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
SIPRNet: 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
SIPRNet: vnguyen@doc.sgov.gov
Phone: (202) 482-6401
Blackberry: (202) 834-9123

Clark, Roger

From: Counsel, General
Sent: Monday, December 06, 2010 11:08 AM
To: Broadcast, DOC
Subject: Follow-up Guidance on WikiLeaks

Last week, you received notice from the Department's Office of CIO and Office of Security reminding you that, even though the classified government documents released by Wikileaks have been posted online and discussed widely in the media, they remain classified and have to be treated as such by federal employees and contractors.

We received additional guidance from OMB on Friday (which you may have read about over the weekend) about obligations for treatment of classified information and the use of non-classified government information technology systems. OMB's guidance appears below.

Cameron F. Kerry
General Counsel
United States Department of Commerce
1401 Constitution Avenue, NW, Room 5870
Washington, DC 20230

tel: 202-482-4772
email: generalcounsel@doc.gov
web: www.ogc.doc.gov

- 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.

Clark, Roger

From: Slusarczyk, Theodore
Sent: Wednesday, December 01, 2010 10:39 AM
To: Clark, Roger
Subject: Re: Broadcast Message - typo

You don't need to do anything. Whoever sends it out will correct it. You could give Jim or John n a call if you want to be extra sure.

From: Clark, Roger
To: Slusarczyk, Theodore; Blackwood, Wayne
Cc: Harper, Pam; bcast-submit
Sent: Wed Dec 01 10:36:53 2010
Subject: RE: Broadcast Message - typo

Can you correct or do I need to resubmit?

From: Slusarczyk, Theodore
Sent: Wednesday, December 01, 2010 10:36 AM
To: Blackwood, Wayne; Clark, Roger
Cc: Harper, Pam; bcast-submit
Subject: Re: Broadcast Message - typo

WikiLeads appears once in this msg.

From: Blackwood, Wayne
To: Slusarczyk, Theodore; Clark, Roger
Cc: Harper, Pam
Sent: Wed Dec 01 10:01:01 2010
Subject: Fw: Broadcast Message

Ted,

Please format and send immediately.

Thanks.

From: Clark, Roger
To: Blackwood, Wayne
Cc: Neal, Earl; Westerback, Lisa; Szykman, Simon; Broadbent, Alfred
Sent: Wed Dec 01 09:58:26 2010
Subject: Broadcast Message

Wayne,

The following text has been approved by OSY, OCIO, and OGC. Please send to ALL Commerce Employees and Contractors as soon as possible. Thanks

To: All Commerce Employees and Contractors

Subject: Guidance regarding WikiLeaks

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.

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: roclark@doc.gov

Clark, Roger

From: Plummer, Christopher
Sent: Monday, December 06, 2010 11:09 AM
To: Clark, Roger; Whiteside, Fred
Subject: FW: Follow-up Guidance on WikiLeaks

From: Counsel, General
Sent: Monday, December 06, 2010 11:08:18 AM
To: Broadcast, DOC
Subject: Follow-up Guidance on WikiLeaks
Auto forwarded by a Rule

Last week, you received notice from the Department's Office of CIO and Office of Security reminding you that, even though the classified government documents released by Wikileaks have been posted online and discussed widely in the media, they remain classified and have to be treated as such by federal employees and contractors.

We received additional guidance from OMB on Friday (which you may have read about over the weekend) about obligations for treatment of classified information and the use of non-classified government information technology systems. OMB's guidance appears below.

Cameron F. Kerry
General Counsel
United States Department of Commerce
1401 Constitution Avenue, NW, Room 5870
Washington, DC 20230

tel: 202-482-4772
email: generalcounsel@doc.gov
web: www.ogc.doc.gov

- 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.

Murphy, Latoya

From: Michelle Mitchell [Michelle.Duff-Mitchell@trade.gov]
Sent: Wednesday, December 01, 2010 2:53 PM
To: Murray, Jennifer; Murphy, Latoya; Canceko, Lyle; Grant, Cedric; Itana, Bontu; Williams, Edward; Cue, Christina
Subject: FW: Guidance regarding WikiLeaks

Importance: High

Some of these broadcast are worth reading-- like today's re: Wikileaks.

Cliff notes version-- don't go on their website and access content bc some information may be classified on the site and if you download it you will get in trouble. This applies to your work laptops and bbs too.

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

From: Broadcast, DOC [mailto:broadcast@doc.gov]
Sent: Wednesday, December 01, 2010 10:57 AM
To: broadcast
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.

DiGiacomo, Brian

From: Szykman, Simon
Sent: Sunday, December 05, 2010 11:09 PM
To: Kerry, Cameron; Ehrenwerth, Justin
Cc: DiGiacomo, Brian; Reich, Jay
Subject: RE: Draft Further Broadcast

Looks good to me, Cam.

- Simon

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

From: Kerry, Cameron
Sent: Sunday, December 05, 2010 7:23 PM
To: Szykman, Simon; Ehrenwerth, Justin
Cc: DiGiacomo, Brian; Reich, Jay
Subject: Draft Further Broadcast

Last week, you received notice from the Department's Office of CIO and Office of Security reminding you that, even though the classified government documents released by Wikileaks have been posted online and discussed widely in the media, they remain classified and have to be treated as such by federal employees and contractors.

We received additional guidance from OMB on Friday (which you may have read about over the weekend) about obligations for treatment of classified information and the use of non-classified government information technology systems. OMB's guidance appears below.

*
Cameron F. Kerry
General Counsel
United States Department of Commerce
1401 Constitution Avenue, NW, Room 5870
Washington, DC 20230

tel: 202-482-4772
email: generalcounsel@doc.gov<<mailto:generalcounsel@doc.gov>>
web: www.ogc.doc.gov<<http://www.ogc.doc.gov>>

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.

Clark, Roger

From: Plummer, Christopher [CPlummer@doc.gov]
Sent: Thursday, December 02, 2010 4:13 PM
To: Clark, Roger
Subject: FW: Wikileaks Site Block ***Situational Awareness***

From: Pardun, John[SMTP:JOHN.PARDUN@USPTO.GOV]
Sent: Thursday, December 02, 2010 4:13:06 PM
To: DOC-CIRT
Cc: Turk, Rod; Blevins, Michael; Nguyen, Vu
Subject: RE: Wikileaks Site Block ***Situational Awareness***
Auto forwarded by a Rule

USPTO has complied with the below instructions for all users that accessed the WiliLeaks.or site as instructed.

The hard drives are at USPTO and are being appropriately stored by the USPTO CIRT team awaiting further guidance.

Thank you,

John Pardun, CISSP
Director, Cybersecurity Division
OCIO Office of Organizational Policy and Governance
US Patent and Trademark Office
Madison West (MDW), 5th Floor, Room 5D01
Office (571) 272-4349

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 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:

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
SIPRNet: 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
SIPRNet: vnguyen@doc.sgov.gov
Phone: (202) 482-6401
Blackberry: (202) 834-9123

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 11.am 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

Clark, Roger

From: Slusarczyk, Theodore
Sent: Wednesday, December 01, 2010 10:31 AM
To: Blackwood, Wayne; Clark, Roger
Cc: Harper, Pam; bcast-submit
Subject: Re: Broadcast Message

I'm not in until 1:00 today. Ccing our bcast senders.

From: Blackwood, Wayne
To: Slusarczyk, Theodore; Clark, Roger
Cc: Harper, Pam
Sent: Wed Dec 01 10:01:01 2010
Subject: Fw: Broadcast Message

Ted,

Please format and send immediately.

Thanks.

From: Clark, Roger
To: Blackwood, Wayne
Cc: Neal, Earl; Westerback, Lisa; Szykman, Simon; Broadbent, Alfred
Sent: Wed Dec 01 09:58:26 2010
Subject: Broadcast Message

Wayne,

The following text has been approved by OSY, OCIO, and OGC. Please send to ALL Commerce Employees and Contractors as soon as possible. Thanks

To: All Commerce Employees and Contractors

Subject: Guidance regarding WikiLeaks

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.

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

Clark, Roger

From: Clark, Roger
Sent: Wednesday, December 01, 2010 4:05 PM
To: Ruland, Timothy P
Subject: FW: WikiLeaks

Tim – since this is a Census employee I will let you answer. Our view is that reading news articles is permissible as long as they do not click on links that take them to the WikiLink site or another site that contains the source document.

Roger

From: Plummer, Christopher
Sent: Wednesday, December 01, 2010 3:55 PM
To: Clark, Roger
Cc: Templeman, Jason
Subject: FW: WikiLeaks

Roger,

This is another Wikileaks email from the DOC-CIRT general email.

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

From: jason.templeman@census.gov [<mailto:jason.templeman@census.gov>]
Sent: Wednesday, December 01, 2010 3:36 PM
To: DOC-CIRT
Subject: WikiLeaks

Hello,

Does reading news articles on CNN or MSNBC related to the release necessitate computer sanitization?

Thank you,
Jason Templeman

Clark, Roger

From: timothy.p.ruland@census.gov
Sent: Wednesday, December 01, 2010 4:11 PM
To: Clark, Roger
Cc: Bradd, William W; Musselman, Patricia Trainor
Subject: Re: FW: WikiLeaks

taken care of, if you get any more send them to Bill Bradd as well. I am off-site tomorrow and on Friday.

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

From: "Clark, Roger" <RClark@doc.gov>
To: "Ruland, Timothy P" <Timothy.P.Ruland@census.gov>
Date: 12/01/2010 04:05 PM
Subject: FW: Wikileaks

Tim - since this is a Census employee I will let you answer. Our view is that reading news articles is permissible as long as they do not click on links that take them to the Wikilink site or another site that contains the source document.

Roger

From: Plummer, Christopher
Sent: Wednesday, December 01, 2010 3:55 PM
To: Clark, Roger
Cc: Templeman, Jason
Subject: FW: Wikileaks

Roger,

This is another Wikileaks email from the DOC-CIRT general email.

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

From: jason.templeman@census.gov [<mailto:jason.templeman@census.gov>]
Sent: Wednesday, December 01, 2010 3:36 PM
To: DOC-CIRT
Subject: WikiLeaks

Hello,

Does reading news articles on CNN or MSNBC related to the release necessitate computer sanitization?

Thank you,
Jason Templeman

From: Whiteside, Fred
Sent By: members of the Federation of Department of Commerce CIRTs and CIRCs
Reply To: members of the Federation of Department of Commerce CIRTs and CIRCs
To: FEDCIRT@LIST.COMMERCE.GOV
Subject: Wikileaks DNS Change
Date: 12/03/2010 01:35 PM

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)*

From: [William W Bradd](#)
To: FWhiteside@DOC.GOV
Cc: [Timothy P Ruland](#)
Subject: Re: Wikileaks DNS Change
Date: 12/03/2010 03:58 PM

Actually, they can be accessed via the following:

h-46-59-1-2.na.cust.bahnhof.se
ns201695.ovh.net
warlogs.owni.fr
911.wikileaks.org
calateralmurder.com
cauce.us
cgisecurity.de
chat.wikileaks.org
wikileakscom.org
citizen-q-usa.biz
citizen-q-usa.com
citizen-q-usa.info
citizen-q-usa.net
citizen-q-usa.org
citizen-q-usa.us
citizenq-usa.biz
citizenq-usa.com
citizenq-usa.info
citizenq-usa.net
citizenq-usa.org
citizenq-usa.us
citizenqusa.biz
citizenqusa.com
citizenqusa.info
citizenqusa.net
citizenqusa.org
citizenqusa.us
colatrilmurder.com
colatteralmurder.com
collateralmurder.com
collateralmurder.org
digitalpublications.com
inbred.org
lasttry.org
ljsf.org
mail.home.e.co.za
mail.ljsf.org
mail.new.spacetechnology.net
mail.special.k.vu
mail.sunshinepress.org
mail.wikileaks.ch
socialsts-never-understand-much-including-dns.mo00.com
wikileaks.ch
wikileaks.de
wikileaks.eu

wikileaks.fi
wikileaks.nl
wikileaks.pl
www.cauce.us
www.collateralmurder.com
www.wikileaks.de
www.wikileaks.fi
213.251.145.96

--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

▼ "Whiteside, Fred" ---12/03/2010 01:35:06 PM---Federation Team Members... APR
and CNN just announced Wikileaks has changed its DNS domain.

From: "Whiteside, Fred" <FWhiteside@DOC.GOV>
To: FEDCIRT@LIST.COMMERCE.GOV
Date: 12/03/2010 01:35 PM
Subject: Wikileaks DNS Change
Sent: members of the Federation of Department of Commerce CIRTs and CIRCs
by: <FEDCIRT@LIST.COMMERCE.GOV>

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)*

Pardun, John

From: Pardun, John
Sent: Wednesday, December 01, 2010 4:49 PM
To: Nguyen, Vu; 'DOC-CIRT@doc.gov'
Cc: Turk, Rod; Blevins, Michael
Subject: RE: Wikileaks Site Block ***Situational Awareness***

As requested, below are the names of users that accessed the Wikileaks.org web site from USPTO's network. We expect to be able to provide final status on collection of the associated hard drives tomorrow. Most of them have already been secured as instructed.

[REDACTED] NR

Thank you,

John Pardun, CISSP
Director, Cybersecurity Division
OCIO Office of Organizational Policy and Governance
US Patent and Trademark Office
Madison West (MDW), 5th Floor, Room 5D01
Office (571) 272-4349

From: Pardun, John
Sent: Tuesday, November 30, 2010 4:41 PM
To: Nguyen, Vu
Cc: Turk, Rod; Blevins, Michael

12/28/2010

Subject: RE: Wikileaks Site Block ***Situational Awareness***

We currently have their USPTO usernames. We will be able to provide the names tomorrow for the purpose of the inadvertent disclosure debrief.

Thanks,

John Pardun, CISSP

Director, Cybersecurity Division
OCIO Office of Organizational Policy and Governance
US Patent and Trademark Office
Madison West (MDW), 5th Floor, Room 5D01
Office (571) 272-4349

From: Nguyen, Vu
Sent: Tuesday, November 30, 2010 4:34 PM
To: Pardun, John; DOC-CIRT
Cc: Turk, Rod; Blevins, Michael
Subject: RE: Wikileaks Site Block ***Situational Awareness***

John,

Please provide us the list of the 22 individuals at USPTO because they may need a security debriefs.

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
SIPRNet: vnguyen@doc.sgov.gov
Phone: (202) 482-6401
Blackberry: (202) 834-9123

From: Pardun, John [mailto:John.Pardun@USPTO.GOV]
Sent: Tuesday, November 30, 2010 3:20 PM
To: DOC-CIRT
Cc: Nguyen, Vu; Turk, Rod; Blevins, Michael
Subject: FW: Wikileaks Site Block ***Situational Awareness***

DOC-CIRT,

USPTO has completed the below requested action by blocking both at Enterprise firewalls and using Bluecoat URL filtering. We have also obtained a list of users that accessed the site since Friday November 26th. USPTO plans to clean the web cache on systems of users that accessed the Wikileaks web site. 22 unique users were identified as having accessed the site. We can provide detail on specific links visited and USPTO network usernames accessing the website when needed.

Please let us know if additional information or action is required.

Thank you,

John Pardun, CISSP

Director, Cybersecurity Division
OCIO Office of Organizational Policy and Governance
US Patent and Trademark Office
Madison West (MDW), 5th Floor, Room 5D01
Office (571) 272-4349

From: Turk, Rod
Sent: Tuesday, November 30, 2010 12:02 PM
To: Pardun, John; Blevins, Michael
Subject: FW: Wikileaks Site Block ***Situational Awareness***
Importance: High

Action due today...

Rod Turk
Director, Office of Organizational Policy and Governance
U.S. Patent & Trademark Office
571-272-1975
rod.turk@uspto.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 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: vnguyen@doc.gov
SIPRNet: vnguyen@doc.sgov.gov
Phone: (202) 482-6401
Blackberry: (202) 834-9123

RE: New Wikileaks Sinkhole Request

[REDACTED]

[REDACTED]

"NR"

From: Schiller, Susannah B.
Sent: Friday, December 03, 2010 8:21 AM
To: Glenn, K. Robert
Subject: RE: New Wikileaks Sinkhole Request

"NR"

[REDACTED]

Doesn't anyone work early in the morning? I just tried every number again (except the Boulder folks), and uniformly got voice mail!

[REDACTED]

[REDACTED]

[REDACTED]

"NR"

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

E: New Wikileaks Sinkhole Request

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
SIPRNet: vnnguyen@doc.sgov.gov
Phone: (202) 482-6401
Blackberry: (202) 834-9123

On 11/16/2010 11:51 AM, Chambers, William wrote:
Network Team:

Please implement ASAP a sinkhole to the following domains. This is related to the infection this morning on Kevin Kimball's machine. The domains are being redirected to from legitimate research si

blogsmonitoringservice.com
casuism.com

Bill Chambers, CISSP, GCIA, GCFW
IT Specialist
IT Security and Networking Division
National Institute of Standards and Technology 100 Bureau Drive Mail Stop 1812 Gaithersburg, MD 20899-1812
301.975.8483 (office)

Schmidt, Carolyn M.

From: Glenn, K. Robert
Sent: Tuesday, December 07, 2010 8:16 AM
To: Antonishek, John K.; Enloe, Christian; Schmidt, Carolyn M.; Waltermire, Karen; Richter, Gale C.
Cc: Glenn, K. Robert
Subject: Draft IT Security Working Group Meeting Agenda for December 14, 2010

[REDACTED]

[REDACTED]

NR

[REDACTED]

[REDACTED]

NR

[REDACTED]

[REDACTED]

- Status/Update on Wikileaks incident

[REDACTED]

[REDACTED]

NR

Katzman, Esther S.

From: ou_secur@nist.gov on behalf of Glenn, K. Robert [robert.glenn@nist.gov]
Sent: Friday, December 10, 2010 1:20 PM
To: Multiple recipients of list
Subject: Draft IT Security Working Group Meeting Agenda for December 14, 2010

Draft agenda below, please let me know if there is anything to include.

IT Security Working Group Meeting Agenda for December 14, 2010

[REDACTED]

"NR"

[REDACTED] "NR"

[REDACTED]

"NR"

- Status/Update on Wikileaks incident

[REDACTED]

"NR"

[REDACTED]

Katzman, Esther S.

From: ou_secur@nist.gov on behalf of Glenn, K. Robert [robert.glenn@nist.gov]
Sent: Tuesday, December 14, 2010 9:10 AM
To: Multiple recipients of list
Subject: RE: Draft IT Security Working Group Meeting Agenda for December 14, 2010

Updated agenda below.

IT Security Working Group Meeting Agenda for December 14, 2010

[REDACTED] "NR"

[REDACTED] "NR"

[REDACTED] "NR"

- Status/Update on Wikileaks incident

[REDACTED] "NR"

Schiller, Susannah B.

From: oismsecure@nist.gov on behalf of Glenn, K. Robert [robert.glenn@nist.gov]
Sent: Friday, December 17, 2010 1:30 PM
To: Multiple recipients of list
Subject: RE: Notes from IT Security Working Group Meeting -- 12/14/10

Thanks, Chuck.

Minor clarification on wikileaks. DoC recommended that we remove the drives and send to DoC, but to minimize impact, the SIIRT team (with help from Robert Sorensen and John Beltz in Boulder) has been going to each user and machine, permanently removing any relevant files.

Rob G.

From: oismsecure@nist.gov [mailto:oismsecure@nist.gov] **On Behalf Of** Charles L. Eater
Sent: Friday, December 17, 2010 1:14 PM
To: Multiple recipients of list
Subject: Notes from IT Security Working Group Meeting -- 12/14/10

All,

Here are some notes from this month's IT Security Working Group Meeting.

[REDACTED]

[REDACTED] "NR"

[REDACTED]

[REDACTED] "NR"

[REDACTED]

[REDACTED] "NR"

[REDACTED]

[REDACTED] "NR"

[REDACTED]

This page
is
non-responsive
and
is being
marked
“NR”

[REDACTED]

NR

[REDACTED]

[REDACTED]

NR

[REDACTED]

[REDACTED]

NR

[REDACTED]

[REDACTED]

NR

[REDACTED]

- Status/Update on Wikileaks incident

- 36 users at NIST accessed the WikiLeaks site prior to the prohibition on such access.
- We have since blocked access to the site.
- We are removing drives from the systems that did access the site and those drives will be sent to the Department in a secure container since they must be treated as possibly containing classified information.
- Rob made it clear that from Pat Gallagher down it has been stated that no one will be in any trouble over the site access since it all occurred prior to any prohibition on access.

[REDACTED]

NR

[REDACTED]

[REDACTED]

NR

[REDACTED]

[REDACTED]

NR

[REDACTED]

This page
is
non-responsive
and
is being
marked
“NR”

RE: Foreign Nationals or US citizens

Subject: RE: Foreign Nationals or US citizens

From: "Glenn, K. Robert" <robert.glenn@nist.gov>

Date: Mon, 6 Dec 2010 12:13:50 -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>

I've now sent emails to the remaining 10 individuals on the list. One has responded to the emails that the access was not by him, but rather a student of his, and that he talked to the student. I've asked for the student's name, and am still waiting for it. Once I get that name, I'll send them a copy of the email and I'll send an update of the list to Roger, with all of the current information.

Rob G.

From: Glenn, K. Robert

Sent: Friday, December 03, 2010 4:45 PM

To: Glenn, K. Robert; Schiller, Susannah B.; Brockett, Del

Cc: Glenn, K. Robert

Subject: RE: Foreign Nationals or US citizens

I just went through my list one more time, no additional hits. Overall, we still need to contact 9 people that we know of. We've now been told by ITL/CSD that they will get us the last user name on Monday morning.

Rob G.

From: Glenn, K. Robert

Sent: Friday, December 03, 2010 3:46 PM

To: Schiller, Susannah B.; Brockett, Del

Cc: Glenn, K. Robert

Subject: RE: Foreign Nationals or US citizens

Susannah, Thank you very much for all of your help with this! I've updated my notes accordingly.

(b)(2) Also, I just got a call from John & David, they identified another incorrect user (one you spoke with), Afzal Godil. The computer actually is used by another guest researcher, [REDACTED]. Unfortunately, [REDACTED] found out the hard way, when SIIRT showed up to start sanitizing the computer and found that Afzal's computer was not the one in question. I've since contacted [REDACTED] went over the script and reassured him that he was not in trouble. I've also asked Yali for nationality information for [REDACTED] (b)(2)

[REDACTED] "NR"

Rob G.

From: Schiller, Susannah B.

Sent: Friday, December 03, 2010 3:27 PM

To: Brockett, Del; Glenn, K. Robert

Subject: RE: Foreign Nationals or US citizens

I made one more pass and got one more person.

Attached is the status of all my contacts

From: Brockett, Del
Sent: Friday, December 03, 2010 2:01 PM
To: Glenn, K. Robert; Schiller, Susannah B.
Subject: RE: Foreign Nationals or US citizens

Agreed let's try at least one more time today.

I will also send the complete list to Mike.

Del

From: Glenn, K. Robert
Sent: Friday, December 03, 2010 1:58 PM
To: Glenn, K. Robert; Schiller, Susannah B.; Brockett, Del
Cc: Glenn, K. Robert
Subject: RE: Foreign Nationals or US citizens

We now have 10 users left (by my records) that have not been contacted, and 1 unknown user. I'll likely try one more time today, but I really need to focus on other issues that I've been putting off all week.

Rob G.

From: Glenn, K. Robert
Sent: Friday, December 03, 2010 1:42 PM
To: Schiller, Susannah B.; Brockett, Del
Cc: Glenn, K. Robert
Subject: RE: Foreign Nationals or US citizens

Me too, I reached [REDACTED] but no one else.

Rob G. (b)(2)

From: Schiller, Susannah B.
Sent: Friday, December 03, 2010 1:36 PM
To: Glenn, K. Robert; Brockett, Del
Subject: RE: Foreign Nationals or US citizens

I just made another try at everyone left on my half of the list. I talked to [REDACTED] but I didn't reach anyone else. (b)(2)

From: Glenn, K. Robert
Sent: Friday, December 03, 2010 12:30 PM
To: Brockett, Del
Cc: Schiller, Susannah B.; Glenn, K. Robert
Subject: RE: Foreign Nationals or US citizens

1 NR!

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

E: Foreign Nationals or US citizens

NR"

[REDACTED]

Clark, Roger

From: Byrd, Teresa
Sent: Thursday, December 02, 2010 1:03 PM
To: Kramer, Shira; Millard, Mary Ann
Subject: RE: Wash Post inquiry on DOC wikileaks guidance

Thank you, I will bring it to Simon's attention.

Teresa A. Byrd

Secretary
Office of the Chief Information Officer
Phone: 202-482-4797
Fax: 201-501-1180
tbyrd@doc.gov

From: Kramer, Shira
Sent: Thursday, December 02, 2010 12:49 PM
To: Byrd, Teresa; Millard, Mary Ann
Subject: FW: Wash Post inquiry on DOC wikileaks guidance

In Joselyn's absence, adding you to this request for assistance.

Thanks,

Shira Kramer
Deputy Press Secretary
Office of Public Affairs
U.S. Department of Commerce
skramer@doc.gov

From: Kramer, Shira
Sent: Thursday, December 02, 2010 12:48 PM
To: Nguyen, Vu; Szykman, Simon
Cc: Bingham, Joselyn
Subject: Wash Post inquiry on DOC wikileaks guidance

Team CIO,

See the reporter inquiry we received from the Washington Post below regarding the DOC Broadcast guidance that was sent out yesterday on wikileaks.

I believe the answer is that "accessing" means we can't go to the site at all and "sanitation" means replacing the computer hard drive, but please confirm.

Thanks so much,

Shira Kramer
Deputy Press Secretary
Office of Public Affairs
U.S. Department of Commerce
skramer@doc.gov

From: Al Kamen [<mailto:kamena@washpost.com>]

Sent: Thursday, December 02, 2010 12:30 PM

To: Shah, Parita

Subject: Need some guidance

Commerce IT folks, pursuant to Obama's 12/29/09 Exec. order, cautioned employees not to look at the WikiLeaks stuff on their computers. There's a line I don't quite understand that says:

"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."

Does "accessing" in this case mean downloading or does it mean just looking at the stuff on your govt. computer.

Also, "sanitization" means? Wiping out your hard drive or something?

Clark, Roger

From: Plummer, Christopher [CPlummer@doc.gov]
Sent: Wednesday, December 01, 2010 4:49 PM
To: Clark, Roger
Subject: FW: Wikileaks Site Block ***Situational Awareness***

From: Pardun, John[SMTP:JOHN.PARDUN@USPTO.GOV]
Sent: Wednesday, December 01, 2010 4:48:51 PM
To: Nguyen, Vu; DOC-CIRT
Cc: Turk, Rod; Blevins, Michael
Subject: RE: Wikileaks Site Block ***Situational Awareness***
Auto forwarded by a Rule

As requested, below are the names of users that accessed the Wikileaks.org web site from USPTO's network. We expect to be able to provide final status on collection of the associated hard drives tomorrow. Most of them have already been secured as instructed.



Thank you,

John Pardun, CISSP
Director, Cybersecurity Division
OCIO Office of Organizational Policy and Governance
US Patent and Trademark Office
Madison West (MDW), 5th Floor, Room 5D01

From: Pardun, John
Sent: Tuesday, November 30, 2010 4:41 PM
To: Nguyen, Vu
Cc: Turk, Rod; Blevins, Michael
Subject: RE: Wikileaks Site Block ***Situational Awareness***

We currently have their USPTO usernames. We will be able to provide the names tomorrow for the purpose of the inadvertent disclosure debrief.

Thanks,

John Pardun, CISSP
Director, Cybersecurity Division
OCIO Office of Organizational Policy and Governance
US Patent and Trademark Office
Madison West (MDW), 5th Floor, Room 5D01
Office (571) 272-4349

From: Nguyen, Vu
Sent: Tuesday, November 30, 2010 4:34 PM
To: Pardun, John; DOC-CIRT
Cc: Turk, Rod; Blevins, Michael
Subject: RE: Wikileaks Site Block ***Situational Awareness***

John,

Please provide us the list of the 22 individuals at USPTO because they may need a security debriefs.

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
SIPRNet: vnnguyen@doc.sgov.gov
Phone: (202) 482-6401
Blackberry: (202) 834-9123

From: Pardun, John [<mailto:John.Pardun@USPTO.GOV>]
Sent: Tuesday, November 30, 2010 3:20 PM
To: DOC-CIRT
Cc: Nguyen, Vu; Turk, Rod; Blevins, Michael
Subject: FW: Wikileaks Site Block ***Situational Awareness***

DOC-CIRT,

USPTO has completed the below requested action by blocking both at Enterprise firewalls and using Bluecoat URL filtering. We have also obtained a list of users that accessed the site since Friday November 26th. USPTO plans to

clean the web cache on systems of users that accessed the Wikileaks web site. 22 unique users were identified as having accessed the site. We can provide detail on specific links visited and USPTO network usernames accessing the website when needed.

Please let us know if additional information or action is required.

Thank you,

John Pardun, CISSP

Director, Cybersecurity Division
OCIO Office of Organizational Policy and Governance
US Patent and Trademark Office
Madison West (MDW), 5th Floor, Room 5D01
Office (571) 272-4349

From: Turk, Rod
Sent: Tuesday, November 30, 2010 12:02 PM
To: Pardun, John; Blevins, Michael
Subject: FW: Wikileaks Site Block ***Situational Awareness***
Importance: High

Action due today...

Rod Turk
Director, Office of Organizational Policy and Governance
U.S. Patent & Trademark Office
571-272-1975
rod.turk@uspto.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 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: vnguyen@doc.gov

SIPRNet: vnnguyen@doc.sgov.gov

Phone: (202) 482-6401

Blackberry: (202) 834-9123

Clark, Roger

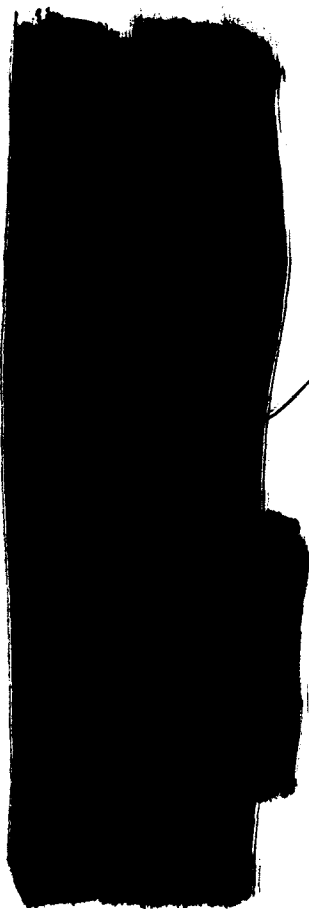
From: Clark, Roger
Sent: Wednesday, December 01, 2010 4:50 PM
To: Dorsey, Eric
Subject: FW: Wikileaks Site Block ***Situational Awareness***

PTO listing

From: Plummer, Christopher [mailto:CPlummer@doc.gov]
Sent: Wednesday, December 01, 2010 4:49 PM
To: Clark, Roger
Subject: FW: Wikileaks Site Block ***Situational Awareness***

From: Pardun, John[SMTP:JOHN.PARDUN@USPTO.GOV]
Sent: Wednesday, December 01, 2010 4:48:51 PM
To: Nguyen, Vu; DOC-CIRT
Cc: Turk, Rod; Blevins, Michael
Subject: RE: Wikileaks Site Block ***Situational Awareness***
Auto forwarded by a Rule

As requested, below are the names of users that accessed the Wikileaks.org web site from USPTO's network. We expect to be able to provide final status on collection of the associated hard drives tomorrow. Most of them have already been secured as instructed.



NR


Thank you,

John Pardun, CISSP

Director, Cybersecurity Division
OCIO Office of Organizational Policy and Governance
US Patent and Trademark Office
Madison West (MDW), 5th Floor, Room 5D01
Office (571) 272-4349

From: Pardun, John
Sent: Tuesday, November 30, 2010 4:41 PM
To: Nguyen, Vu
Cc: Turk, Rod; Blevins, Michael
Subject: RE: Wikileaks Site Block ***Situational Awareness***

We currently have their USPTO usernames. We will be able to provide the names tomorrow for the purpose of the inadvertent disclosure debrief.

Thanks,

John Pardun, CISSP

Director, Cybersecurity Division
OCIO Office of Organizational Policy and Governance
US Patent and Trademark Office
Madison West (MDW), 5th Floor, Room 5D01
Office (571) 272-4349

From: Nguyen, Vu
Sent: Tuesday, November 30, 2010 4:34 PM
To: Pardun, John; DOC-CIRT
Cc: Turk, Rod; Blevins, Michael
Subject: RE: Wikileaks Site Block ***Situational Awareness***

John,

Please provide us the list of the 22 individuals at USPTO because they may need a security debriefs.

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
SIPRNet: vnguyen@doc.sgov.gov
Phone: (202) 482-6401
Blackberry: (202) 834-9123

From: Pardun, John [mailto:John.Pardun@USPTO.GOV]
Sent: Tuesday, November 30, 2010 3:20 PM
To: DOC-CIRT
Cc: Nguyen, Vu; Turk, Rod; Blevins, Michael
Subject: FW: Wikileaks Site Block ***Situational Awareness***

DOC-CIRT,

USPTO has completed the below requested action by blocking both at Enterprise firewalls and using Bluecoat URL filtering. We have also obtained a list of users that accessed the site since Friday November 26th. USPTO plans to clean the web cache on systems of users that accessed the Wikileaks web site. 22 unique users were identified as having accessed the site. We can provide detail on specific links visited and USPTO network usernames accessing the website when needed.

Please let us know if additional information or action is required.

Thank you,

John Pardun, CISSP

Director, Cybersecurity Division
OCIO Office of Organizational Policy and Governance
US Patent and Trademark Office
Madison West (MDW), 5th Floor, Room 5D01
Office (571) 272-4349

From: Turk, Rod
Sent: Tuesday, November 30, 2010 12:02 PM
To: Pardun, John; Blevins, Michael
Subject: FW: Wikileaks Site Block ***Situational Awareness***
Importance: High

Action due today...

Rod Turk
Director, Office of Organizational Policy and Governance
U.S. Patent & Trademark Office
571-272-1975
rod.turk@uspto.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 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: vnguyen@doc.gov
SIPRNet: vnguyen@doc.sgov.gov
Phone: (202) 482-6401
Blackberry: (202) 834-9123