

EXHIBIT C

Approved for public release by the ODNI 20160114

~~SECRET//NOFORN~~

1 BENJAMIN C. MIZER
 2 Principal Deputy Assistant Attorney General
 MELINDA HAAG
 3 United States Attorney
 ELIZABETH J. SHAPIRO
 4 Deputy Branch Director
 RODNEY PATTON
 5 Trial Attorney
 JULIA BERMAN
 6 Trial Attorney
 7 U.S. Department of Justice
 8 Civil Division, Federal Programs Branch
 20 Massachusetts Avenue, NW
 9 Washington, D.C. 20001
 Phone: (202) 305-7919/Fax: (202) 616-8460
 10 Email: Rodney.Patton@usdoj.gov

11
 12 UNITED STATES DISTRICT COURT
 NORTHERN DISTRICT OF CALIFORNIA
 13 SAN FRANCISCO DIVISION

14	ELECTRONIC FRONTIER FOUNDATION,) No. 14-CV-03010-RS
)
15	Plaintiff,) CLASSIFIED DECLARATION OF
) JAMES B. RICHBERG,
16	v.) OFFICE OF THE DIRECTOR OF
) NATIONAL INTELLIGENCE
17	NATIONAL SECURITY AGENCY, OFFICE)
	OF THE DIRECTOR OF NATIONAL) EX PARTE, IN CAMERA
18	INTELLIGENCE,) SUBMISSION
)
19	Defendant.)
) Date: February 18, 2016, 1:30 p.m.
20) Courtroom 3, 17 th Floor
)
21)
) Hon. Richard Seeborg
22)

23
 24
 25
 26
 27 Classified *In Camera*. *Ex Parte* Declaration of James B. Richberg, Office of the Director of National Intelligence
Electronic Frontier Found. v. National Security Agency, et al. (No. 14-cv-03010-RS)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

1 **(U) CLASSIFIED DECLARATION OF JAMES B. RICHBERG,**
 2 **NATIONAL INTELLIGENCE MANAGER FOR CYBER,**
 3 **OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE**

4 Pursuant to 28 U.S.C. § 1746, I, James B. Richberg, declare the following to be true and
 5 correct:

6 **(U) I. BACKGROUND ON DECLARANT**

7 1. (U) I am the National Intelligence Manager for Cyber (NIM-Cyber) for the Director of
 8 National Intelligence (DNI), who, in turn, serves as the head of the Intelligence Community (IC)
 9 and the principal advisor to the President, the National Security Council, and the Homeland
 10 Security Council on intelligence matters related to national security.¹ Prior to becoming the NIM-
 11 Cyber in May 2014, I served as the Deputy NIM-Cyber from 2010 to 2013 and then the Acting
 12 NIM-Cyber from 2013 to 2014.

13 2. (U) By way of further background, I served as a CIA officer for 20 years, where I
 14 performed and managed a variety of activities. During my career there, I developed significant
 15

16
 17
 18 ¹ (U) Congress created the position of the Director of National Intelligence (DNI) in the Intelligence Reform and
 19 Terrorism Prevention Act of 2004, Pub. L. No. 108-458, §§ 1101(a) and 1097, 118 Stat. 3638, 3643-63, 3698-99
 20 (2004) (amending Sections 102 through 104 of Title 1 of the National Security Act of 1947). Subject to the authority,
 21 direction, and control of the President, the DNI serves as the head of the Intelligence Community and as the principal
 22 adviser to the President and the National Security Council for intelligence matters related to the national security. 50
 23 U.S.C. §§ 3023(b)(1), (2). The responsibilities and authorities of the DNI are set forth in the National Security Act of
 24 1947, as amended. These responsibilities include ensuring that national intelligence is provided to the President, heads
 25 of the departments and agencies of the Executive Branch, the Chairman of the Joint Chiefs of Staff and senior military
 26 commanders, and the Senate and House of Representatives and committees thereof. 50 U.S.C. § 3024(a) (1). The
 27 DNI is charged with establishing the objectives of: determining the requirements and priorities for, and managing and
 28 directing the tasking, collection, analysis, production, and dissemination of national intelligence by elements of the
 IC. 50 U.S.C. §§ 3024(f)(1)(A)(i) and (ii). In addition, the National Security Act of 1947, as amended, provides that
 the DNI "shall protect intelligence sources and methods from unauthorized disclosure." 50 U.S.C. § 3024(i)(1).
 Consistent with this responsibility, the DNI establishes and implements guidelines for the IC for the classification of
 information under applicable law, executive orders, or other presidential directives, and for access to and
 dissemination of intelligence. 50 U.S.C. § 3024(i)(2)(A), (B).

~~SECRET//NOFORN~~

Approved for public release by the ODNI 20160114

~~SECRET//NOFORN~~

1 expertise in cyber operations. In 2002, I joined the Office of the National Counterintelligence
2 Executive (ONCIX), which is currently a component of the Office of the Director of National
3 Intelligence (ODNI).² There, I led the process that assesses the damage to U.S. national security
4 resulting from espionage or other unauthorized exposure of classified information. I subsequently
5 assumed responsibility for the Congressionally-mandated and Presidentially-approved annual
6 assessment of significant foreign intelligence threats to the U.S. I also chaired the 2005
7 Quadrennial Intelligence Community Review examination of counterintelligence as a potentially
8 disruptive "system-breaking" issue, and led planning for the implementation of the 2005 U.S.
9 Counterintelligence Strategy. During this time, I became very familiar with counterintelligence
10 issues and the collection priorities of foreign intelligence agencies. From 2005 to 2007, I held
11 various senior leadership positions in ONCIX, including serving as the Acting Deputy Director of
12 National Counterintelligence. In May of 2007, I joined the interagency team developing the
13 Comprehensive National Cybersecurity Initiative (CNCI) on behalf of the DNI and the Executive
14 Office of the President. I was one of the architects of the CNCI, which is a phased approach to
15 improving the ability of the United States to secure and defend its national and economic security
16 interests against the full spectrum of cyber threats.
17
18
19

20 (U) II. ROLE OF THE NIM-CYBER

21
22
23
24

25 ² (U) The function of the ODNI is to assist the DNI in carrying out his duties and responsibilities under the
26 Act and other applicable provisions of law, and to carry out such other duties as may be prescribed by the President
or by law.

~~SECRET//NOFORN~~

Approved for public release by the ODNI 20160114

~~SECRET//NOFORN~~

1 3. (U) In my current role as NIM-Cyber, I am the DNI's intelligence community (IC) lead for
2 cyber intelligence issues. Specifically, I am responsible to the DNI for the integration of IC
3 collection and analysis on cyber intelligence issues; I am also responsible for coordinating and
4 supporting the IC's efforts to provide accurate, timely, and comprehensive advice to national
5 policy and decision makers on cyber intelligence issues.
6

7 4. ~~(S//REL TO USA, FVEY)~~ [REDACTED]
8 [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED]
12 [REDACTED]
13 [REDACTED]

- 14 • ~~(S//REL TO USA, FVEY)~~ [REDACTED]
- 15 [REDACTED]
- 16 • ~~(S//REL TO USA, FVEY)~~ [REDACTED]
- 17 [REDACTED]
- 18 • ~~(S//REL TO USA, FVEY)~~ [REDACTED]

19 5. (U) As part and parcel of those duties, I work extensively with the IC to develop cyber
20 intelligence strategies and goals so that a full range of intelligence requirements are met on daily,
21 short-term and long-term bases. NIM Cyber also promotes integration through use of best
22 practices, to include strategy boards and integrated intelligence campaigns.
23

24 6. (U) As the NIM Cyber, I have a comprehensive understanding of cyber issues and am
25 required to provide strategic oversight of cyber intelligence activities, including the Vulnerabilities
26

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

1 Equities Process, which is discussed in Section IV of this declaration. I am responsible to the DNI
2 for the integration of collection and analysis on cyber intelligence issues, as well as for providing
3 support to all elements of the IC. My mission portfolio extends across all regions and countries.

4 **(U) III. PURPOSE OF THIS DECLARATION**

5 7. (U) Through the exercise of my official duties, I have become familiar with this civil action;
6 the underlying FOIA request; the Government's October 30, 2015 Memorandum of Points and
7 Authorities in Support of the Defendants' Motion for Summary Judgment, with accompanying
8 exhibits; and the Plaintiff's December 4, 2015 Opposition to the Government's Motion for
9 Summary Judgment/ Cross Motion for Summary Judgment, with accompanying exhibits. I am
10 also very familiar with the classified document entitled "Commercial and Government
11 Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy
12 and Process" ("the VEP document").
13

14 8. (U) I am aware that on October 30, 2015, the Plaintiff was provided a redacted version of
15 the VEP document. I am also aware that, contemporaneous with this declaration (hereinafter the
16 January 14, 2016 Declaration), the government will provide Plaintiff with another version of that
17 document (hereinafter the January 14, 2016 VEP Document) containing fewer redactions than the
18 version previously disclosed on October 30, 2015. I am familiar with both of these documents as
19 well.
20

21 9. (U) I submit this declaration in support of the U.S. Department of Justice's opposition to
22 Plaintiff's cross motion for summary judgment and its reply in support of its motion for summary
23 judgment in this proceeding. The purpose of this declaration is to explain, in a classified, *ex parte*
24
25
26

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

1 and *in camera* submission to the Court, that the information in the January 14, 2016 VEP document
2 has not been disclosed to the public by any government official acting in her official capacity and
3 that its release would disclose classified information and reveal intelligence sources and methods.

4 10. (U) I make the following statements based upon personal knowledge and information
5 made available to me in my official capacity:
6

7 **(U) IV. THE VULNERABILITIES EQUITIES PROCESS (VEP)**

8 11. (U) The VEP was developed to codify and systematize the U.S. government's handling of
9 "zero day" exploits. "Zero day" exploits are flaws in information technology (IT) hardware or
10 software products for which no mitigation is available from the product vendor. These flaws can
11 be exploited to obtain information from or to disrupt activities on a particular computer or
12 computer network. The name derives from the fact that the IT user has "zero days" to prepare or
13 react because the threat to the system is immediate. In practice, the "zero day" designation applies
14 to both unknown vulnerabilities and those that are known but remain "un-patched" or otherwise
15 un-mitigated. Reasons for a delay in remediation vary. Many complex products can have
16 thousands of flaws ranging from trivial 'bugs' to serious vulnerabilities, and not all are easy to
17 identify. Applying "patches" is not always a simple task, as product developers have to ensure
18 that any fix not only addresses the problem but also leaves other hardware and software
19 components in the system un-harmed. In some cases, economic reasons mitigate against such
20 remediation, such as when a product line is retired or the vendor opts to discontinue support. Legal
21 barriers may also impair a fix, such as when a user is running a pirated or counterfeit version of a
22 product and is thus not eligible to receive vendor support.
23
24
25
26

~~SECRET//NOFORN~~

Approved for public release by the ODNI 20160114

~~SECRET//NOFORN~~

1 12. (U) The United States Government (USG) is critically dependent on computer information
2 systems to manage day-to-day activities. In the event a vulnerability in a government computer
3 system is not "patched" it leaves that system vulnerable to representatives of foreign intelligence
4 services and others eager to exploit the vulnerability to gain un-authorized access. The government
5 is also highly dependent on hardware and software vendors to identify and close vulnerabilities,
6 and also on its own cybersecurity centers to identify and coordinate the closure of these
7 vulnerabilities and to mitigate exploitation by intruders.

9 13. (U) Prior to the adoption of the VEP, individual government entities would identify and
10 discuss vulnerabilities and communicate knowledge of their existence to vendor community and
11 cybersecurity/information assurance personnel on an *ad hoc* basis. In some cases, knowledge of
12 vulnerabilities was only discussed "in-house" within a single government agency. This process
13 was informal, based on personal contacts and organizational mission; dependent upon the initiative
14 of the individuals involved; and did not facilitate consistent and traceable communication on this
15 important issue.

17 14. (U) In 2008, I worked with other government officials to help establish the Comprehensive
18 National Cybersecurity Initiative (CNCI). This was the largest effort to date to build a
19 comprehensive approach to Federal and national cybersecurity. As an adjunct to the CNCI effort,
20 in 2008 and 2009 a working group consisting of a number of different Federal agencies was formed
21 to develop a formal and consistent process for sharing computer vulnerabilities. The working
22 group discussed how the member organizations currently shared information on vulnerabilities,
23 when they shared it, and the methodology applied in balancing potentially competing
24

26
27 Classified *In Camera*. *Ex Parte* Declaration of James B. Richberg, Office of the Director of National Intelligence
Electronic Frontier Found. v. National Security Agency, et al. (No. 14-cv-03010-RS)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

1 organizational equities. It also discussed how to improve the existing informal process to optimize
2 sharing of vulnerability information, balance equities, and ultimately develop a more transparent
3 and consistent vulnerability equities process. The VEP that began to emerge was designed to
4 consider all types of zero-day vulnerabilities in an inter-agency process. In developing the VEP,
5 the USG recognized that not all organizations see the entire picture of vulnerabilities, and each
6 organization may have its own equities and concerns regarding the prioritization of patches and
7 fixes, as well as its own distinct mission obligations.

9 **(U) V. THE GOVERNMENT HAS NOT OFFICIALLY DISCLOSED THE**
10 **INFORMATION IN THE JANUARY 14, 2016 VEP DOCUMENT THAT IS CURRENTLY**
11 **CLASSIFIED AND/OR REFERS TO INTELLIGENCE SOURCES AND METHODS.**

12 15. (U) The protected information within the January 14, 2016 VEP document falls into four
13 categories. These four categories comprise information regarding: (1) certain actions taken in
14 response to the identification of a vulnerability; (2) timelines pertaining to the functioning of the
15 VEP; (3) the identities of certain entities involved in particular aspects of the VEP; and (4) the
16 process for addressing cryptographic vulnerabilities. Each category is set forth below and will be
17 discussed in turn.

18
19 **(U) A. Certain Actions Taken in Response to the Identification of a Vulnerability**

20 16. (U) Certain actions that may be taken in response to the identification of a vulnerability
21 are redacted in the January 14, 2016 VEP document. Redactions taken to protect information
22 within this category are found in Sections 3., 5., 6.2.b., 6.2.c., 6.6.2., 6.8.1., 7.n., 7.o., Figure 1.,
23 and Annex A. These actions have not been officially disclosed. If disclosed, they would reveal
24
25
26

~~SECRET//NOFORN~~

Approved for public release by the ODNI 20160114

~~SECRET//NOFORN~~

1 currently classified information and would implicate intelligence sources and methods, as
2 described below:

3 17. ~~(S//REL TO USA, FVEY)~~ [REDACTED]

4 [REDACTED]
5 [REDACTED]
6 [REDACTED]
7 [REDACTED]
8 [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED]
12 [REDACTED]
13 [REDACTED]
14 [REDACTED]

15 18. ~~(S//REL TO USA, FVEY)~~ [REDACTED]

16 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]

23 ³ ~~(S//REL TO USA, FVEY)~~ [REDACTED]

24 [REDACTED]
25 [REDACTED]
26 [REDACTED]

~~(S//REL TO USA, FVEY)~~

~~SECRET//NOFORN~~

Approved for public release by the ODNI 20160114

~~SECRET//NOFORN~~

1 [REDACTED]

2 [REDACTED]

3 [REDACTED]

4 [REDACTED]

5 [REDACTED]

6 [REDACTED]

7 [REDACTED]

8 [REDACTED]

9 [REDACTED]

10 19. ~~(S//REL TO USA, FVEY)~~ [REDACTED]

11 [REDACTED]

12 [REDACTED]

13 [REDACTED]

14 [REDACTED]

15 [REDACTED]

16 [REDACTED]

17 [REDACTED]

18 [REDACTED]

20

21 ~~⁵ (S//REL TO USA, FVEY)~~ [REDACTED]

22 ~~⁶ (S//REL TO USA, FVEY)~~ [REDACTED]

23 ~~⁷ (S//REL TO USA, FVEY)~~ [REDACTED]

24 ~~⁸ (S//REL TO USA, FVEY)~~ [REDACTED]

25 ~~⁹ (S//REL TO USA, FVEY)~~ [REDACTED]

26 ~~¹⁰ (S//REL TO USA, FVEY)~~ [REDACTED]

27 ~~¹¹ (S//REL TO USA, FVEY)~~ [REDACTED]

28 ~~¹² (S//REL TO USA, FVEY)~~ [REDACTED]

~~SECRET//NOFORN~~

Approved for public release by the ODNI 20160114

~~SECRET//NOFORN~~

1 20. ~~(S//REL TO USA, FVEY)~~ [REDACTED]

2 [REDACTED]

3 [REDACTED]

4 [REDACTED]

5 [REDACTED]

6 [REDACTED]

7 [REDACTED]

8 [REDACTED]

9 [REDACTED]

10 [REDACTED]

11 [REDACTED]

12 [REDACTED]

13 [REDACTED]

14 [REDACTED]

15 [REDACTED]

16 [REDACTED]

17 [REDACTED]

18 [REDACTED]

19 [REDACTED]

20 [REDACTED]

21 [REDACTED]

22 [REDACTED]

23 [REDACTED]

¹³ ~~(S//REL TO USA, FVEY)~~ [REDACTED]

¹⁴ ~~(S//REL TO USA, FVEY)~~ [REDACTED]

¹⁵ ~~(S//REL TO USA, FVEY)~~ [REDACTED]

¹⁶ ~~(S//REL TO USA, FVEY)~~ [REDACTED]

~~SECRET//NOFORN~~

Approved for public release by the ODNI 20160114

~~SECRET//NOFORN~~

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[REDACTED]

22. ~~(S//REL TO USA, FVEY)~~ [REDACTED]

[REDACTED]

23. ~~(S//REL TO USA, FVEY)~~ [REDACTED]

[REDACTED]

~~SECRET//NOFORN~~

Approved for public release by the ODNI 20160114

~~SECRET//NOFORN~~

1 [REDACTED]

2 [REDACTED]

3 [REDACTED]

4 [REDACTED]

5 [REDACTED]

6 [REDACTED]

7 [REDACTED]

8 [REDACTED]

9 24. (U) This redacted information falls within the ambit of protected information previously
 10 identified in paragraph 32 of the October 30, 2015 Hudson declaration regarding (1) "the U.S.
 11 Government's policies and processes employed in identifying and reporting...vulnerabilities
 12 discovered in national security systems and how and when those vulnerabilities should be
 13 adjudicated and disseminated through the Vulnerabilities Equities Process," and (2) "the specific
 14 considerations that apply when a vulnerability is identified."

15

16 **(U) B. Timelines Pertaining to the Functioning of the VEP**

17

18 25. (U) Timelines for activities conducted under the VEP are redacted in the January 14,
 19 2016 VEP document. Redactions taken to protect information within this category are found in:
 20 Sections 6.6.1.b, 6.6.1.c, and 6.8.1. These timelines have not been officially disclosed to the
 21 public. If disclosed, they would reveal currently classified information and would implicate
 22 intelligence sources and methods, as described below.

23

24

25

26 ¹⁷ ~~(S//REL TO USA, FVEY)~~ [REDACTED]

~~SECRET//NOFORN~~

Approved for public release by the ODNI 20160114

~~SECRET//NOFORN~~

1 26. ~~(S//REL TO USA, FVEY)~~ [REDACTED]

2 [REDACTED]

3 [REDACTED]

4 [REDACTED]

5 [REDACTED]

6 [REDACTED]

7 [REDACTED]

8 [REDACTED]

9 27. ~~(S//REL TO USA, FVEY)~~ [REDACTED]

10 [REDACTED]

11 [REDACTED]

12 [REDACTED]

13 [REDACTED]

14 [REDACTED]

15 [REDACTED]

16 [REDACTED]

17 [REDACTED]

18 [REDACTED]

19 [REDACTED]

20 28. (U) The redacted information discussed in this section is referenced in paragraph 32 of

21 Jennifer Hudson's October 30, 2015 VEP declaration, where she states that information is being

22 withheld regarding "the timelines involved in the process." As Ms. Hudson notes in the

23

24

25 ¹⁸ ~~(S//REL TO USA, FVEY)~~ [REDACTED]

26 ¹⁹ ~~(S//REL TO USA, FVEY)~~ [REDACTED]

28 ~~SECRET//NOFORN~~

Approved for public release by the ODNI 20160114

~~SECRET//NOFORN~~

1 subsequent paragraph (33) in that declaration, “[i]t would be useful for a foreign intelligence
2 service to know what actions the government would take in response to an identified vulnerability
3 and the timing of those actions so that it could develop countermeasures to ensure that it derives
4 the greatest possible benefit from exploitation of that vulnerability.”

5 **(U) C. The Identities of Certain Entities Involved in Particular Aspects of the VEP**

6
7 29. (U) Information that describes certain entities involved in particular aspects of the VEP
8 continues to be redacted in the January 14, 2016 VEP document. Redactions taken to protect
9 information within this category are found in Sections 5., 6.2.b., 6.3 and 6.7, as well as Figure 6.1
10 and Annex A. This information has not been officially disclosed to the public. If disclosed, this
11 information would reveal currently classified information and would implicate intelligence
12 sources and methods, as described below:
13

14 30. ~~(S//NF)~~ [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]

21
22
23 ²⁰ ~~(S//REL TO USA, FVEY)~~ [REDACTED]

24 [REDACTED]
25 [REDACTED]
26 ²¹ ~~(S//REL TO USA, FVEY)~~ [REDACTED]

28 ~~SECRET//NOFORN~~

Approved for public release by the ODNI 20160114

~~SECRET//NOFORN~~

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[REDACTED]

31. ~~(S//NF)~~ [REDACTED]

[REDACTED]

32. ~~(S//REL TO USA, FVEY)~~ [REDACTED]

[REDACTED]

²² ~~(S//REL TO USA, FVEY)~~ [REDACTED]

²³ ~~(S//REL TO USA, FVEY)~~ [REDACTED]

~~SECRET//NOFORN~~

Approved for public release by the ODNI 20160114

~~SECRET//NOFORN~~

[REDACTED]

[REDACTED]

[REDACTED]

33. (U) The redacted information discussed in this section falls within the ambit of protected information set forth in paragraph 32 of the October 30, 2015 Hudson declaration as "information that would identify certain agencies that participate in the process" and "the conditions under which each agency participates."

(U) D. The Process for Addressing Cryptographic Vulnerabilities

34. (U) Information that discusses the process for addressing vulnerabilities in cryptographic systems is found in Subsection 5.g and is redacted in the January 14, 2016 VEP Document. Information regarding this process has not been disclosed to the public. If disclosed, it would reveal currently classified information and would implicate intelligence sources and methods, as described below:

35. ~~(S//REL TO USA, FVEY)~~ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

1 36. ~~(S//REL TO USA, FVEY)~~ [REDACTED]

2 [REDACTED]

3 [REDACTED]

4 [REDACTED]

5 [REDACTED]

6 [REDACTED]

7 [REDACTED]

8 [REDACTED]

9 [REDACTED]

10 [REDACTED]

11

12 37. (U) This information falls within the ambit of protected information regarding “the U.S.

13 Government’s policies and processes employed in identifying and reporting cryptographic

14 vulnerabilities...and how and when those vulnerabilities should be adjudicated and disseminated

15 through the Vulnerabilities Equities Process,” as set forth in paragraph 32 of the October 30, 2015

16 Hudson declaration.

17

18

19

20

21

22

23

24

25

26

28 ~~SECRET//NOFORN~~

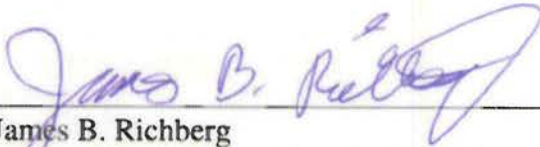
Approved for public release by the ODNI 20160114

~~SECRET//NOFORN~~

CONCLUSION

1
2 (U) I certify that that all the information contained within this declaration is true and
3 correct to the best of my knowledge and belief.

4 Executed this 14th day of January, 2016.

5
6 
7 _____
8 James B. Richberg
9 National Intelligence Manager for Cyber
10 Office of the Director of National Intelligence
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

~~SECRET//NOFORN~~