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

NOV 2 4 2020

John Greenewald
The Black Vault
27305 W Live Oak Rd, Ste 1203
Castaic, CA 91384-4520

Re: 21-M001

Dear Mr. Greenewald,

Thank you for your November 14, 2020, Mandatory Declassification Review (MDR) request of Situational Awareness Report (SAR) 2010-SA-0025.

As the Initial Denial Authority, I have determined that the record contains material still meeting the standards for classification as established by Executive Order 13526. Some unclassified material is also exempt from disclosure under Title 5, United States Code, section 552(b)(3).

If you are not satisfied with our action on this request, you may file an administrative appeal. Information about the exemptions cited and the appeal process is enclosed.

DAVID T. ISAACSON
Major General, U.S. Army
Chief of Staff

Attachments:
Enclosure a/s

Exemptions Cited:

Executive Order 13526, Classified National Security Information:
Section 1.4(a) – military plans, weapons systems, or operations
Section 1.7(e) – individually unclassified items of information that reveal an additional association or relationship that (1) meets the standards for classification under this order; and (2) is not otherwise revealed in the individual items of information

Title 5, United States Code, Section 552, Freedom of Information Act:
(b)(3) – information specifically exempted from disclosure by statute
10 U.S.C. § 130e – defense critical infrastructure security information

Administrative Appeal:

USCYBERCOM/J0 FOIA
9800 Savage Road, Suite 6171
Fort George G. Meade, MD 20755
Phone: (301) 688-3585
Email: cybercom_foia@cybercom.mil

* Appeal should cite case number above, be clearly marked "MDR Appeal" and filed within 60 calendar days from the date of this letter.

This document is made available through the declassification efforts
and research of John Greenewald, Jr., creator of:

The Black Vault

The Black Vault is the largest online Freedom of Information Act (FOIA) document clearinghouse in the world. The research efforts here are responsible for the declassification of hundreds of thousands of pages released by the U.S. Government & Military.

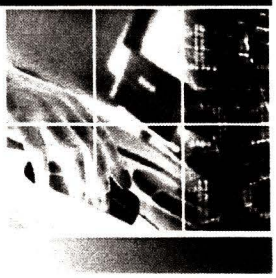
Discover the Truth at: **http://www.theblackvault.com**

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

E.O. 13526 Sec. 1.4(a)

(U) Summary

(~~S//NF~~) The internet-based [ ] WikiLeaks and its media partners are in the process of posting to the internet [ ] documents extracted [ ] [ ]. WikiLeaks says the material will be posted in 'stages' over the next few months. Diplomatic Security cables referencing [ ] are among the leaked [ ] 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 [ ]. In the recent months, [ ] actors have shown increasing interest in obtaining sensitive documents posted on the WikiLeaks website. In July 2010, 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, [ ] 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 [ ]. USCC expects [ ] to modify their cyber operations against the U.S. in order to maintain [ ]. These changes [ ] [ ] Although the direct implications will be resident with [ ] [ ] USCC expects that other Foreign Intelligence Services (FIS) active in CNO against the US will use this information to tailor their respective [ ] [ ] as "lessons learned".

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

(~~S//NF~~) On 16 November 2010, the IRTF provided an initial assessment of the [ ] [ ] believed to have been compromised from the [ ] These documents have been in WikiLeak's possession [ ] [ ]. **The SIPRNET version of the [ ] database has been temporarily suspended by State, but the JWICS site at [ ] 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 [ ] 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)

E.O. 13526 Sec. 1.4(a)

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

(~~S//NF~~) At this time, there is no indication that information on the U.S. Government's to WikiLeaks.

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

(~~S//NF~~) The 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 data. In particular, the reports identify technologies. The collected data also identifies capabilities on those systems. The adversary TTPs and indicators that were disclosed are to monitor, detect, and counter these threats.

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

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

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

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

diplomats and government officials, government agency . **[A]**

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

(U) Mitigation

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

(~~S//REL TO USA, FVEY~~) As a consequence of the possible compromise of the

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

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 NIPRNet email
- Ensure compliance with all email security guidance and requirements in DISA's Security Technical Implementation Guides (STIGs) and
- Based on mission constraints and Command risk tolerance, by a experienced security-conscious administrator.

- DoD Components should deny access to [redacted] DoD systems.
- E-mail system administrators and Computer Network Defense Service Providers (CNDSPs) should review all email logs for suspicious email message characteristics. This includes [redacted]
- 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 [redacted] level of trust of an [redacted] It is always advisable to verify the origination of an email prior to clicking 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 [redacted] cables are expected to reveal a [redacted] which include [redacted] Based upon this release, it is expected that these actors will modify [redacted] 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 [redacted].

(U) Additional Information

5 U.S.C. § 552
(b)(3) 10 U.S.C. § 130e

(U//~~FOUO~~) For more information, contact the [redacted] directly and reference this SAR.

(U//~~FOUO~~) Additional situational awareness reports can be found [redacted]

(U) References

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

B. [redacted]

E.O. 13526 Sec. 1.7(e)

Downloaded Classified DoD and Coalition Documents from Wikileaks in July and August 2010, 22 Nov 2010

C. [redacted]

(U) Contact Information

For all questions relating to network defense, please contact [redacted]

[redacted]

SIPRNET E-mail [redacted]

Phone: (COMM: [redacted]

5 U.S.C. § 552
(b)(3) 10 U.S.C. § 130e

For all questions relating to intelligence assessment, please contact the J2 Intel Watch:

SIPRNET E-mail [redacted]

Phone: (COMM: [redacted]

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