DEPARTMENT OF DEFENSE
UNITED STATES CYBER COMMAND
9800 SAVAGE ROAD, Suite 6171
FORT GEORGE G. MEADE, MARYLAND 20755

Reply to:
Chief of Staff

January 8, 2018

Mr. John Greenwald
27305 W. Live Oak Road
Suite #1203
Castaic, CA 91384

Dear Mr. Greenwald,

Thank you for your 21 Nov 2017 Freedom of Information Act request. U.S. Strategic Command referred your request to U.S. Cyber Command on 22 Nov 2017 for processing. After carefully reviewing the enclosed document, I have determined certain portions are releasable. However, there are portions I am withholding.

As the Initial Denial Authority, I am partially denying the enclosed document as specific information is currently and properly classified in the interest of national defense or foreign policy according to Executive Order 13526, *Classified National Security Information*, Section 1.4(a). I am also denying the release of certain UNCLASSIFIED portions as they meet the standards for classification pursuant to Executive Order 13526, Section 1.7.(e). Specifically, when these UNCLASSIFIED portions are combined, they reveal an additional association or relationship that: 1) meets the standards for classification under Executive Order 13526; and 2) are not otherwise revealed in the individual items of information. I am also denying portions located on page six as release could pose a risk of harm to U.S. Cyber Command operations.

In accordance with 5 U.S.C. § 552, *Freedom of Information Act*, Exemptions 1 and 7(E) are hereby invoked, and require this information be withheld.

If you are not satisfied with this action, you may appeal this response to the appellate authority, Ms. Joo Chung, Director of Oversight and Compliance, Office of the Secretary of Defense. The appellate address is: ODCMO, Director of Oversight and Compliance, 4800 Mark Center Drive ATTN: DPCLTD, FOIA Appeals, Mailbox #24, Alexandria VA 22350-1700. As an alternative, you may use the OSD FOIA request portal at http://pal.whs.mil/palMain.aspx; or e-mail your appeal to OSD.FOIA-APPEAL@mail.mil. Your appeal should be submitted within 90 calendar days of this letter and should cite case number 18-020, and be clearly marked "Freedom of Information Act Appeal."

Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows: Office of Government Information

Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, e-mail at ogis@nara.gov; telephone at (202) 741-5770; toll free at 1-977-684-6448; or facsimile at (202) 741-5769.

Sincerely

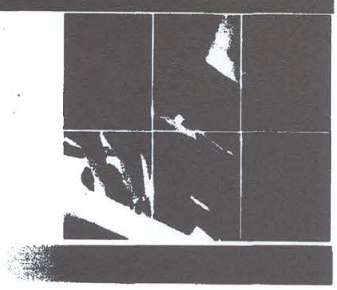
STEPHEN G. FOGARTY
Major General, USA
Chief of Staff

UNITED STATES STRATEGIC COMMAND

United States Cyber Command

Fusion Cell

SAR 2010-SA-0025



(U//~~FOUO~~) Situational Awareness Report 2010-SA-0025 WikiLeaks Release of Classified Documents from a Department of State Database

(U) Date: 02 December 2010

(U) Table of Contents

(U) Summary

(~~S//NF~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) WikiLeaks says the material will be posted in 'stages' over the next few months. Diplomatic Security cables referencing (b)(1) Sec 1.4(a) are among the leaked (b)(1) Sec documents and have already been referenced by a US media organization. **[A]**

(~~S//NF~~) During 2010, WikiLeaks has already uploaded hundreds of thousands of classified documents known as the (b)(1) Sec 1.4(a) In the recent months, (b)(1) Sec 1.4(a) actors have shown increasing interest in obtaining sensitive documents posted on the WikiLeaks website. In July 2010, a (b)(1) Sec 1.4(a) visited the WikiLeaks page and downloaded classified Department of Defense (DoD) and Coalition documents and data associated with Operation Enduring Freedom (OEF) and Operation Iraqi Freedom (OIF). On 9 October 2010, (b)(1) Sec 1.4(a) logged into a compromised U.S. hop point and performed reconnaissance on the WikiLeaks website. **[B, C]**

(~~S//NF~~) The release of the latest set of classified data will likely result in observable changes in OPSEC procedures, coordination and collaboration among Computer Network Operations (CNO) organizations, Tactics, Techniques, and Procedures (TTPs), and overall sophistication levels (b)(1) Sec 1.4(a) USCC expects (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) S Although the direct implications will be resident with (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) USCC expects that other Foreign Intelligence Services (FIS) active in CNO against the US will use this information to tailor their respective (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) as "lessons learned".

(U//~~FOUO~~) Impact to Cyber Operations

(~~S//NF~~) On 16 November 2010, the IRTF provided an initial assessment of the (b)(1) Sec 1.4(a) (b)(1) Sec believed to have been compromised from the (b)(1) Sec These documents have been in WikiLeak's possession (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) **The SIPRNET version of the (b)(1) S database has been temporarily suspended by State, but the JWICS site at (b)(1) Sec 1.4(a) is accessible to everyone and should be used to identify equities specific to your organization. [A]**

(~~S//NF~~) USCC, NSA, and LECI components have conducted (b)(1) Sec 1.4(a) database in an effort to identify documents that may disclose cyber operations equities. The following sections summarize various categories of information relating to cyber operations that are likely to be exposed via WikiLeaks.

~~(U//FOUO)~~ Named Area of Interests (NAI)

~~(S//NF)~~ A number of cables were identified as having disclosed U.S. government's insight (b)(1) Sec 1.4(a)

~~(S//NF)~~ At this time, there is no indication that information on the U.S. Government's (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

~~(U//FOUO)~~ Adversary TTPs

~~(S//NF)~~ The (b)(1) S cables clearly state that U.S. Government entities have knowledge of specific adversary TTPs, including malware, toolsets, IP addresses, and domains used in intrusion activity. One of the documents also highlighted DoD's knowledge and tracking of adversary's use of (b)(1) Sec 1.4(a) data. In particular, the reports identify (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) technologies. The collected data also identifies (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) those systems. The adversary TTPs and indicators that were disclosed are (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) to monitor, detect, and counter these threats.

~~(S//NF)~~ (b)(1) Sec 1.4(are expected to modify their current infrastructure and intrusion techniques. Based on adversary changes, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Public disclosure of this information may impact (b)(1) Sec 1.4(a) of near and long term threats.

~~(U//FOUO)~~ U.S. Government Entities and Personnel

~~(S//NF)~~ Included in the (b)(1) S cables are detailed reports on the results of audits conducted at (b)(1) Sec 1.4 locations (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

~~(S//NF)~~ The (b)(1) S cables included names, contact information, and job titles (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) The IRTF also reported that a significant number of reports originated from (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(~~S//NF~~) The implications of a FIS becoming aware of U.S. Government and DoD involvement in cyber related missions and equities is (b)(1) Sec 1.4(a) (b)(1) Sec 1. The individuals referenced in the DCD cables (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(U) Mitigation

(U//~~FOUO~~) Renaming of Intrusion Sets

(~~S//REL TO USA, FVEY~~) As a consequence of the possible compromise of the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) A permanent Inter-agency working group will be established to manage intrusion set names and indicator sets. This effort will result in improved analysis and reporting across Team Cyber.

(U//~~FOUO~~) Short term mitigation strategies

(~~S//NF~~) The possible spillage may result (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) DoD Components should consider the following mitigation actions. These may be implemented temporarily around the release of this information or, if feasible, left in-place permanently:

- Ensure compliance with standing INFOCON-3 requirements for e-mail security, specifically (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)
- Ensure compliance with all email security guidance and requirements in DISA's Security Technical Implementation Guides (STIGs) and (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)
- Based on mission constraints and Command risk tolerance, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) by a experienced security-conscious administrator.

- DoD Components should deny access to (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)
- E-mail system administrators and Computer Network Defense Service Providers (CNDSPs) should review all email logs for suspicious email message characteristics. This includes (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)
- DoD Components should reinforce standard Spear-phishing Awareness Training issues such as:
  - Do not open attachments or click on links in emails from unknown senders
  - Consider the (b)(1) Sec 1.4(a) level of trust of an (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) It is always advisable to (b)(1) Sec 1.4(a) on an attachment or URL link.
  - Users must be as vigilant when using personal email accounts from home as they are when using official email accounts.

(U) Conclusion

(~~S//NF~~) The overall impact to the DoD cyber missions (b)(1) Sec 1.4(a) cables are expected to reveal a (b)(1) Sec 1.4(a) which include (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) It is imperative that all DoD and IC organizations remain vigilant to changes, network traffic anomalies, or an fluctuations in malicious activity relative to status quo activity as this new information is released and circulated in the public domain. All organizations must be observant to potential efforts of our adversaries to leverage this new information against DoD in efforts to further their cyber initiatives (b)(1) Sec 1.4(a)

(U) Additional Information

(U//~~FOUO~~) For more information, contact the (b)(1) Sec 1.7(e) (b)(1) Sec 1. directly and reference this SAR.

(U//~~FOUO~~) Additional situational awareness reports can be found (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(U) References

A. S-10-0222/IRTF, Review of State Department Cables for Department of Defense Equities, 16 Sep 2010

B. (b)(1) Sec 1.7(e)
Downloaded Classified DoD and Coalition Documents from Wikileaks in July and August 2010, 22 Nov 2010

C. (b)(1) Sec 1.7(e)

(U) Contact Information

For all questions relating to network defense, please contact (b)(7)(E)
(b)(7)(E)
SIPRNET E-mail (b)(7)(E)
Phone: (COMM:

For all questions relating to intelligence assessment, please contact the J2 Intel Watch:
SIPRNET E-mail (b)(7)(E)
Phone: (COMM:

Derived from: ~~Multiple Sources~~
Declassify on: ~~20351129~~