U.S. Department of Justice

Federal Bureau of Investigation
Washington, D.C. 20535

February 28, 2020

MR. WILLIAM F MARSHALL
JUDICIAL WATCH
SUITE 800
425 THIRD STREET, SOUTHWEST
WASHINGTON, DC 20024

FOIPA Request No.: 1391365-000
Civil Action No.: 18-cv-154
Subject: Communications between Peter Strzok and Lisa Page (February 1, 2015 – Present)

Dear Mr. Marshall:

The enclosed documents were reviewed under the Freedom of Information Act (FOIA), Title 5, United States Code, Section 552. Below you will find check boxes under the appropriate statue headings with indicate the types of exemptions asserted to protect information which is exempt from disclosure. The appropriate exemptions are noted on the enclosed pages next to redacted information. In addition, a deleted page information sheet was inserted to indicate where pages were withheld entirely and identify which exemptions were applied. The checked exemption boxes used to withhold information are further explained in the enclosed Explanation of Exemptions.

Section 552

☐ (b)(1)
☐ (b)(2)
☐ (b)(3)
____
____
____
☐ (b)(4)
☑ (b)(5)
☑ (b)(6)

☐ (b)(7)(A)
☐ (b)(7)(B)
☑ (b)(7)(C)
☐ (b)(7)(D)
☑ (b)(7)(E)
☐ (b)(7)(F)
☐ (b)(8)
☐ (b)(9)

Section 552a

☐ (d)(5)
☐ (j)(2)
☐ (k)(1)
☐ (k)(2)
☐ (k)(3)
☐ (k)(4)
☐ (k)(5)
☐ (k)(6)
☐ (k)(7)

500 pages of potentially responsive records were reviewed.
139 pages are being released in whole or in part.
26 pages are being withheld in full per exemptions.
219 pages are being withheld duplicate.
86 pages are being withheld referral/consult.
30 pages were determined to be non-records/non-responsive to the FOIA request.

Below you will also find additional informational paragraphs about your request. Where applicable, check boxes are used to provide you with more information about the processing of your request. Please read each item carefully.

☑ Document(s) were located which originated with, or contained information concerning, other Government Agency (ies) [OGA].

☐ This information has been referred to the OGA(s) for review and direct response to you.

☑ We are consulting with another agency. The FBI will correspond with you regarding this information when the consultation is completed.

□ In accordance with standard FBI practice and pursuant to FOIA exemption (b)(7)(E) and Privacy Act exemption (j)(2) [5 U.S.C. § 552/552a (b)(7)(E)/(j)(2)], this response neither confirms nor denies the existence of your subject's name on any watch lists.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the Freedom of Information Act (FOIA). See 5 U.S. C. § 552(c) (2006 & Supp. IV (2010). This response is limited to those records subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist. Enclosed for your information is a copy of the Explanation of Exemptions.

If you are not satisfied with the Federal Bureau of Investigation's determination in response to this request, you may administratively appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, 441 G Street, NW, 6th Floor, Washington, D.C. 20530, or you may submit an appeal through OIP's FOIA STAR portal by creating an account following the instructions on OIP's website: https://www.justice.gov/oip/submit-and-track-request-or-appeal. Your appeal must be postmarked or electronically transmitted within ninety (90) days of the date of my response to your request. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal." Please cite the FOIPA Request Number assigned to your request so it may be easily identified.

You may seek dispute resolution services by contacting the Office of Government Information Services (OGIS). 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 1-877-684-6448; or facsimile at 202-741-5769. Alternatively, you may contact the FBI's FOIA Public Liaison by emailing foipaquestions@fbi.gov. If you submit your dispute resolution correspondence by email, the subject heading should clearly state "Dispute Resolution Services." Please also cite the FOIPA Request Number assigned to your request so it may be easily identified.

Please direct any further inquiries about this case to the Assistant United States Attorney representing the Government in this matter. Please use the FOIPA Request Number and/or Civil Action Number in all correspondence or inquiries concerning your request.

You may direct any further inquiries to the attorney representing the Government in this matter.

☑ See additional information which follows.

Sincerely,

David M. Hardy
Section Chief
Record/Information
Dissemination Section
Information Management Division

Enclosure(s)

In response to your Freedom of Information Act (FOIA) request, enclosed is a processed copy of Bates Stamped documents, FBI(18-cv-154)-9536 through FBI(18-cv-154)-10035. The enclosed documents represent the twenty-first interim release of information responsive to your request.

The FBI conducted email searches for any email communication between Peter Strzok and Lisa Page. This search located both official government records and non-record personal communications between these two individuals.

The FBI reviewed 500 pages of these emails. While conducting this review, the FBI individually analyzed the emails to determine whether they pertained to official government business constituting records under the FOIA or whether they consisted of purely personal communications between the two individuals. As a result of the FBI's review, it determined 30 pages were non-record, personal communications not subject to the FOIA; and 470 pages consisted of responsive FBI records.

As previously indicated, document(s) were located which originated with, or contained information concerning another agency (ies). We are consulting with the other agency (ies) and are awaiting their response. Our office has processed all other information currently in our possession. The FBI will correspond with you regarding those documents when the consultation is completed.

To minimize costs to both you and the FBI, duplicate copies of the same document were not processed.

EXPLANATION OF EXEMPTIONS

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

(b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;

(b)(2) related solely to the internal personnel rules and practices of an agency;

(b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

(b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(b)(9) geological and geophysical information and data, including maps, concerning wells.

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

(d)(5) information compiled in reasonable anticipation of a civil action proceeding;

(j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;

(k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;

(k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;

(k)(4) required by statute to be maintained and used solely as statistical records;

(k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service he release of which would compromise the testing or examination process;

(k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

FEDERAL BUREAU OF INVESTIGATION
FREEDOM OF INFORMATION ACT (FOIA)
DELETED PAGE INFORMATION SHEET
FOIA Request No.:1391365-000 Civil
Action No.: 18-cv-154

Total Withheld Page(s) = 361

Bates Page Reference	**Reason for Withholding** (i.e., exemptions with coded rationale, duplicate, sealed by order of court, etc.)
FBI(18-cv-154)-9537 thru FBI(18-cv-154)-9539	b5-1, 3; b6-1; b7C-1; b7E-6
FBI(18-cv-154)-9540 thru FBI(18-cv-154)-9544	Duplicate to FBI(18-cv-154)-3194 thru FBI(18-cv-154)-3198
FBI(18-cv-154)-9545 thru FBI(18-cv-154)-9549	Referral/Consult
FBI(18-cv-154)-9558	Other - Non-records/Non-responsive to the FOIA request
FBI(18-cv-154)-9559 thru FBI(18-cv-154)-9561	Duplicate to FBI(18-cv-154)-3215 thru FBI(18-cv-154)-3218
FBI(18-cv-154)-9562	Other - Non-records/Non-responsive to the FOIA request
FBI(18-cv-154)-9563 thru FBI(18-cv-154)-9574	Referral/Consult
FBI(18-cv-154)-9577	Other - Non-records/Non-responsive to the FOIA request
FBI(18-cv-154)-9578 thru FBI(18-cv-154)-9583	Duplicate to FBI(18-cv-154)-3244 thru FBI(18-cv-154)-3247
FBI(18-cv-154)-9584 thru FBI(18-cv-154)-9587	Referral/Consult
FBI(18-cv-154)-9588 thru FBI(18-cv-154)-9591	Duplicate to FBI(18-cv-154)-3244 thru FBI(18-cv-154)-3247
FBI(18-cv-154)-9592	Other - Non-records/Non-responsive to the FOIA request
FBI(18-cv-154)-9593	Duplicate to FBI(18-cv-154)-3248
FBI(18-cv-154)-9594	Other - Non-records/Non-responsive to the FOIA request
FBI(18-cv-154)-9598 thru FBI(18-cv-154)-9605	Referral/Consult
FBI(18-cv-154)-9607	Duplicate to FBI(18-cv-154)-9606
FBI(18-cv-154)-9608 thru FBI(18-cv-154)-9639	Referral/Consult
FBI(18-cv-154)-9640 thru FBI(18-cv-154)-9671	Duplicate to FBI(18-cv-154)-9608 thru FBI(18-cv-154)-9639
FBI(18-cv-154)-9672	Other - Non-records/Non-responsive to the FOIA request
FBI(18-cv-154)-9673 thru FBI(18-cv-154)-9695	Referral/Consult
FBI(18-cv-154)-9696 thru FBI(18-cv-154)-9718	Duplicate to FBI(18-cv-154)-9673 thru FBI(18-cv-154)-9695
FBI(18-cv-154)-9729	Other - Non-records/Non-responsive to the FOIA request
FBI(18-cv-154)-9730 thru FBI(18-cv-154)-9731	Duplicate to FBI(18-cv-154)-3271 thru FBI(18-cv-154)-3272
FBI(18-cv-154)-9733	Other - Non-records/Non-responsive to the FOIA request

FBI(18-cv-154)-9773 thru FBI(18-cv-154)-9811	Duplicate to FBI(18-cv-154)-9734 thru FBI(18-cv-154)-9772
FBI(18-cv-154)-9812	Duplicate to FBI(18-cv-154)-3273
FBI(18-cv-154)-9814	Other - Non-records/Non-responsive to the FOIA request
FBI(18-cv-154)-9816	Duplicate to FBI(18-cv-154)-3274 thru FBI(18-cv-154)-3275
FBI(18-cv-154)-9818	b5-1
FBI(18-cv-154)-9820 thru FBI(18-cv-154)-9822	Other - Non-records/Non-responsive to the FOIA request
FBI(18-cv-154)-9828	Other - Non-records/Non-responsive to the FOIA request
FBI(18-cv-154)-9830 thru FBI(18-cv-154)-9833	Other - Non-records/Non-responsive to the FOIA request
FBI(18-cv-154)-9834 thru FBI(18-cv-154)-9844	Duplicate to FBI(18-cv-154)-3279 thru FBI(18-cv-154)-3289
FBI(18-cv-154)-9845 thru FBI(18-cv-154)-9878	Duplicate to FBI(18-cv-154)-9890 thru FBI(18-cv-154)-9923
FBI(18-cv-154)-9879 thru FBI(18-cv-154)-9889	Duplicate to FBI(18-cv-154)-3279 thru FBI(18-cv-154)-3289
FBI(18-cv-154)-9890 thru FBI(18-cv-154)-9894	b5-1
FBI(18-cv-154)-9908 thru FBI(18-cv-154)-9923	b5-1; b7E-7
FBI(18-cv-154)-9925	Other - Non-records/Non-responsive to the FOIA request
FBI(18-cv-154)-9927 thru FBI(18-cv-154)-9928	Other - Non-records/Non-responsive to the FOIA request
FBI(18-cv-154)-9932 thru FBI(18-cv-154)-9934	Other - Non-records/Non-responsive to the FOIA request
FBI(18-cv-154)-9950 thru FBI(18-cv-154)-9964	Duplicate to FBI(18-cv-154)-9935 thru FBI(18-cv-154)-9949
FBI(18-cv-154)-9966 thru FBI(18-cv-154)-9979	Duplicate to FBI(18-cv-154)-9936 thru FBI(18-cv-154)-9949
FBI(18-cv-154)-9980 thru FBI(18-cv-154)-9981	Duplicate to FBI(18-cv-154)-3310 thru FBI(18-cv-154)-3311
FBI(18-cv-154)-9982	Other - Non-records/Non-responsive to the FOIA request
FBI(18-cv-154)-9986 thru FBI(18-cv-154)-9987	Duplicate to FBI(18-cv-154)-3115 thru FBI(18-cv-154)-3116
FBI(18-cv-154)-9991	Other - Non-records/Non-responsive to the FOIA request
FBI(18-cv-154)-9997	Other - Non-records/Non-responsive to the FOIA request
FBI(18-cv-154)-10000 thru FBI(18-cv-154)-10001	Duplicate to FBI(18-cv-154)-3327 thru FBI(18-cv-154)-3328
FBI(18-cv-154)-10002	Other - Non-records/Non-responsive to the FOIA request
FBI(18-cv-154)-10003 thru FBI(18-cv-154)-10004	Referral/Consult
FBI(18-cv-154)-10005 thru FBI(18-cv-154)-10006	Other - Non-records/Non-responsive to the FOIA request
FBI(18-cv-154)-10007	Duplicate to FBI(18-cv-154)-10008
FBI(18-cv-154)-10013	Duplicate to FBI(18-cv-154)-10014
FBI(18-cv-154)-10015	Other - Non-records/Non-responsive to the FOIA request
FBI(18-cv-154)-10017 thru FBI(18-cv-154)-10018	Duplicate to FBI(18-cv-154)-3339

FBI(18-cv-154)-10024 thru FBI(18-cv-154)-10025	Duplicate to FBI(18-cv-154)-3359 thru FBI(18-cv-154)-3362
FBI(18-cv-154)-10026 thru FBI(18-cv-154)-10029	Duplicate to FBI(18-cv-154)-3348 thru FBI(18-cv-154)-3349
FBI(18-cv-154)-10031	b5-1, 3; b6-1; b7C-1; b7E-6

xxxxxxxxxxxxxxxxxxxxxx

X Deleted Page(s) X

X No Duplication Fee X

X For this Page X

Xxxxxxxxxxxxxxxxxxxxxx

Strzok, Peter P. (CD) (FBI)

From: Strzok, Peter P. (CD) (FBI)
Sent: Wednesday, December 14, 2016 8:50 PM
To: Page, Lisa C. (OGC) (FBI)
Subject: RE: [redacted]

b5 -1

And thank you ?

-------- Original message --------
From: "Page, Lisa C. (OGC) (FBI)" [redacted]
Date: 12/14/2016 8:47 PM (GMT-05:00)
To: "Strzok, Peter P. (CD) (FBI) [redacted]
Subject: Fwd [redacted]

b5 -1
b6 -1
b7C -1
b7E -6

[redacted]

b5 -1, 3
b6 -1
b7C -1
b7E -6

Strzok, Peter P. (CD) (FBI)

From:	Strzok, Peter P. (CD) (FBI)
Sent:	Thursday, December 15, 2016 7:50 AM
To:	Page, Lisa C. (OGC) (FBI)
Subject:	FW: Thursday

FYSA

From [redacted](CD) (FBI) b6 -1
Sent: Thursday, December 15, 2016 7:24 AM b7C -1
To: Strzok, Peter P. (CD) (FBI) [redacted] b7E -6
Subject: Thursday

Sir, as a reminder. I will be in Leesburg all day. I responded to your question yesterday afternoon, not sure you saw it. [redacted] As such, they were delayed. I will have someone deliver them today once we receive them back. These do not appear to be all that interesting or revealing, but are on topic. I'll discuss more with you tomorrow. [redacted] b7E -7

[redacted] b6 -1
Chief, b7C -1
Counterespionage Group

Strzok, Peter P. (CD) (FBI)

From:	Strzok, Peter P. (CD) (FBI)
Sent:	Thursday, December 15, 2016 8:05 AM
To:	Page, Lisa C. (OGC) (FBI)
Subject:	FW: UK article on Dem Hacks

Shaddy sh*t at AU... ;)

EXCLUSIVE: Ex-British ambassador who is now a WikiLeaks operative claims Russia did NOT provide Clinton emails - they were handed over to him at a D.C. park by an intermediary for 'disgusted' Democratic whistleblowers

- Craig Murray, former British ambassador to Uzbekistan and associate of Julian Assange, told the Dailymail.com he flew to Washington, D.C. for emails
- He claims he had a clandestine hand-off in a wooded area near American University with one of the email sources
- The leakers' motivation was 'disgust at the corruption of the Clinton Foundation and the 'tilting of the primary election playing field against Bernie Sanders'
- Murray says: 'The source had legal access to the information. The documents came from inside leaks, not hacks'
- 'Regardless of whether the Russians hacked into the DNC, the documents Wikileaks published did not come from that,' Murray insists
- Murray is a controversial figure who was relieved of his post as British ambassador amid allegations of misconduct but is close to Wikileaks

By Alana Goodman In Washington, Dc For Dailymail.com

Published: 15:33 EST, 14 December 2016 | Updated: 18:01 EST, 14 December 2016

A Wikileaks envoy today claims he personally received Clinton campaign emails in

A Wikileaks envoy today claims he personally received Clinton campaign emails in Washington D.C. after they were leaked by 'disgusted' whisteblowers - and not hacked by Russia.

Craig Murray, former British ambassador to Uzbekistan and a close associate of Wikileaks founder Julian Assange, told Dailymail.com that he flew to Washington, D.C. for a clandestine hand-off with one of the email sources in September.

'Neither of [the leaks] came from the Russians,' said Murray in an interview with Dailymail.com on Tuesday. 'The source had legal access to the information. The documents came from inside leaks, not hacks.'

His account contradicts directly the version of how thousands of Democratic emails were published before the election being advanced by U.S. intelligence.

Craig Murray (left), former British ambassador to Uzbekistan and a close associate of Wikileaks founder Julian Assange (right), told the Dailymail.com that he flew to Washington, D.C. for a clandestine hand-off with one of the email sources in September

Murray is a controversial figure who was removed from his post as a British ambassador amid allegations of misconduct. He was cleared of those but left the diplomatic service in acrimony.

His links to Wikileaks are well known and while his account is likely to be seen as both unprovable and possibly biased, it is also the first intervention by Wikileaks since reports surfaced last week that the CIA believed Russia hacked the Clinton emails to help hand the election to Donald Trump.

Murray's claims about the origins of the Clinton campaign emails comes as U.S. intelligence officials are increasingly confident that Russian hackers infiltrated both the Democratic National Committee and the email account of top Clinton aide John Podesta.

In Podesta's case, his account appeared to have been compromised through a basic 'phishing' scheme, the New York Times reported on Wednesday.

U.S. intelligence officials have reportedly told members of Congress during classified briefings that they believe Russians passed the documents on to Wikileaks as part of an influence operation to swing the election in favor of Donald Trump.

But Murray insisted that the DNC and Podesta emails published by Wikileaks did not come from the Russians, and were given to the whistleblowing group by Americans who had authorized access to the information.

'Neither of [the leaks] came from the Russians,' Murray said. 'The source had legal access to the information. The documents came from inside leaks, not hacks.'

He said the leakers were motivated by 'disgust at the corruption of the Clinton Foundation and the tilting of the primary election playing field against Bernie Sanders.'

Murray said he retrieved the package from a source during a clandestine meeting in a wooded area near American University, in northwest D.C. He said the individual he met with was not the original person who obtained the information, but an intermediary.

Murray claims he met with the person who passed the emails over in a Washington, D.C. part near American University

His account cannot be independently verified but is in line with previous statements by Wikileaks - which was the organization that published the Podesta and DNC emails.

Wikileaks published the DNC messages in July and the Podesta messages in October. The messages revealed efforts by some DNC officials to undermine the presidential campaign of Sen. Bernie Sanders, who was running against Hillary Clinton.

Others revealed that Clinton aides were concerned about potential conflicts and mismanagement at the Clinton Foundation.

Murray declined to say where the sources worked and how they had access to the information, to shield their identities.

He suggested that Podesta's emails might be 'of legitimate interest to the security services' in the U.S., due to his communications with Saudi Arabia lobbyists and foreign officials.

Murray said he was speaking out due to claims from intelligence officials that Wikileaks was given the documents by Russian hackers as part of an effort to help Donald Trump win the U.S. presidential election.

'I don't understand why the CIA would say the information came from Russian hackers when they must know that isn't true,' he said. 'Regardless of whether the Russians hacked into the DNC, the documents Wikileaks published did not come from that.'

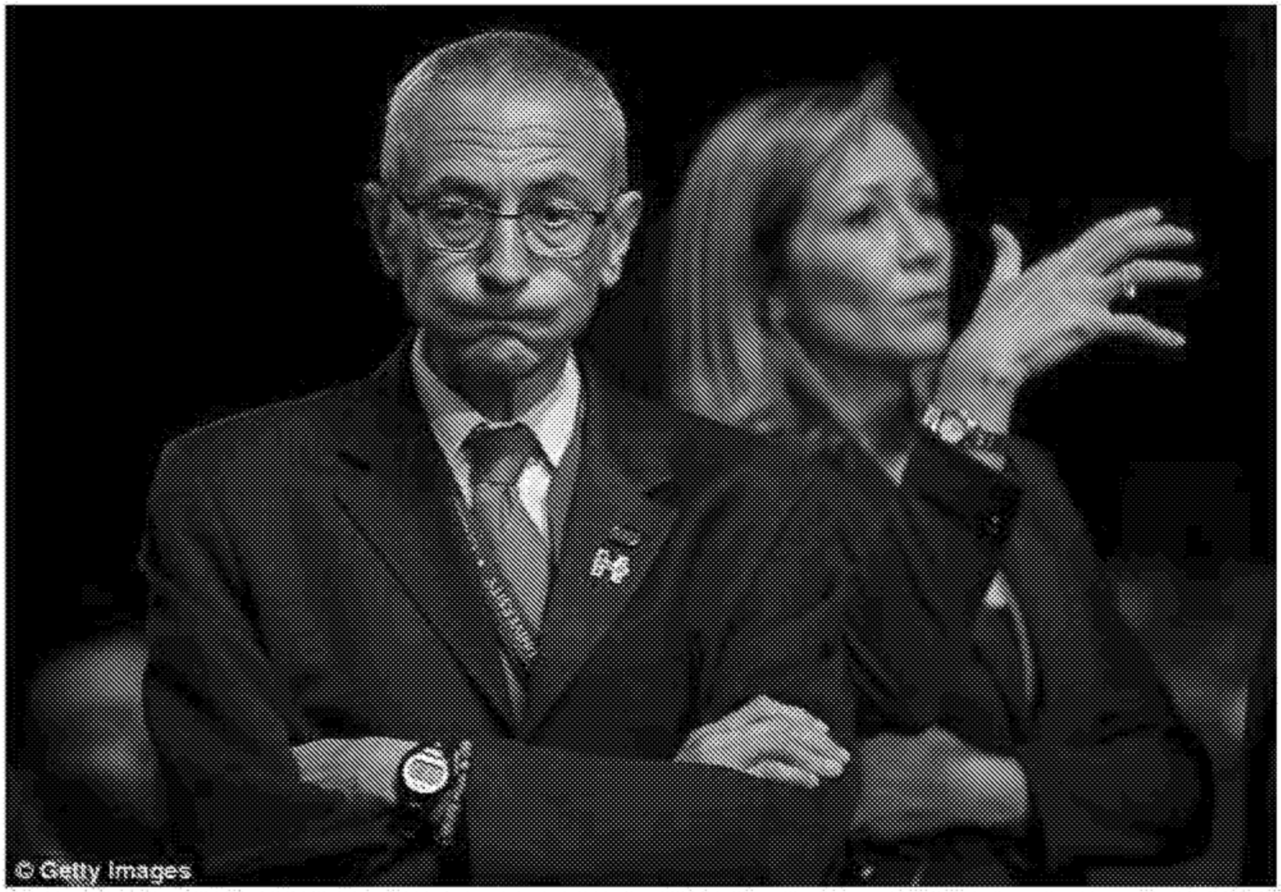
Murray was a vocal critic of human rights abuses in Uzbekistan while serving as ambassador between 2002 and 2004, a stance that pitted him against the UK Foreign Office.

He describes himself as a 'close associate' of Julian Assange and has spoken out in support of the Wikileaks founder who has faced rape allegations and is currently confined to the Ecuadorian embassy in London.

Assange has similarly disputed that charges that Wikileaks received the leaked emails from Russian sources.

'The Clinton camp has been able to project a neo-McCarthyist hysteria that Russia is responsible for everything,' Assange told John Pilger during an interview in November.

'Hillary Clinton has stated multiple times, falsely, that 17 US intelligence agencies had assessed that Russia was the source of our publications. That's false – we can say that the Russian government is not the source.'



© Getty Images

Murray suggested that John Podesta's emails might be 'of legitimate interest to the security services' in the U.S., due to his communications with Saudi Arabia lobbyists and foreign officials

The Washington Post reported last Friday that U.S. intelligence agencies had 'identified individuals with connections to the Russian government who provided WikiLeaks with thousands of hacked emails.'

The paper said U.S. senators were presented with information tying Russia to the leaks during a recent briefing by intelligence officials.

'It is the assessment of the intelligence community that Russia's goal here was to favor one candidate over the other, to help Trump get elected,' a senior U.S. official familiar with the briefing told the Post. 'That's the consensus view.'

The paper said U.S. senators were presented with information tying Russia to the leaks during a recent briefing by intelligence officials.

'It is the assessment of the intelligence community that Russia's goal here was to favor one candidate over the other, to help Trump get elected,' a senior U.S. official familiar with the briefing told the Post. 'That's the consensus view.'

The Obama administration has been examining Russia's potential role in trying to influence the presidential election. Officials said Russians hacked the Republican National Committee, but did not release that information in a deliberate effort to damage Clinton and protect Donald Trump.

Several congressional committees are also looking into the suspected Russian interference.

While there is a consensus on Capitol Hill that Russia hacked U.S. political groups and officials, some Republicans say it's not clear whether the motive was to try to swing the election or just to collect intelligence.

'Now whether they intended to interfere to the degree that they were trying to elect a certain candidate, I think that's the subject of investigation,' said Sen. John McCain on CBS Face the Nation. 'But facts are stubborn things, they did hack into this campaign.'

President elect Donald Trump raised doubts about the reports and said this was an 'excuse' by Democrats to explain Clinton's November loss.

'It's just another excuse. I don't believe it,' said Trump on Fox News Sunday.

Read more: http://www.dailymail.co.uk/news/article-4034038/Ex-British-ambassador-WikiLeaks-operative-claims-Russia-did-NOT-provide-Clinton-emails-handed-D-C-park-intermediary-disgusted-Democratic-insiders.html#ixzz4SuYJIrim

-----Original Message-----
From: [redacted] (LO) (FBI)
Sent: Thursday, December 15, 2016 7:56 AM
To: Strzok, Peter P. (CD) (FBI) [redacted]
Cc: Moffa, Jonathan C. (CD) (FBI) [redacted]
Subject: UK article on Dem Hacks

b6 -1
b7C -1
b7E -6

Pete --

Thought this was interesting.

[redacted]

b6 -1
b7C -1

http://www.dailymail.co.uk/news/article-4034038/Ex-British-ambassador-WikiLeaks-operative-claims-Russia-did-NOT-provide-Clinton-emails-handed-D-C-park-intermediary-disgusted-Democratic-insiders.html

Strzok, Peter P. (CD) (FBI)

From: Strzok, Peter P. (CD) (FBI)
Sent: Friday, December 16, 2016 8:32 PM
To: Page, Lisa C. (OGC) (FBI)
Subject: Fwd: Hey Pete...you around?

-------- Original message --------
From: "Kortan, Michael P. (DO) (FBI)" [redacted]
Date: 12/16/2016 8:21 PM (GMT-05:00)
To: "Strzok, Peter P. (CD) (FBI)" [redacted]
Subject: RE: Hey Pete...you around?

b6 -1
b7C -1
b7E -6

My thinking too. Im still working with them. More changes to come. Thanks. M

From: Strzok, Peter P. (CD) (FBI)
Sent: Friday, December 16, 2016 8:20 PM
To: Kortan, Michael P. (DO) (FBI) [redacted]
Subject: RE: Hey Pete...you around?

b6 -1
b7C -1
b7E -6

[redacted]

b5 -1

-------- Original message --------
From: "Kortan, Michael P. (DO) (FBI)" [redacted]
Date: 12/16/2016 8:12 PM (GMT-05:00)
To: "Strzok, Peter P. (CD) (FBI) [redacted]
Subject: RE: Hey Pete...you around?

b6 -1
b7C -1
b7E -6

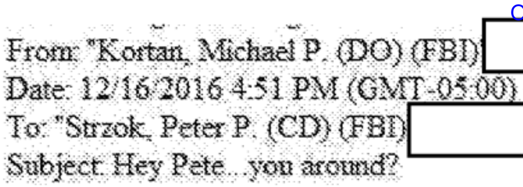
No problem. Was just interested in your thoughts on the evolving Wash Post story today. They are now updating once again. Tx, M

From: Strzok, Peter P. (CD) (FBI)
Sent: Friday, December 16, 2016 8:10 PM
To: Kortan, Michael P. (DO) (FBI) [redacted]
Subject: RE: Hey Pete...you around?

b6 -1
b7C -1
b7E -6

Sorry Mike just clearing email. I'm on cell [redacted] if you still need me.

-------- Original message --------



From: "Kortan, Michael P. (DO) (FBI)[redacted]
Date: 12/16/2016 4:51 PM (GMT-05:00)
To: "Strzok, Peter P. (CD) (FBI)[redacted]
Subject: Hey Pete...you around?

b6 -1
b7C -1
b7E -6

Strzok, Peter P. (CD) (FBI)

From:	Strzok, Peter P. (CD) (FBI)
Sent:	Monday, December 19, 2016 12:35 PM
To:	Baker, James A. (OGC) (FBI); Anderson, Trisha B. (OGC) (FBI); Page, Lisa C. (OGC) (FBI); [redacted] OGC) (FBI) [redacted] (DO) (FBI)
Cc:	Moffa, Jonathan C. (CD) (FBI)
Subject:	New footnote

b6 -1
b7C -1

Just sent you new footnote language on red side.

Strzok, Peter P. (CD) (FBI)

Subject:	BSS/BSS mtg
Location:	4012
Start:	Monday, December 19, 2016 3:00 PM
End:	Monday, December 19, 2016 3:30 PM
Show Time As:	Tentative
Recurrence:	(none)
Meeting Status:	Not yet responded
Organizer:	Strzok, Peter P. (CD) (FBI)
Required Attendees:	Page, Lisa C. (OGC) (FBI)

Strzok, Peter P. (CD) (FBI)

Subject:	BSS/BSS mtg
Location:	4012
Start:	Monday, December 19, 2016 3:00 PM
End:	Monday, December 19, 2016 3:30 PM
Recurrence:	(none)
Meeting Status:	Accepted
Organizer:	Strzok, Peter P. (CD) (FBI)
Required Attendees:	Page, Lisa C. (OGC) (FBI)

Strzok, Peter P. (CD) (FBI)

From:	Strzok, Peter P. (CD) (FBI)
Sent:	Monday, December 19, 2016 5:45 PM
To:	Rybicki, James E. (DO) (FBI); Priestap, E. W. (CD) (FBI); Page, Lisa C. (OGC) (FBI); Baker, James A. (OGC) (FBI); Anderson, Trisha B. (OGC) (FBI); [redacted] (OGC) (FBI)
Cc:	Kortan, Michael P. (DO) (FBI)
Subject:	RE: SW

b6 -1
b7C -1

I do not. Checking...

-------- Original message --------
From: "Rybicki, James E. (DO) (FBI)"[redacted]
Date: 12/19/2016 5:30 PM (GMT-05:00)
To: "Priestap, E. W. (CD) (FBI)"[redacted]"Strzok, Peter P. (CD) (FBI)" b6 -1
[redacted]"Page, Lisa C. (OGC) (FBI)"[redacted]"Baker, James A. (OGC) b7C -1
(FBI)[redacted]Anderson, Trisha B. (OGC) (FBI)" b7E -6
[redacted]OGC) (FBI)[redacted]
Cc: "Kortan, Michael P. (DO) (FBI)"[redacted]
Subject: SW

Do we have a copy of the search warrant that will be unsealed tomorrow (with redactions in place)?

Thanks,
Jim

James Rybicki
Chief of Staff
Federal Bureau of Investigation
[redacted] b6 -1
b7C -1

Strzok, Peter P. (CD) (FBI)

From: Strzok, Peter P. (CD) (FBI)
Sent: Tuesday, December 20, 2016 4:56 PM
To: Page, Lisa C. (OGC) (FBI); McCabe, Andrew G. (DO) (FBI); Sporre, Eric W. (CYD) (FBI)
Cc: Smith, Scott S. (PG) (FBI); [redacted] CYD) (FBI); [redacted] DO) (FBI); Priestap, E. W. (CD) (FBI); Baker, James A. (OGC) (FBI) b6 -1 b7C -1
Subject: RE: post-SIOC brief for the AG

OK will be there

-------- Original message --------
From: "Page, Lisa C. (OGC) (FBI) [redacted] b6 -1
Date: 12/20/2016 4:51 PM (GMT-05:00) b7C -1
To: "McCabe, Andrew G. (DO) (FBI)" [redacted] "Sporre, Eric W. (CYD) (FBI)" b7E -6
[redacted] "Strzok, Peter P. (CD) (FBI)" [redacted]
Cc: "Smith, Scott S. (PG) (FBI)" [redacted] CYD) (FBI)"
[redacted] DO) (FBI)" [redacted] "Priestap, E. W.
(CD) (FBI) [redacted] "Baker, James A. (OGC) (FBI)" [redacted]
Subject: RE: post-SIOC brief for the AG

Adding Jim Baker.

From: McCabe, Andrew G. (DO) (FBI)
Sent: Tuesday, December 20, 2016 4:50 PM
To: Page, Lisa C. (OGC) (FBI) [redacted] Sporre, Eric W. (CYD) (FBI) [redacted] b6 -1
Strzok, Peter P. (CD) (FBI [redacted] b7C -1
Cc: Smith, Scott S. (PG) (FBI [redacted] CYD) (FBI) b7E -6
[redacted] DO) (FBI [redacted] Priestap, E. W. (CD)
(FBI [redacted]
Subject: RE: post-SIOC brief for the AG

Thanks all. Let's plan I need a quick pre-brief tomorrow immediately following the morning Intel brief at 0800.

Thanks.

Andrew G. McCabe
Deputy Director
Federal Bureau of Investigation b6 -1
[redacted] b7C -1

b6 -1
b7C -1
b7E -6

-------- Original message --------
From: "Page, Lisa C. (OGC) (FBI) [redacted]

From: Page, Lisa C. (OGC) (FBI) [redacted]
Date: 12/20/16 4:43 PM (GMT-05:00)
To: "Sporre, Eric W. (CYD) (FBI) [redacted] "Strzok, Peter P. (CD) (FBI)"
[redacted]
Cc: "Smith, Scott S. (PG) (FBI) [redacted] (CYD) (FBI)"
[redacted] (DO) (FBI)" [redacted] "Priestap, E. W. (CD) (FBI) [redacted] "McCabe, Andrew G. (DO) (FBI)" [redacted]
Subject: post-SIOC brief for the AG

b6 -1
b7C -1
b7E -6

[redacted]

b5 -3

Lisa

Strzok, Peter P. (CD) (FBI)

From: Strzok, Peter P. (CD) (FBI)
Sent: Tuesday, December 20, 2016 4:58 PM
To: Anderson, Trisha B. (OGC) (FBI) [redacted] (OGC) (FBI); Page, Lisa C. (OGC) (FBI) [redacted] OGC) (FBI); Moffa, Jonathan C. (CD) (FBI)
Cc: [redacted] OGC) (FBI)
Subject: RE: Message to SACs/ADICs

b6 -1
b7C -1

Good

-------- Original message --------
From: "Anderson, Trisha B. (OGC) (FBI)" [redacted]
Date: 12/20/2016 4:46 PM (GMT-05:00)
To: [redacted] OGC) (FBI) [redacted] "Page, Lisa C. (OGC) (FBI)" [redacted] (OGC) (FBI)" [redacted] "Strzok, Peter P. (CD) (FBI)" [redacted] "Moffa, Jonathan C. (CD) (FBI)" [redacted]
Cc: [redacted] (OGC) (FB [redacted]
Subject: RE: Message to SACs/ADICs

b6 -1
b7C -1
b7E -6

The language looks good to me.

From: [redacted] (OGC) (FBI)
Sent: Tuesday, December 20, 2016 4:45 PM
To: Page, Lisa C. (OGC) (FBI [redacted] OGC) (FBI) [redacted] Strzok, Peter P. (CD) (FBI [redacted] Moffa, Jonathan C. (CD) (FBI) [redacted] Anderson, Trisha B. (OGC) (FBI) [redacted]
Cc: [redacted] OGC) (FBI) [redacted]
Subject: RE: Message to SACs/ADICs

b6 -1
b7C -1
b7E -6

Yeah, complicated. If we're good with this, I can send it on to Rich, copying you all.

From: Page, Lisa C. (OGC) (FBI)
Sent: Tuesday, December 20, 2016 4:36 PM
To: [redacted] OGC) (FBI) [redacted] (OGC) (FBI) [redacted] Strzok, Peter P. (CD) (FBI) [redacted] Moffa, Jonathan C. (CD) (FBI) [redacted] Anderson, Trisha B. (OGC) (FBI) [redacted]
C [redacted] OGC) (FBI) [redacted]
Subject: RE: Message to SACs/ADICs

b6 -1
b7C -1
b7E -6

Oh.

Yeah, never mind.

From: [redacted] OGC) (FBI)
Sent: Tuesday, December 20, 2016 4:30 PM

b6 -1
b7C -1

To [redacted] (OGC) (FBI) [redacted] Page, Lisa C. (OGC) (FBI) [redacted] b6 -1
Strzok, Peter P. (CD) (FBI [redacted] Moffa, Jonathan C. (CD) (FBI) b7C -1
[redacted] Anderson, Trisha B. (OGC) (FBI) [redacted] b7E -6
Cc [redacted] OGC) (FBI [redacted]
Subject: RE: Message to SACs/ADICs

[redacted] b5 -1, 3

[redacted] b6 -1
Assistant General Counsel b7C -1
National Security Law Branch
[redacted]

From: [redacted] (OGC) (FBI) b6 -1
Sent: Tuesday, December 20, 2016 4:18 PM b7C -1
To: Page, Lisa C. (OGC) (FBI [redacted] Strzok, Peter P. (CD) (FBI [redacted] b7E -6
Moffa, Jonathan C. (CD) (FBI) [redacted] Anderson, Trisha B. (OGC) (FBI)
[redacted] (OGC) (FBI) [redacted]
Cc [redacted] OGC) (FBI [redacted]
Subject: RE: Message to SACs/ADICs

[redacted] b5 -1
b6 -1
b7C -1

[redacted]

From: Page, Lisa C. (OGC) (FBI)
Sent: Tuesday, December 20, 2016 4:13 PM
To [redacted] OGC) (FBI) [redacted] Strzok, Peter P. (CD) (FBI) b6 -1
[redacted] Moffa, Jonathan C. (CD) (FBI [redacted] Anderson, Trisha B. b7C -1
(OGC) (FBI) [redacted] OGC) (FBI [redacted] b7E -6
Subject: RE: Message to SACs/ADICs

My only question is [redacted] b5 -1

From [redacted] (OGC) (FBI)
Sent: Tuesday, December 20, 2016 3:45 PM
To: Strzok, Peter P. (CD) (FBI) [redacted] Moffa, Jonathan C. (CD) (FBI) b6 -1
[redacted] Anderson, Trisha B. (OGC) (FBI [redacted] Page, Lisa C. b7C -1
(OGC) (FBI) [redacted] OGC) (FBI [redacted] b7E -6
Subject: Message to SACs/ADICs
Importance: High

Rich Quinn asked me to draft up something [redacted] b5 -1, 3
Of course, they want to send it out at 4. I'd appreciate your thoughts/comments before mass dissemination.

[redacted]

b5 -1, 2, 3

[redacted]
Assistant General Counsel
National Security Law Branch
Office of the General Counsel
Federal Bureau of Investigation
[redacted]

b6 -1
b7C -1

Confidentiality Statement:
This message is transmitted to you by the Office of the General Counsel of the Federal Bureau of Investigation. The message, along with any attachments, may be confidential and legally privileged. If you are not the intended recipient of this message, please destroy it promptly without further retention or dissemination (unless otherwise required by law). Please notify the sender of the error by a separate e-mail or by calling [redacted]

Strzok, Peter P. (CD) (FBI)

From: Strzok, Peter P. (CD) (FBI)
Sent: Tuesday, December 20, 2016 7:23 PM
To: Page, Lisa C. (OGC) (FBI)[redacted](DO) (FBI) b6 -1 b7C -1
Subject: Fwd: Npr
Importance: High

-------- Original message --------
From: "Strzok, Peter P. (CD) (FBI)"[redacted] b6 -1 b7C -1 b7E -6
Date: 12/20/2016 7:22 PM (GMT-05:00)
To: "Priestap, E. W. (CD) (FBI)"[redacted]'Moffa, Jonathan C. (CD) (FBI)"
[redacted]
Subject: Npr

Bill Evanina, "the head of US counterintelligence," about to talk on npr about putting together the report on Russian Intel activities.

Did he coordinate with anyone?

Strzok, Peter P. (CD) (FBI)

From:	Strzok, Peter P. (CD) (FBI)
Sent:	Tuesday, December 20, 2016 7:40 PM
To:	Page, Lisa C. (OGC) (FBI)
Subject:	Fwd: For America's Top Spy Catcher, A World Of Problems To Fix — And Prevent : Parallels : NPR

http://www.npr.org/sections/parallels/2016/12/20/506296243/for-americas-top-spy-catcher-a-world-of-problems-to-fix-and-prevent

For America's Top Spy Catcher, A World Of Problems To Fix — And Prevent

William Evanina, the head of U.S. counterintelligence, estimates that more than 100 Russian spies are currently operating on U.S. soil.

Courtesy of the Office of the Director of National Intelligence

William Evanina holds two official job titles: national counterintelligence executive and director of the National Counterintelligence and Security Center.

Eyes glazing over? Here's a simpler way to think of him: as the nation's spy catcher in chief.

As the head of U.S. counterintelligence, Evanina is in charge of keeping America's secrets out of enemy hands. 2016 has proved an exceptionally challenging year, between Russian hacks and another massive data breach at the National Security Agency.

But before we get to those, here's a story that yields some insight into the kind of year

Evanina has had: On May 4, he was meeting a friend and former colleague at the Silver Diner in McLean, Va. They were tucking into lunch when they heard a crash.

"A lot of people started yelling, 'Gun!' And then there was multiples crashes," Evanina remembers.

A Hummer had slammed into the diner. The man driving it — a cook who had been suspended — backed up and tried again, three or four times.

"And then he set himself on fire, trying to burn the restaurant down," says Evanina, who may now run counterintelligence efforts for the entire U.S. government, but remains — by training and instinct — an FBI agent.

Evanina helped pull the man from the burning Hummer. And then he cuffed him.

"I'm still an FBI agent," he says, "and until that day is over, I will be an FBI agent, and that entails carrying handcuffs."

One customer died from his injuries. The man Evanina cuffed — the suspended cook — was charged with second-degree murder.

"Crazy things happen," says Evanina. "I just happened to be in the right place at the right time. When you look at that individual, that is the epitome of the insider threat."

Insider threats are a phenomenon Evanina has had to confront more often than he might have liked over his 27-year career. In 2013, when NSA contractor Edward Snowden fled the country carrying a laptop stuffed with secrets, Evanina was assigned to the investigation. At the time, he was assistant special agent in charge of the FBI's Washington field office.

This, he says, "makes it difficult for me to opine on Edward Snowden. But in my job now, I handle the damage assessment aspect of Mr. Snowden. On a quarterly basis, we develop a damage assessment, provide that to Congress and the White House."

That means every three months, Evanina briefs official Washington on the ongoing fallout from Snowden. Which raises the question: How much classified material may yet come to light? Evanina says Snowden is estimated to have taken 1.5 million documents.

"If you subtract the give or take 1,000 that have been disclosed, there's a lot more to go," he says. "We have a pretty good fundamental idea, every agency does, as to what documents were stolen by Mr. Snowden. And we've put them into tranches, in terms of significance and in terms of damage that could be caused. And every day, every [U.S. intelligence] agency is watching the world media to see what's being disclosed."

This year, the world learned of yet another possible inside job at the NSA. Harold "Hal" Martin III, another contractor, was arrested in August. Like Snowden, he had worked at the NSA. He was working for the Pentagon at the time of his arrest.

Federal prosecutors have not claimed evidence of links between Martin and a foreign power. But at his house in Maryland, investigators found huge piles of classified documents, which Martin is alleged to have stolen over a two-decade period.

Coming just three years after the Snowden episode, is there any way to view Martin's case as something other than an epic security failure?

Evanina says there is. "Someone who is in an insider threat, who's seeking to do damage, will do the damage," he says. "It's really, really difficult to stop that person once they've made a decision."

Evanina says the answer is not to rely on intrusive security checks. He insists the NSA's internal security is excellent. Instead, he argues that spy agencies need to do a better job of monitoring behavioral indicators: identifying when employees are vulnerable — whether through financial or marital troubles or because they've been passed over for promotion — and then intervening before they act in detrimental ways.

Evanina also says that obsessing over Snowden or Martin will get you only so far. "We spend a lot of time on fixing what's happened, and not enough time on what the future looks like six months from now," he says. "What are the new technologies and capabilities to take [classified materials] away?"

Speaking of the future, Evanina will spend the next several weeks helping to pull together a White House-ordered review of election year cyber-intrusions. The review follows an October statement issued by Evanina's boss, Director of National Intelligence James Clapper, and by the Department of Homeland Security, which concludes that Russia's "senior-most officials" authorized recent hacks.

Evanina's role is to unravel which Russian spy agencies were involved.

"It gets characterized as the 'government of Russia,' " he says. "Well, in our world, it's a little bit more complicated than that."

An investigation by the private cybersecurity firm Crowdstrike has attributed the hacks to Russia's military and domestic security agencies. Evanina is probing that further.

"There's an intense competitiveness within the Russian intelligence services," he notes. "The GRU [main intelligence directorate] and the SVR [foreign intelligence service] and the FSB [federal security service] are competing for resource dollars and for activity here in the U.S."

That presents both challenge and opportunity for American spy agencies. Knowing which specific adversary they're dealing with, Evanina says, helps to inform the response.

Meanwhile, he estimates that more than 100 Russian spies are operating on U.S. soil right now.

"They're here to do their country's bidding," he says. "Acquiring plans and intentions of our country, and stealing our trade secrets and proprietary information. Our job is to identify them and track them down, surveil them and neutralize their efforts."

As to where the Russians operate, Evanina says they're in big cities: "Washington, D.C. New York City. Los Angeles. San Francisco. Our innovation hubs."

That's because Russian intelligence officers are focused on America's energy, telecommunications and financial sectors, he says. So there's plenty to keep Evanina busy until next June, when he wraps up his tour as the country's top spy catcher.

Strzok, Peter P. (CD) (FBI)

From:	Strzok, Peter P. (CD) (FBI)
Sent:	Wednesday, December 21, 2016 7:33 PM
To:	Page, Lisa C. (OGC) (FBI)
Subject:	FW: On Russia, Cyber, and Espionage

http://www.defenseone.com/technology/2016/12/are-we-new-era-espionage/133932/?oref=defenseone_today_nl

This weekend, Michael Morell, the former acting director of the CIA, was asked about the intelligence community's findings that Russia interfered in the presidential election. His answer was unequivocal: The country isn't grasping the magnitude of the story, he told The Cipher Brief. "To me, and this is to me not an overstatement, this is the political equivalent of 9/11."

-----Original Message-----
From: [redacted](DI) (FBI)
Sent: Wednesday, December 21, 2016 5:05 PM
To: Moffa, Jonathan C. (CD) (FBI[redacted]Strzok, Peter P. (CD) (FBI)
[redacted](CD) (FBI)[redacted]
[redacted](CD) (FBI[redacted]
[redacted](DI) (FBI[redacted]Tsiumis, Allison R. (CYD) (FBI)
[redacted]CYD) (FB[redacted]
(CYD) (FBI[redacted](CD) (FBI)[redacted]
[redacted](CD) (FBI)[redacted]
Subject: On Russia, Cyber, and Espionage

b6 -1
b7C -1
b7E -6

Folks,

I don't recognize many of the folks quoted, but this short piece from The Atlantic (reposted in Defense One) is worth a glance: http://www.defenseone.com/technology/2016/12/are-we-new-era-espionage/133932/?oref=defenseone_today_nl

[redacted]
Senior National Intelligence Officer
Federal Bureau of Investigation
[redacted]

b6 -1
b7C -1

Strzok, Peter P. (CD) (FBI)

From:	Strzok, Peter P. (CD) (FBI)
Sent:	Thursday, December 22, 2016 12:35 PM
To:	Page, Lisa C. (OGC) (FBI); [redacted] (DO) (FBI)
Subject:	Fwd: House Intel report on Snowden today
Attachments:	hpsci_snowden_review_declassified.pdf

b6 -1
b7C -1

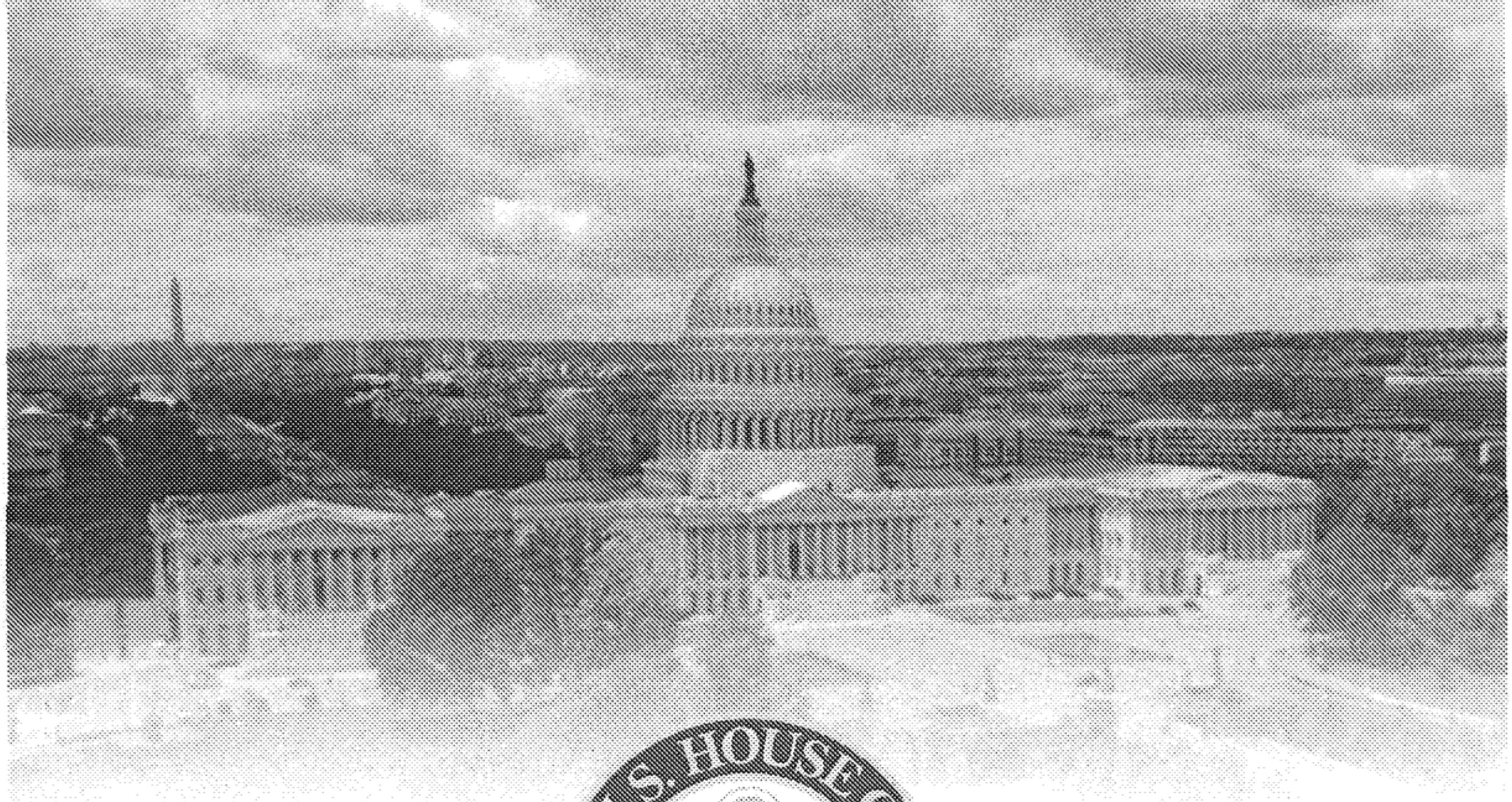
FYI, Mike sent to Andy [redacted]

b7E -4

-------- Original message --------
From: "Kortan, Michael P. (DO) (FBI)" [redacted]
Date: 12/22/2016 12:23 PM (GMT-05:00)
To: "Steinbach, Michael B. (DO) (FBI)" [redacted] "Priestap, E. W. (CD) (FBI)" [redacted] "Strzok, Peter P. (CD) (FBI)" [redacted] "Herring, Jason V. (CD) (FBI) [redacted]
Cc: "McCabe, Andrew G. (DO) (FBI)" [redacted]
Subject: House Intel report on Snowden today

b6 -1
b7C -1
b7E -6

Fyi, The news media made note of the reference that he is in regular contact with the host country services.



(U) Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden

September 15, 2016

(U) Executive Summary

(U) In June 2013, former National Security Agency (NSA) contractor Edward Snowden perpetrated the largest and most damaging public release of classified information in U.S. intelligence history. In August 2014, the Chairman and Ranking Member of the House Permanent Select Committee on Intelligence (HPSCI) directed Committee staff to carry out a comprehensive review of the unauthorized disclosures. The aim of the review was to allow the Committee to explain to other Members of Congress—and, where possible, the American people—how this breach occurred, what the U.S. Government knows about the man who committed it, and whether the security shortfalls it highlighted had been remedied.

(U) Over the next two years, Committee staff requested hundreds of documents from the Intelligence Community (IC), participated in dozens of briefings and meetings with IC personnel, conducted several interviews with key individuals with knowledge of Snowden's background and actions, and traveled to NSA Hawaii to visit Snowden's last two work locations. The review focused on Snowden's background, how he was able to remove more than 1.5 million classified documents from secure NSA networks, what the 1.5 million documents contained, and the damage their removal caused to national security.

(U) The Committee's review was careful not to disturb any criminal investigation or future prosecution of Snowden, who has remained in Russia since he fled there on June 23, 2013. Accordingly, the Committee did not interview individuals whom the Department of Justice identified as possible witnesses at Snowden's trial, including Snowden himself, nor did the Committee request any matters that may have occurred before a grand jury. Instead, the IC provided the Committee with access to other individuals who possessed substantively similar knowledge as the possible witnesses. Similarly, rather than interview Snowden's NSA co-workers and supervisors directly, Committee staff interviewed IC personnel who had reviewed reports of interviews with Snowden's co-workers and supervisors. The Committee remains hopeful that Snowden will return to the United States to face justice.

(U) The bulk of the Committee's 37-page review, which includes 237 footnotes, must remain classified to avoid causing further harm to national security; however, the Committee has made a number of unclassified findings. These findings demonstrate that the public narrative popularized by Snowden and his allies is rife with falsehoods, exaggerations, and crucial omissions, a pattern that began before he stole 1.5 million sensitive documents.

(U) First, Snowden caused tremendous damage to national security, and the vast majority of the documents he stole have nothing to do with programs impacting individual privacy interests—they instead pertain to military, defense, and intelligence programs of great interest to America's adversaries. A review of the materials Snowden compromised makes clear that he handed over secrets that protect American troops overseas and secrets that provide vital defenses against terrorists and nation-states. Some of Snowden's disclosures exacerbated and accelerated existing trends that diminished the IC's capabilities to collect against legitimate foreign intelligence targets, while others resulted in the loss of intelligence streams that had saved American lives. Snowden insists he has not shared the full cache of 1.5 million classified documents with anyone; however, in June 2016, the deputy chairman of the

Russian parliament's defense and security committee publicly conceded that "Snowden did share intelligence" with his government. Additionally, although Snowden's professed objective may have been to inform the general public, the information he released is also available to Russian, Chinese, Iranian, and North Korean government intelligence services; any terrorist with Internet access; and many others who wish to do harm to the United States.

(U) The full scope of the damage inflicted by Snowden remains unknown. Over the past three years, the IC and the Department of Defense (DOD) have carried out separate reviews—with differing methodologies—of the damage Snowden caused. Out of an abundance of caution, DOD reviewed all 1.5 million documents Snowden removed. The IC, by contrast, has carried out a damage assessment for only a small subset of the documents. The Committee is concerned that the IC does not plan to assess the damage of the vast majority of documents Snowden removed. Nevertheless, even by a conservative estimate, the U.S. Government has spent hundreds of millions of dollars, and will eventually spend billions, to attempt to mitigate the damage Snowden caused. These dollars would have been better spent on combating America's adversaries in an increasingly dangerous world.

(U) Second, Snowden was not a whistleblower. Under the law, publicly revealing classified information does not qualify someone as a whistleblower. However, disclosing classified information that shows fraud, waste, abuse, or other illegal activity to the appropriate law enforcement or oversight personnel—including to Congress—does make someone a whistleblower and affords them with critical protections. Contrary to his public claims that he notified numerous NSA officials about what he believed to be illegal intelligence collection, the Committee found no evidence that Snowden took any official effort to express concerns about U.S. intelligence activities—legal, moral, or otherwise—to any oversight officials within the U.S. Government, despite numerous avenues for him to do so. Snowden was aware of these avenues. His only attempt to contact an NSA attorney revolved around a question about the legal precedence of executive orders, and his only contact to the Central Intelligence Agency (CIA) Inspector General (IG) revolved around his disagreements with his managers about training and retention of information technology specialists.

(U) Despite Snowden's later public claim that he would have faced retribution for voicing concerns about intelligence activities, the Committee found that laws and regulations in effect at the time of Snowden's actions afforded him protection. The Committee routinely receives disclosures from IC contractors pursuant to the Intelligence Community Whistleblower Protection Act of 1998 (IC WPA). If Snowden had been worried about possible retaliation for voicing concerns about NSA activities, he could have made a disclosure to the Committee. He did not. Nor did Snowden remain in the United States to face the legal consequences of his actions, contrary to the tradition of civil disobedience he professes to embrace. Instead, he fled to China and Russia, two countries whose governments place scant value on their citizens' privacy or civil liberties—and whose intelligence services aggressively collect information on both the United States and their own citizens.

(U) To gather the files he took with him when he left the country for Hong Kong, Snowden infringed on the privacy of thousands of government employees and contractors. He obtained his colleagues' security credentials through misleading means, abused his access as a systems administrator to search his co-workers' personal drives, and removed the personally identifiable information of thousands of IC employees and contractors. From Hong Kong he went to Russia, where he remains a guest of the Kremlin to this day.

(U) It is also not clear Snowden understood the numerous privacy protections that govern the activities of the IC. He failed basic annual training for NSA employees on Section 702 of the Foreign Intelligence Surveillance Act (FISA) and complained the training was rigged to be overly difficult. This training included explanations of the privacy protections related to the PRISM program that Snowden would later disclose.

(U) Third, two weeks before Snowden began mass downloads of classified documents, he was reprimanded after engaging in a workplace spat with NSA managers. Snowden was repeatedly counseled by his managers regarding his behavior at work. For example, in June 2012, Snowden became involved in a fiery e-mail argument with a supervisor about how computer updates should be managed. Snowden added an NSA senior executive several levels above the supervisor to the e-mail thread, an action that earned him a swift reprimand from his contracting officer for failing to follow the proper protocol for raising grievances through the chain of command. Two weeks later, Snowden began his mass downloads of classified information from NSA networks. Despite Snowden's later claim that the March 2013 congressional testimony of Director of National Intelligence James Clapper was a "breaking point" for him, these mass downloads ***predated*** Director Clapper's testimony by eight months.

(U) Fourth, Snowden was, and remains, a serial exaggerator and fabricator. A close review of Snowden's official employment records and submissions reveals a pattern of intentional lying. He claimed to have left Army basic training because of broken legs when in fact he washed out because of shin splints. He claimed to have obtained a high school degree equivalent when in fact he never did. He claimed to have worked for the CIA as a "senior advisor," which was a gross exaggeration of his entry-level duties as a computer technician. He also doctored his performance evaluations and obtained new positions at NSA by exaggerating his résumé and stealing the answers to an employment test. In May 2013, Snowden informed his supervisor that he would be out of the office to receive treatment for worsening epilepsy. In reality, he was on his way to Hong Kong with stolen secrets.

(U) Finally, the Committee remains concerned that more than three years after the start of the unauthorized disclosures, NSA, and the IC as a whole, have not done enough to minimize the risk of another massive unauthorized disclosure. Although it is impossible to reduce the chance of another Snowden to zero, more work can and should be done to improve the security of the people and computer networks that keep America's most closely held secrets. For instance, a recent DOD Inspector General report directed by the Committee found that NSA has yet to effectively implement its post-Snowden security improvements. The Committee has taken actions to improve IC information security in the Intelligence Authorization Acts for Fiscal Years 2014, 2015, 2016, and 2017, and looks forward to working with the IC to continue to improve security.

Table of Contents

(U) Scope and Methodology

(U) Since June 2013, the unauthorized disclosures of former NSA contractor Edward Snowden and the impact of these disclosures on the U.S. Intelligence Community (IC) have been a subject of continual Committee oversight. The Committee held an open hearing on the disclosures on June 18, 2013, and, over the next year, held eight additional hearings and briefings, followed by numerous staff-level briefings on Snowden's disclosures.

(U) In August 2014, then-Chairman Rogers and Ranking Member Ruppersberger directed Committee staff to begin a review of the actions and motivations of Edward Snowden related to his removal of more than 1.5 million classified documents from secure NSA networks. The intent was not to duplicate the damage assessments already under way in the executive branch; rather, the report would help explain to other Members of Congress—and, where possible, the American people—how the "most massive and damaging theft of intelligence information in our history" occurred,[1] what the U.S. Government knows about the man who perpetrated it, and what damage his actions caused.

(U) Over the next two years, Committee staff requested hundreds of documents from the IC, participated in dozens of briefings and meetings with IC personnel, and conducted several interviews with key individuals with knowledge of Snowden's background and actions, and traveled to NSA Hawaii to visit Snowden's last two work locations.

(U) The Committee's product is a review, not an investigation, largely in deference to any criminal investigation or future prosecution. Since he arrived in Russia on June 23, 2013, Snowden has not returned to the United States to face the criminal charges against him. Accordingly, the Committee did not interview or seek documents from individuals whom the Department of Justice identified as possible witnesses at Snowden's trial, including Snowden himself, nor did the Committee request any matters that may have occurred before a grand jury. Instead, the IC provided the Committee with access to other individuals who possessed substantively similar knowledge. Similarly, rather than interview Snowden's NSA co-workers and supervisors directly, Committee staff interviewed IC personnel who had reviewed reports of interviews with Snowden's co-workers and supervisors.

(U) The Committee's review has informed numerous congressionally directed actions and resource allocation decisions in the enacted Intelligence Authorization Acts for Fiscal Years 2014, 2015, and 2016, and in the House-passed Intelligence Authorization Act for Fiscal Year 2017.

(U) Early Life

(U) Edward Joseph Snowden was born on June 21, 1983, in Elizabeth City, North Carolina. His parents, Lon Snowden, a Coast Guard chief petty officer, and Elizabeth Snowden,

[1] Testimony of Director of National Intelligence James R. Clapper, HPSCI Worldwide Threats Hearing (Open Session, Feb. 4, 2014).

a federal court clerk, moved the family to Annapolis, Maryland, when Edward was a child.[2] In 2001, his parents divorced.[3]

(U) By his own account, Snowden was a poor student.[4] He dropped out of high school in his sophomore year and began taking classes at the local community college.[5] Snowden hoped that the classes would allow him to earn a General Education Diploma (GED), but nothing the Committee found indicates that he did so. To the contrary, on an applicant resume submitted to NSA in 2012, Snowden indicated that he graduated from "Maryland High School" in 2001;[6] earlier, in 2006, Snowden had posted on a public web forum that he did not "have a degree of ANY type. I don't even have a high school diploma."[7]

(U) After leaving community college, Snowden eventually enlisted in the Army Reserve as a special forces recruit. He left after five months, receiving a discharge in September 2004 without finishing training courses.[8] Snowden would later claim he had to leave basic training because "he broke both his legs in a training accident."[9] An NSA security official the Committee interviewed took a different view, telling Committee staff that Snowden was discharged after suffering from "shin splints," a common overuse injury.[10]

(U) Unable to pursue his preferred military career, Snowden turned to security guard work. In February 2005, the University of Maryland's Center for the Advanced Study of

[2] "NSA Leaker Edward Snowden Has Ties to North Carolina," *Raleigh News & Observer* (Aug. 1, 2013).

[3] John M. Broder & Scott Shane, "For Snowden, A Life of Ambition, Despite the Drifting," *New York Times* (June 15, 2013).

[4] Glenn Greenwald, Ewen MacAskill, and Laura Poitras, "Edward Snowden: the Whistleblower Behind the NSA Surveillance Revelations," *The Guardian* (June 11, 2013), *available at* https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance (accessed June 28, 2016).

[5] Matthew Mosk, et al., "TIMELINE: Edward Snowden's Life As We Know It," ABC News, (June 13, 2013).

[6] *See, e.g.*, Edward Snowden Resume. Regarding "High School Education," the resume Snowden submitted to NSA's Tailored Access Operations unit says as follows: For "Grad/Exit dt," Snowden wrote "2001-06-21;" For his "School," Snowden wrote "Maryland High School"; and for "Level Achieved", Snowden wrote "High School Graduate."

[7] *See supra*, note 3. One of Snowden's associates claims to have reviewed official educational records that demonstrate Snowden's passage of a high school equivalency test and receipt of high school equivalency diploma in June 2004. Any receipt of such a diploma in 2004 stands in tension with Snowden's 2006 claim to not have a "degree of any type [or]… even a high school diploma"; and with his 2012 resume, which stated that he either left or graduated from "Maryland High School" in 2001.

[8] "What We Know About NSA Leaker Edward Snowden," *NBC News* (June 10, 2013), *available at* http://usnews.nbcnews.com/_news/2013/06/10/18882615-what-we-know-about-nsa-leaker-snowden?lite (accessed June 28, 2016); *see also* "Edward Snowden Did Enlist For Special Forces, US Army Confirms," *The Guardian* (June 10, 2013), *available at* http://www.theguardian.com/world/2013/jun/10/edward-snowden-army-special forces (accessed September 15, 2016).

[9] "Edward Snowden Did Enlist For Special Forces, US Army Confirms," *The Guardian* (June 10, 2013), *available at* http://www.theguardian.com/world/2013/jun/10/edward-snowden-army-special forces (accessed September 15, 2016).

[10] *See supra*, note 6. If untreated, shin splints can progress into stress fractures, but the Committee found no evidence that Snowden was involved in a training accident.

Language (CASL) sponsored Snowden for a Top Secret security clearance.[11] The investigation for that clearance turned up only one piece of derogatory information: [redacted] of Snowden's said she did not recommend him for access to classified information.[12] Snowden sought counseling [redacted], and the counselor recommended him for a position of trust with no reservations.[13] The favorable investigation, combined with a successful polygraph test, enabled Snowden to work at CASL's lobby reception desk as a "security specialist." He worked there for four months, until he was hired by BAE Systems to work on a CIA Global Communications Services Contract.

~~(S//NF)~~ Snowden's stint as a BAE Systems contractor was similarly short-lived. For less than a year, he worked as a systems administrator who "managed installations and application rollouts" in the Washington, DC, area.[14] In August 2006, he converted from a contractor to a CIA employee. As part of that conversion, Snowden went through an "entrance on duty" psychological evaluation. [redacted].[15]

(U) CIA Employment

(U) Snowden was not, as he would later claim, a "senior advisor" at CIA.[16] Rather, his only position as a CIA employee was as a Telecommunications Information Systems Officer, or TISO. The job description for a TISO makes clear that the position is an entry-level IT support function, not a senior executive. TISOs "operate, maintain, install, and manage telecommunications systems," and "provide project management and systems integration for voice and data communications systems," including "support to customers after installation."[17] Even so, the position may have appealed to Snowden because TISOs "typically spend 60-70% of their career abroad."[18]

(U) In November 2006—less than three months after starting with CIA—Snowden contacted the Agency's Inspector General (IG) seeking "guidance" because he felt he was "being

[11] NSA, Edward Snowden Timeline (Sept. 30, 2014). Overall document classified C//NF; cited portion classified U//FOUO.
[12] NSA, FBI, and NCSC, "'Negative Information' Found in Edward Snowden's Personnel Security File," (Sept. 30, 2014). Overall document classified U//FOUO.
[13] *Id.*
[14] CIA Office of Security, "Response to HPSCI Staffer Meeting," (Nov. 18, 2014). Overall document classified S//NF; cited portion classified S//NF.
[15] *Id.*
[16] Laura Poitras and Glenn Greenwald, "NSA Whistleblower Edward Snowden: 'I Don't Want To Live in a Society that Does These Sorts of Things," *The Guardian* (Jun. 9, 2013), *available at* http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video (accessed May 2, 2016).
[17] CIA, Careers and Internships, "Telecommunications Information Systems Officer – Entry/Developmental," www.cia.gov (Oct. 2, 2015).
[18] *Id.*

unfairly targeted" by his supervisor.[19] After entering on duty, Snowden believed there were "morale and retention issues" among his fellow TISOs.[20] He raised those concerns with his training supervisor, the chief of the communications training unit, but "felt they were left unaddressed."[21] He next tried the chief and deputy chief of his operational group, but was similarly dissatisfied with their response.[22]

(U) Undeterred, Snowden spent the next week surveying the other TISOs who entered on duty at the same time as him.[23] He wrote up his findings and sent them to the CIA's Strategic Human Capital Office. Then, instead of attempting to raise his concerns again with his supervisor or work collaboratively with other TISOs to resolve the concerns, Snowden sent his concerns to the Deputy Director of CIA for Support—the head of the entire Directorate of Support and one of the ten most senior executives of CIA.[24]

(U) In his e-mail, Snowden complained about the process of assigning new TISOs to overseas locations, the pay of TISOs compared to contractors who performed similar work, and the difficulty for TISOs to transfer laterally to other jobs.[25]

~~(C)~~ Despite his lack of experience, the 23-year-old Snowden told the Deputy Director he felt "pretty disenfranchised" because his immediate supervisors did not take his unsolicited recommendations to heart.[26]

(U) Snowden told the IG that, after he contacted the Deputy Director for Support, his supervisors pulled him in to their offices for unscheduled counseling. In his view, they were "extremely hostile" and "seem[ed] to believe I have trouble bonding with my classmates."[27] Those counseling sessions prompted Snowden to contact the IG to help protect him from "reprisal for speaking truth to power."

(U) One day after receiving his complaint, an IG employee responded to Snowden and recommended he contact the CIA's Ombudsman, an official who could help Snowden sort through the options available to him and mediate disputes between managers and employees.[28] The IG employee also directed Snowden to the relevant Agency regulation regarding the factors managers could consider when deciding to retain an employee beyond the initial three-year trial period.[29] Whether that response satisfied Snowden is unclear; shortly after receiving it, Snowden sent another message to the IG employee instructing him to disregard the initial request because

[19] E-mail from Snowden to CIA Office of Inspector General (Nov. 2, 2006). Overall document classified S; cited portion marked U//AIUO.
[20] *Id.* Overall document classified S; cited portion not portion-marked.
[21] *Id.* Overall document classified S; cited portion not portion-marked.
[22] *Id.* Overall document classified S; cited portion not portion-marked.
[23] *Id.* Overall document classified S; cited portion not portion-marked.
[24] *Id.* Overall document classified S; cited portion not portion-marked.
[25] *Id.* Overall document classified S; cited portion not portion-marked.
[26] *Id.* Overall document classified S; cited portion classified C.
[27] *Id.* Overall document classified S; cited portion not portion-marked
[28] E-mail from CIA Office of Inspector General to Edward Snowden (Nov. 3, 2006). Overall document classified S; cited portion classified U//AIUO.
[29] *Id.* Overall document classified S; cited portion classified U//AIUO.

the issue had been "addressed."[30] During the rest of his time at CIA, Snowden did not contact the IG.

~~(S)~~ After the completion of his training, Snowden was assigned to [redacted] in March 2007 for his first TISO assignment.[31] Snowden was, in the words of his supervisor, "an energetic officer" with a "plethora" of experience on Microsoft operating systems, but he "often does not positively respond to advice from more senior officers, . . . does not recognize the chain of command, often demonstrates a lack of maturity, and does not appear to be embracing the CIA culture."[32]

~~(S)~~ A few months after starting in [redacted], Snowden asked to apply for a more senior position in [redacted] as a regional communications officer. His supervisor did not endorse his application. When he was not selected for the position, Snowden responded by starting "a controversial e-mail exchange with very senior officers" in which he questioned the selection board's professional judgment.[33] Years later, when characterizing his experience as a CIA TISO, Snowden would write that he was "specially selected by [CIA's] Executive Leadership Team for [a] high-visibility assignment" that "required exceptionally wide responsibility."[34] The description is in tension with his supervisor's account of a junior officer who "needed more experience before transitioning to such a demanding position."[35]

~~(S)~~ Snowden also modified CIA's performance review software in connection with his annual performance review, by manipulating the font. [36] This behavior led to Snowden's recall for "professional consultations" with the head of all CIA technical officers in Europe.[37] This was the first but not the only time more senior CIA officers attempted to correct Snowden's behavior. His supervisor in [redacted] cataloged six counseling sessions between October 2007 and April 2008, nearly one per month, regarding his behavior at work.[38] In September 2008, Snowden requested to leave [redacted] "short of tour," that is, before his scheduled rotation date to a new assignment.[39] The request was denied. Disobeying orders, Snowden traveled back to the Washington, D.C., area for his and his fiancée's medical appointments. Because of his disobedience, Snowden's supervisors recommended he not return to [redacted].[40]

[30] E-mail from Snowden to CIA Office of Inspector General (Nov. 3, 2006). Overall document classified S; cited portion classified U//AIUO.

[31] NSA, Edward Snowden Timeline (Sept. 30, 2014); overall document classified C//NF; cited portion classified C//NF.

[32] Memorandum for the Record by Senior Telecommunications Officer – Europe, "TISO [redacted]—Edward Snowden" (Sept. 4, 2008).

[33] CIA Office of Security, "Response to HPSCI Staffer Meeting," (Nov. 18, 2014).

[34] Edward Snowden Resume.

[35] Memorandum for the Record by Senior Telecommunications Officer – Europe, "TISO [redacted]—Edward Snowden" (Sept. 4, 2008). Overall document classified S//NF; cited portion classified S.

[36] *Id.* Overall document classified S//NF; cited portion classified S.

[37] *Id.* Overall document classified S//NF; cited portion classified S.

[38] Memorandum for the Record by Office in Charge, [redacted], "TISO [redacted]—Edward Snowden" (Dec. 18, 2008). Overall document classified S//NF; cited portion classified S.

[39] *Id.* Overall document classified S//NF; cited portion classified S.

[40] *Id.* Overall document classified S//NF; cited portion classified S.

~~(S//NF)~~ In January 2009, CIA submitted a "fitness for duty" report for Snowden, an administrative tool to determine whether Snowden had any work-related medical issues.[41] The Agency also assigned him to a position in the Washington, D.C., area so he could be available for any medical appointments.[42]

~~(S//NF)~~ Several years later, Snowden claimed that, while in [redacted], he had ethical qualms about working for CIA.[43] None of the memoranda for the record detailing his numerous counseling sessions mention Snowden expressing any concerns about [redacted]. Neither the CIA IG nor any other CIA intelligence oversight official or manager has a record of Snowden expressing any concerns about the legality or morality of CIA activities.

(U) Transition to NSA Contractor

~~(C//NF)~~ Around the same time that Snowden returned to the D.C. area, he applied for a position with an NSA contractor, Perot Systems, as a systems administrator. He was still a CIA employee at the time and his clearance remained in good standing with no derogatory information.[44] On March 25, 2009, Perot Systems sponsored Snowden for employment; six days later, on March 31, NSA Security checked the Intelligence Community-wide security database, "Scattered Castles," to verify Snowden's clearance.[45]

(U) Seeing no derogatory information in Scattered Castles, NSA Security approved Snowden for access eight days later, on April 7.[46]

~~(S//NF)~~ On April 16, Snowden formally resigned as a CIA employee.[47] CIA's Security Office updated his Scattered Castles record on April 20, [redacted].[48] Because NSA had checked the database three weeks earlier, NSA Security did not learn of the [redacted] in his record at that time.[49] It is unclear if NSA Security would have treated Snowden's onboarding any differently had NSA been aware of [redacted].

[41] CIA Office of Security, "Response to HPSCI Staffer Meeting," (Nov. 18, 2014). Overall document classified S//NF; cited portion classified S//NF.

[42] *Id.* Overall document classified S//NF; cited portion classified S//NF.

[43] [redacted]

[44] NSA, Edward Snowden Timeline (Sept. 30, 2014). Overall document classified C//NF; cited portion classified C//NF.

[45] *Id.* Overall document classified C//NF; cited portion classified U//FOUO.

[46] *Id.* Overall document classified C//NF; cited portion classified U//FOUO.

[47] *Id.* Overall document classified C//NF; cited portion classified C//NF.

[48] CIA Office of Security, "Response to HPSCI Staffer Meeting," (Nov. 18, 2014). Overall document classified S//NF.

[49] NSA, Edward Snowden Timeline (Sept. 30, 2014). Overall document classified C//NF; cited portion classified C//NF. The alerting function for [redacted] in Scattered Castles has since been fixed.

(U) From May 2009 to February 2012, Snowden worked in a variety of roles supporting IC contracts for Dell, which had purchased Perot Systems in 2009. He worked as an IT systems administrator at NSA sites in [redacted] for a little more than a year, where he supported NSA's Agency Extended Information Systems Services (AXISS) contracts.[50]

(U) One co-worker recalled that while he was working in [redacted], Snowden traveled to Thailand to learn how to be a ship's captain, but never finished the training course. According to another co-worker, at some point before he was stationed in [redacted], Snowden took a trip to China and spoke about his admiration for the Chinese people and Chinese martial arts.[51] The same co-worker remembered Snowden expressing his view that the U.S. government had overreached on surveillance and that it was illegitimate for the government to obtain data on individuals' personal computers.[52] There are no indications of how Snowden attempted to square this belief with his continued employment in support of the foreign signals intelligence mission of NSA.

(U) Other co-workers from Snowden's time in [redacted] recalled him as someone frustrated with his lack of access to information. One remembered Snowden complaining how he lacked access at CIA;[53] another recalled him attempting to gain access to information about the war in Iraq that was outside of his job responsibilities.[54] Although Snowden did not obtain the information he was looking for, he later claimed it was "typical" of the U.S. government to cover up embarrassing information.[55]

~~(C//NF)~~ In September 2010, Snowden returned to the United States and Dell attempted to move him to a position where he would support IT systems at CIA. Because of the [redacted] in Scattered Castles, however, CIA refused to grant Snowden access to its information.[56] Dell put Snowden on leave for three months while waiting for a position that did not require a security clearance to open up. Eventually, one did: In December 2010, Snowden started work in an uncleared "systems engineer/pre-sales technical role" for Dell supporting a CIA contract.[57]

(U) Snowden was also due for a periodic background reinvestigation in the fall of 2010. OPM contractor U.S. Information Services completed that review in May 2011, finding no derogatory information. According to an after-the-fact review by the National Counterintelligence Executive, the reinvestigation was "incomplete" and "did not present a complete picture of Mr. Snowden."[58] Among its other flaws, the investigation never attempted to verify Snowden's CIA employment or speak to his CIA supervisors, nor did it attempt to independently verify Snowden's self-report of a past security violation—areas where further

[50] *Id.* Overall document classified C//NF; cited portion classified U//FOUO.

[51] Interview with NSA Attorney (Feb. 8, 2016) (report of interview with [redacted]).

[52] *Id.* The same co-worker, [redacted], also mentioned that Snowden considered himself a privacy advocate.

[53] Interview with NSA Attorney (Feb. 8, 2016) (report of interview with [redacted]).

[54] *Id.* (report of interview with [redacted]).

[55] *Id.* (report of interview with [redacted]).

[56] NSA, Edward Snowden Timeline (Sept. 30, 2014). Overall document classified C//NF; cited portion classified C//NF.

[57] *Id.* Overall document classified C//NF; cited portion classified C//NF.

[58] National Counterintelligence Executive, Technical and quality review of the April 2011 Single Scope Background Investigation – Periodic Reinvestigation on Mr. Snowden," (Aug. 23, 2013); overall document classified U//FOUO.

information could have alerted NSA to CIA's concerns.[59] Contrary to best practices, the investigation also failed to develop any character references beyond the two people Snowden himself listed, his mother and his girlfriend. [60]

~~(S)~~ From August 31, 2011, to January 11, 2012, Snowden took a leave of absence from Dell. His Dell co-workers offered conflicting accounts of how he spent his leave,[61] [redacted]

(U) NSA Hawaii – Contract Systems Administrator

(U) Snowden returned from leave in early 2012 and took a position as a general systems administrator supporting Dell's AXISS work at NSA's Hawaii Cryptologic Center.[62] As part of the change in station, he took a counterintelligence polygraph examination. The first exam was "inconclusive," but did not lead to NSA Security developing any further information; the second was successful.[63] At the end of March 2012, Snowden moved to Hawaii.

(U) The job Snowden performed in Hawaii was similar to his duties during the previous three years with Dell. He was a field systems administrator, working in technical support office of NSA Hawaii. Some of his work involved moving large numbers of files between different internal Microsoft SharePoint servers for use by other NSA Hawaii employees. Although most NSA Hawaii staff had moved to a new building at the start of 2012, Snowden and other technical support workers remained in the Kunia "tunnel," an underground facility originally built for aircraft assembly during World War Two.

(U) Snowden had few friends among his co-workers at NSA Hawaii.[64] Those co-workers described him as "smart" and "nerdy," but also someone who was "arrogant," "introverted," and "squirrelly"; an "introvert" who frequently "jumped to conclusions."[65] His supervisors found his work product to be "adequate," but he was chronically late for work, frequently not showing up until the afternoon.[66] Snowden claimed he had trouble waking up on time because he stayed up late playing video games.[67]

(U) Few of Snowden's Hawaii co-workers recall him expressing political opinions. One remembered a conversation in which Snowden claimed the Stop Online Piracy Act and the

[59] *Id.*
[60] *Id.*
[61] Interview with NSA Attorney (Feb. 8, 2016).
[62] NSA, Edward Snowden Timeline (Sept. 30, 2014). Dell Federal was a subcontractor to CACI International for NSA's AXISS Field IT support contracts. E-mail from NSA Legislative Affairs to HPSCI Staff, "Responses to Your Questions on Read and Return Documents for HPSCI Media Leaks Review," (Dec. 2, 2014, at 3:47 PM). Overall document cited U//FOUO; cited portion classified U//FOUO.
[63] *Id.*
[64] Interview with NSA Security Official (Jan. 28, 2016).
[65] Interview with NSA Attorney (Jan. 28, 2016).
[66] *Id.*
[67] *Id.*

Protect Intellectual Property Act would lead to online censorship.[68] In the same conversation, Snowden told his colleague that he had not read either bill.[69] The same co-worker recalled Snowden once claiming that, based on his meetings with Chinese hackers at a conference, the United States caused problems for China but China never caused problems for the United States.[70] Although no other co-worker in Hawaii recalled Snowden expressing any sympathy for foreign governments, a different co-worker from the Kunia tunnel remembered that Snowden defended the actions of Private Bradley Manning.[71]

(U) One incident early in Snowden's time at NSA Hawaii merits further description. In June 2012, Snowden installed a patch to a group of servers on classified networks that supported NSA field sites, including NSA Hawaii. Although the patch was intended to fix a vulnerability to the classified servers, the patch caused the servers to crash, resulting in a loss of network access for several NSA sites.[72] One of NSA's senior technical support managers, a government employee, fired off an e-mail to a number of systems administrators, asking who had installed the troublesome patch and sarcastically chiding that individual for failing to test the patch before loading it.[73]

(U) Snowden replied to all the recipients and added the deputy head of NSA's technical services directorate to the e-mail thread. This individual was several levels above the immediate government supervisors whom Snowden could have contacted first. Calling the initial e-mail "not appropriate and . . . not helpful," Snowden accused the middle manager of focusing on "evasion and finger-pointing rather than problem resolution."[74]

(U) Snowden received a quick rebuke. The NSA civilian employee in Washington responsible for managing field AXISS contracts sent Snowden an e-mail telling him his response was "totally UNACCEPTABLE" because "[u]nder no circumstances will any contractor call out or point fingers at any government manager whether you agree with their handling of an issue or not."[75] She further instructed Snowden that if he "felt the need to discuss with any management it should have been done with the site management you are working with and no one else."[76]

~~(S)~~ That weekend, Snowden came in to work [redacted][77]

[68] Interview with NSA Attorney (Jan. 28, 2016) (citing co-worker [redacted]).
[69] *Id.* (citing co-worker [redacted])
[70] *Id.* (citing co-worker [redacted])
[71] *Id.*; Interview with NSA Attorney (Feb. 8, 2016) (citing co-worker [redacted]).
[72] Interview with [redacted] (Oct. 28, 2015).
[73] E-mail from [redacted], "RE: (U) ICA-tcp issues with KB2653956," (Jun. 21, 2012, at 1:20AM). Overall document classified U//FOUO.
[74] E-mail from Edward Snowden, "RE: (U) ICA-tcp issues with KB2653956," (Jun. 21, 2012, at 1:00PM). Overall document classified U//FOUO.
[75] E-mail from [redacted], "(U) E-mail you sent in response to ICA-tcp issues with a patch," (Jun. 22, 2012, at 3:26AM). Overall document classified U//FOUO.
[76] *Id.*
[77] Interview with NSA Security Official (Jan. 28, 2016).

(U) The following Monday, he sent an e-mail to the NSA middle manager saying he "understood how bad this e-mail looked for what was intended to be a relatively benign message" and acknowledging that the e-mail "never should have happened in the first place."[78] The manager accepted the apology, explaining that his problem with the message "had nothing to do with the content but with distribution" because he did not understand "the elevation of the issue to such a high management level"; that is, to the deputy head of NSA's technical services directorate.[79]

(U) Snowden would later publicly claim that his "breaking point"—the final impetus for his unauthorized downloads and disclosures of troves of classified material—was March 2013 congressional testimony by Director of National Intelligence James Clapper.[80]

~~(S//REL TO USA, FVEY)~~ But only a few weeks after his conflict with NSA managers, on July 12, 2012—eight months before Director Clapper's testimony—Snowden began the unauthorized, mass downloading of information from NSA networks.[81] [redacted] [82] [redacted] [83]

(U) Snowden's Downloading and Removal Process

(U) Snowden used several methods to gather information on NSA networks, none of which required advanced computer skills.

(U) At first, Snowden used blunt tools to download files en masse from NSA networks. Two non-interactive downloading tools, commonly known as "scraping" tools, called "wget" and DownThemAll! were available on NSA classified networks for legitimate system administrator purposes.[84] Both tools were designed to allow users to download large numbers of files over slow or unstable network connections.[85] Snowden used the two tools with a list of website addresses, sometimes writing simple programming scripts to generate the lists. For

[78] E-mail from Edward Snowden, "RE: (U) ICA-tcp issues with KB2653956" (Jun. 25, 2012, at 2:31AM). Overall document classified U//FOUO.

[79] E-mail from [redacted], "RE: (U) ICA-tcp issues with KB2653956" (Jun. 25, 2012, at 1:51AM). Overall document classified U//FOUO.

[80] "Transcript: ARD Interview with Edward Snowden," (Jan. 26, 2014), *available at* https://edwardsnowden.com/2014/01/27/video-and-interview-with-edward-snowden.

[81] NSA, Edward Snowden Timeline (Sept. 30, 2014). Overall document classified C//NF; cited portion classified C//REL TO USA, FVEY.

[82] NSA, "Methods Used by Edward Snowden To Remove Documents from NSA Networks," (Oct. 29, 2014). Overall document classified S//REL TO USA, FVEY; cited portion classified S//REL.

[83] [redacted]

[84] NSA, "Methods Used by Edward Snowden To Remove Documents from NSA Networks," (Oct. 29, 2014). Overall document classified S//REL TO USA, FVEY; cited portion classified U//FOUO

[85] *Id.* Overall document classified S//REL TO USA, FVEY; cited portion classified U//FOUO

instance, if NSA webpages were set up in numerical order (i.e., page 1, page 2, page 3, and so on), Snowden programmed a script to automatically collect the pages.[86] Neither scraping tool targeted areas of potential privacy or civil liberties concerns; rather, Snowden downloaded *all* information from internal NSA networks and classified webpages of other IC elements.[87]

~~(S//NF)~~ [redacted].[88]

~~(S//REL)~~ [redacted].[89] [redacted].[90]

(U) Exceeding the access required to do his job, Snowden next began using his systems administrator privileges to search across other NSA employees' personal network drives and copy what he found on their drives.[91] Snowden also enlisted his unwitting colleagues to help him, asking several of his co-workers for their security credentials so he could obtain information that they could access, but he could not.[92] One of these co-workers subsequently lost his security clearance and resigned from NSA employment.[93]

~~(S//REL)~~ Snowden infringed the privacy of at least [redacted] NSA personnel by searching their network drives without their permission, removing a copy of any documents he found to be of interest.[94] [redacted][95] [redacted][96]

[86] *Id.* Overall document classified S//REL TO USA, FVEY; cited portion classified U//FOUO
[87] *Id.* Overall document classified S//REL TO USA, FVEY; cited portion classified U//FOUO
[88] NSA, "HPSCI Recollection Summary Paper," (Jan. 26, 2015). Overall document classified S//NF; cited portion classified S//NF. *See infra* for a more detailed description of the files Snowden removed.
[89] NSA, "Methods Used by Edward Snowden To Remove Documents from NSA Networks," (Oct. 29, 2014). Overall document classified S//REL TO USA, FVEY; cited portion classified S//REL TO USA, FVEY.
[90] Interview with NSA Security Official (Jan. 28, 2016). [redacted]
[91] NSA, "Methods Used by Edward Snowden To Remove Documents from NSA Networks," (Oct. 29, 2014). Overall document classified S//REL TO USA, FVEY; cited portion classified U//FOUO.
[92] HPSCI Memorandum for the Record, NSA Briefing to HPSCI Staff (July 22, 2013).
[93] NSA Legislative Affairs Memorandum to Staff Director and Minority Staff Director (Feb. 10, 2014). Overall document classified U; document not portion-marked.
[94] Interview with NSA Security Official (Jan. 28, 2016); NSA, "Number of Personal Network Drives Searched," (Mar. 14, 2016). Overall document classified S//REL TO USA, FVEY; cited portion classified S//REL TO USA, FVEY.
[95] Interview with NSA Security Official (Jan. 28, 2016).
[96] *Id.*

(U) Snowden's searches quickly expanded beyond surveillance programs. Some of the personal network drives Snowden searched belonged to individuals involved in the hiring decision for a job for which Snowden had applied. On these individuals' network drives, Snowden searched for human resources files and files related to the promotion and hiring decisions.[97]

~~(S//REL)~~ Snowden first saved the information he gathered on his personal network drive.[98] At some point in 2012, a fellow systems administrator noticed that Snowden's personal drive used a significantly larger amount of memory than most other employees and asked him what he was doing.[99] Snowden responded that he was downloading system patches for NSA networks, a task that was consistent with his job responsibilities.[100] [redacted][101]

(U) In late August 2012, Snowden requested a "thin-on-thick" machine for his desk.[102] At the time, NSA Hawaii was in the middle of a transition from "thick clients,"—physical desktop computers at each worker's desk, to "thin clients,"—virtual desktops hosted on servers. On a "thin client," there is no traditional desktop computer at workers' desks, rather, each user has a client that provides a display and input, with computing processors, memory, and storage on network servers. Snowden's "thin-on-thick" setup meant that he had a physical desktop computer at his desk, but he only used its computing power and hard drive to operate a virtual computer. This "thin-on-thick" setup allowed NSA Hawaii to reap some of the benefits of thin clients, such as uniform security policies and improved information sharing, without the cost of buying new thin client devices. NSA Hawaii could also make use of a large quantity of "thick client" desktop computers it had recently purchased.[103] Yet the thin-on-thick setup opened up a loophole for Snowden to exploit.

~~(S//NF)~~ Snowden knew NSA's networks recorded and logged every action by users on thick client workstations while connected to the network.[104] He also knew that auditing controls

[97] NSA, "Number of Personal Network Drives Searched," (Mar. 14, 2016). Overall document classified S//REL TO USA, FVEY; cited portion classified S//REL TO USA, FVEY.
[98] NSA, "Methods Used by Edward Snowden To Remove Documents from NSA Networks," (Oct. 29, 2014). Overall document classified S//REL TO USA, FVEY; cited portion classified S//REL TO USA, FVEY.
[99] Interview with NSA Attorney (Jan. 28, 2016).
[100] *Id.*
[101] NSA, "Methods Used by Edward Snowden To Remove Documents from NSA Networks," (Oct. 29, 2014). Overall document classified S//REL TO USA, FVEY; cited portion classified S//REL TO USA, FVEY.
[102] NSA Response to HPSCI Question on Thin-on-Thick Computer at Snowden's Workstation (Mar. 2, 2016). Overall document classified S//NF; cited portion classified S//NF. Because thin-on-thick workstations were prevalent at NSA Hawaii at the time, Snowden did not have to go through any special approval process to obtain a thin-on-thick workstation.
[103] Interview with NSA Security Official (Jan. 28, 2016).
[104] NSA, "Response to HPSCI Document Request – Question # 10" (May 1, 2015). Overall document classified S//NF; cited portion classified S//NF. [redacted]

would send an alert to network security personnel if he tried to remove data from the network. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted][106]

~~(S//REL)~~ [redacted][108]

~~(S//REL)~~ There is no evidence that NSA was aware of this specific vulnerability to its networks. Because Snowden's legitimate work responsibilities involved transferring large amounts of data between different SharePoint servers, the large quantities of data he copied as Step 1 of the exfiltration process did not trigger any NSA alerts for abnormal network traffic.[109]

[105] NSA, "Purpose of Functioning CD-ROM and USB Drive," (Mar. 14, 2016). Overall document classified S//REL USA, FVEY; cited portion classified S//REL USA, FVEY.

[106] NSA, "Methods Used by Edward Snowden To Remove Documents from NSA Networks," (Oct. 29, 2014). Overall document classified S//REL TO USA, FVEY; cited portion classified S//REL TO USA, FVEY. *See also id.* for additional details on the NSA forensics process that allowed for the reconstruction of Snowden's methods.

[107] [redacted]

[108] Interview with NSA Security Official (Jan. 28, 2016).

[109] NSA, "Response to HPSCI Document Request – Question # 10" (May 1, 2015). Overall document classified S//REL USA, FVEY; cited portion classified S//REL USA, FVEY. Although Snowden, as a systems administrator, was authorized to transfer large quantities of data on the NSA network, he was *not* authorized to remove data from the network for his intended purpose of later transferring it to removable media so he could disclose it.

[redacted][110]

(U) NSA Hawaii – Gaining More Access and Departing for China and Russia

(U) After he began removing documents in the summer of 2012, Snowden spent several months applying for employment as a NSA civilian. In September 2012, he took a test to obtain a position in the Tailored Access Operations office, or TAO, the group within NSA responsible for computer network exploitation operations. After finding the test and its answers among the documents he had taken off of NSA networks, he passed the test.[111] Based on the test result and his exaggerated resume,[112] TAO offered him a position. The pay grade TAO offered, however—a GS-12 position that would have paid around $70,000 per year—was not sufficient for Snowden. He instead believed he should have been offered a GS-15 position that would have paid nearly $120,000 per year.[113]

~~(C)~~ [redacted][114]

(U) In early December 2012, Snowden attempted to contact journalist Glenn Greenwald. To hide his identity, Snowden used the pseudonym "Cincinnatus" and asked Greenwald for his public encryption key so Snowden could send him documents securely.[115] In January 2013, he contacted filmmaker Laura Poitras.[116]

(U) In late March 2013, Snowden finally obtained a new position, not with NSA as a civilian but with Booz Allen Hamilton as a contractor.[117] He would be a SIGINT Development Analyst, meaning he analyzed foreign networks and cyber operators to help NSA's National Threat Operation Center (NTOC) in its cyber defense efforts. NTOC's operations helped defend U.S. military networks from attacks by foreign cyber actors, including Russia and China.

[110] NSA, "Purpose of Functioning CD-ROM and USB Drive," (Mar. 14, 2016).

[111] Bryan Burrough, Sarah Ellison, and Suzanna Andrews, "The Snowden Saga: A Shadowland of Secrets and Light," *Vanity Fair* (May 2014), *available at* www.vanityfair.com/news/politics/2014/05/edward-snowden-politics-interview (quoting NSA Deputy Director Rick Ledgett).

[112] Edward Snowden Resume (June 28, 2012). Snowden described himself as a "Senior Advisor" at "Dell/NSA/CIA/DIA" rather than as a systems administrator. Resume inflation was a habit for Snowden—in the files he sent to Glenn Greenwald, he described himself as an NSA Special Advisor "under corporate cover" and as a former CIA "field officer." *See* Glenn Greenwald, No Place to Hide at 32.

[113] Interview with NSA Security Official (Jan. 28, 2016).

[114] NSA, Edward Snowden Timeline (Sept. 30, 2014).

[115] Glenn Greenwald, No Place to Hide at 7 (2014).

[116] NSA, Edward Snowden Timeline (Sept. 30, 2014).

[117] NSA, Edward Snowden Timeline (Sept. 30, 2014).

~~(C//NF)~~ In his new position, Snowden had access to more documents on NSA networks, many of which he later removed.[118] Because there was not a thin-on-thick workstation at Snowden's new desk, he had to return after hours to his old desk—located at a different NSA facility a twenty-minute drive away—to exfiltrate documents [redacted].[119] His NTOC job did not require him to visit his old building, so he had no reason other than document removal to return.[120]

(U) On May 15, 2013, Snowden told his Booz Allen Hamilton supervisor that he needed to take two weeks of leave without pay to return to the continental United States for medical reasons.[121] According to his supervisor, Snowden had previously claimed he suffered from epilepsy,[122] although he never presented evidence of a diagnosis from any doctor.[123] Four days later, Snowden flew to Hong Kong without telling either his girlfriend or his mother (who was in Hawaii at the time visiting him) where he was going.[124] The Committee found no conclusive evidence indicating why Snowden chose Hong Kong as his destination, but, according to later accounts, Snowden believed he would be safe in the city based on its tradition of free speech.[125]

(U) On Friday May 31, Snowden's leave without pay ended. The following Monday, June 3, Booz Allen Hamilton started looking for him.[126] Two days later, on June 5, Booz Allen reported Snowden to NSA's Office of Security and Greenwald published the first of Snowden's disclosures.[127]

(U) Four days after the first Greenwald articles were published, Snowden revealed himself as the source of the disclosures.[128] According to press reports, between June 10 and June 23, Snowden hid in the apartments of refugees in Hong Kong while his lawyer worked to arrange transit for him out of the city.[129] On June 23, 2013, he flew from Hong Kong to Moscow's Sheremetyvevo airport, accompanied by Wikileaks activist Sarah Harrison.[130] The next day, he failed to appear on a flight to Havana and disappeared from public view until August 1, 2013, when Russia granted him asylum and he left the airport.[131] As of September 15, 2016, Snowden remains in Russia.

[118] Interview with NSA Security Official (Jan. 28, 2016).
[119] NSA, "Response to HPSCI Document Request – Question #2" (June 24, 2015). Overall document classified S//NF; cited portion classified C//REL.
[120] *Id.* Cited portion classified C//REL.
[121] NSA, Edward Snowden Timeline (Sept. 30, 2014).
[122] Interview with NSA Attorney (Jan. 28, 2016) (citing BAH supervisor).
[123] Interview with NSA Security Official (Jan. 28, 2016).
[124] NSA, Edward Snowden Timeline (Sept. 30, 2014); Interview with NSA Security Official (Jan. 28, 2016).
[125] *See* Luke Harding, The Snowden Files (2014) at 108.
[126] NSA, Edward Snowden Timeline (Sept. 30, 2014).
[127] Glenn Greenwald, "Verizon Order: NSA Collecting Phone Records of Millions of Americans Daily," *The Guardian* (June 5, 2013).
[128] *See* Luke Harding, The Snowden Files (2014) at 146-52.
[129] Theresa Tedesco, "How Snowden Escaped," *National Post* (Sept. 6, 2016), *available at* http://news.nationalpost.com/features/how-edward-snowden-escaped-hong-kong/
[130] Luke Harding, The Snowden Files (2014) at 224.
[131] *Id.* at 229-30, 250.

~~(S//NF)~~ [redacted].[132] Additionally, although Snowden's objective may have been to inform the public, the information he released is also available to Russian, Chinese, Iranian, and North Korean intelligence services; any terrorist with Internet access; and many others who wish to do harm to the United States.

~~(S//NF)~~ When he fled Hong Kong, Snowden left a number of encrypted computer hard drives behind. [redacted][133]

(U) Communications with Intelligence Oversight Personnel

(U) In March 2014 public testimony to the European Parliament, Snowden claimed that he reported his concerns about "clearly problematic programs to more than ten distinct officials" at NSA.[134] Snowden also publicly stated that he "specifically expressed concern about [NSA's] suspect interpretation of the law," inviting "members of Congress to request a written answer to this question [from the NSA]."[135] The Committee requested such an answer from NSA,[136] and found no evidence to support these claims. The Committee further found no evidence that Snowden attempted to communicate concerns about the legality or morality of intelligence activities to any officials, senior or otherwise, during his time at either CIA or NSA.

(U) As already described, one of Snowden's Hawaii co-workers recalls him defending Bradley Manning's actions,[137] another remembered him criticizing bills under consideration in Congress that he regarded as harmful to online privacy[138] and criticizing U.S. foreign policy toward China.[139] None of his co-workers or his supervisors, however, recall Snowden raising concerns about the legality or morality of U.S. intelligence activities.[140]

[132] DIA, Information Review Task Force-2, "Initial Assessment" (Dec. 26, 2013), at 3. Overall document classified TS//SI//RSEN/OC/NF; cited portion classified S//NF.
[133] HPSCI Memorandum for the Record, Insider Threat/Counterintelligence Monthly Briefing (Feb. 4, 2014).
[134] Edward Snowden, Testimony to the European Parliament (Mar. 7, 2014) at 6.
[135] Bryan Burrough, Sarah Ellison, and Suzanna Andrews, "The Snowden Saga: A Shadowland of Secrets and Light," *Vanity Fair* (May 2014), *available at* www.vanityfair.com/news/politics/2014/05/edward-snowden-politics-interview.
[136] Letter from HPSCI Chairman Mike Rogers to Director James Clapper (Aug. 5, 2014) (requesting, among other things, "[a]ll communications between Edward Snowden and any IC or Department of Defense compliance, legal, or Inspector General personnel").
[137] *See supra*, note 71.
[138] *See supra*, note 68.
[139] *See supra*, note 70.
[140] Interview with NSA Attorney (Jan. 28, 2016) (citing supervisors, co-workers). The co-worker who recalled Snowden defending Manning expressly mentioned that Snowden did not believe Americans' privacy rights were being violated and that Snowden had no qualms about the legality of the NSA mission. *See* Interview with NSA Attorney (Feb. 8, 2016) (citing co-worker [redacted]).

(U) Neither did Snowden raise any concerns with IC oversight personnel. As previously discussed, Snowden contacted the CIA IG within a few months of his start at the Agency to complain about training issues and management style, but he later dropped the complaint.[141] He did not contact the NSA IG, the Department of Defense (DOD) IG, or the Intelligence Community (IC) IG, all of whom could have responded to a complaint regarding unlawful intelligence activities. Nor did Snowden attempt to contact the Committee or the Senate Select Committee on Intelligence through the procedures available to him under the Intelligence Community Whistleblower Protection Act (IC WPA). He could have done this anonymously if he feared retribution.

(U) Snowden did, however, contact NSA personnel who worked in an internal oversight office about his personal difficulty understanding the safeguards against unlawful intelligence activities. While on a trip to NSA headquarters at Ft. Meade in June 2012, Snowden visited a training officer in the internal oversight and compliance office of the Signals Intelligence Directorate. The training officer remembered that Snowden was upset because he had failed NSA's internal training course on how to handle information collected under FISA Section 702, the legal authority by which the government can target the communications of non-U.S. persons outside the United States.[142]

(U) The internal training is a rigorous computer-based course that walks NSA employees and contractors through the laws and regulations that govern the proper handling of information collected under the authority of FISA Section 702, including information collected under the programs Snowden would later disclose, PRISM and "upstream" collection. At the end of the course, NSA personnel take a scenario-based test to gauge their comprehension of the material; if they do not receive a minimum score on the test, they must retake the computer-based training course. All of the answers to the test questions can be found within the training material. After three failures of the computer-based course, the individual must attend an in-person training course to ensure they are able to understand the rules governing Section 702, including privacy protections.

(U) According to the training officer, Snowden had failed the computer-based training course and was afraid of the consequences.[143] He was also upset because he believed the course was rigged.[144] After the training officer explained to Snowden that he could take the course again—and that careful reading would allow him to find all of the answers to the test—Snowden became calm and left the oversight and compliance office.[145] At no point during his visit to the compliance office did Snowden raise any concerns about how NSA used Section 702, PRISM, or "upstream" collection.[146]

[141] *See supra*, notes 19 through 30.
[142] NSA, "OVSC1203 Issue Regarding Course Content and Trick Questions," overall document classified TS//NF; cited portion classified U//FOUO.
[143] Interview with [redacted] (Oct. 28, 2015).
[144] *Id*
[145] *Id.*
[146] *Id.*

(U) In April 2013—after he had removed documents multiple times from NSA systems—Snowden contacted the NSA Office of General Counsel with a question about a different training course.[147] He was curious about the mandatory training on United States Signals Intelligence Directive 18, which is the foundational authority for NSA's collection activities overseas targeting foreigners.[148] Specifically, he believed the training erroneously accorded the same precedence to statutes and executive orders. A few days later, an NSA attorney clarified that while executive orders have the force of law, they cannot trump a statute.[149] Snowden did not respond to that e-mail; he also did not raise any concerns about the legality or morality of U.S. intelligence activities.[150]

(U) Was Snowden a Whistleblower?

(U) As a legal matter, during his time with NSA, Edward Snowden did not use whistleblower procedures under either law or regulation to raise his objections to U.S. intelligence activities, and thus, is not considered a whistleblower under current law. He did not file a complaint with the DOD or IC IG's office, for example, or contact the intelligence committees with concerns about fraud, waste, abuse, mismanagement, or violations of law. Instead, Snowden disclosed classified information to the press.

(U) Snowden, however, has argued that even a lawful disclosure would have resulted in retaliation against him.

(U) Among other things, Snowden has argued that he was unable to raise concerns about NSA programs because he was not entitled to protection as an IC whistleblower given his status as a contractor. (He was with Booz Allen at the time of his leaks to the press.) But the 1998 IC WPA applies to IC employees as well as contractors. Although the statute does not explicitly prohibit reprisals, the IC WPA channel nevertheless enables confidential, classified disclosures and oversight, as well as a measure of informal source protection by Congress. The statute specifically authorizes *IC contractors* to inform the intelligence committees of adverse actions taken as a consequence of IC WPA-covered disclosures.

(U) Moreover, explicit protection against such actions was conferred on Snowden by DoD regulation 5240 1-R. Snowden's unauthorized disclosures involved Executive Order (EO) 12333 activities as well as activities conducted under FISA. At least with respect to intelligence activities authorized under E.O. 12333—and, according to the DoD Senior Intelligence Oversight Official, activities conducted under other authorities—5240 1-R *requires* employees and contractors of a DoD intelligence element to report "questionable activities," or "conduct that constitutes, or is related to, [an] intelligence activity *that may violate the law, any Executive*

[147] E-mail from Edward Snowden to NSA Office of General Counsel (Apr. 5, 2013, at 4:11PM), overall document classified U//FOUO; cited portion classified U//FOUO.
[148] *Id.*, cited portion classified U//FOUO.
[149] E-mail from NSA Office of General Counsel Attorney to Edward Snowden (Apr. 8, 2013, at 1:37PM), overall document classified U//FOUO; cited portion classified U//FOUO.
[150] IC on the Record, "Edward J. Snowden email inquiry to the NSA Office of General Counsel," (May 29, 2014) ("There was not additional follow-up noted.").

Order or Presidential directive ... or applicable DoD policy[.]"[151] 5240 1-R also says that DoD senior leaders shall "ensure that *no adverse action is taken against any employee* [or contractor] because the employee reports [questionable activities]" pursuant to the regulation.[152] The IC IG's Executive Director for Intelligence Community Whistleblowing & Source Protection (ICW&SP), a former employee of the DoD IG's staff, has advised HPSCI staff that these procedures applied to Snowden during his employment as an NSA contractor and would have helped to shield him from retaliation for voicing his objections internally.

(U) Finally, Snowden also likely was covered by 10 U.S.C. § 2409 (Section 2409). As written at the time of Snowden's leaks,[153] Section 2409 was primarily focused on protecting DoD contractors from reprisals if they properly disclosed a "violation of law related" to a DoD contract. However, Snowden has not advanced any contract-related claims about NSA surveillance. Rather, he generally disagreed with NSA surveillance programs on policy and constitutional grounds.

(U) If Snowden did have concerns with programs related to a DoD contract, then the prior version of Section 2409 authorized him to raise those concerns without fear of retaliation with a "Member of Congress, a representative of a Committee of Congress, an Inspector General, the Government Accountability Office, a Department of Defense employee responsible for contract oversight or management, or an authorized official of an agency or the Department of Justice[.]"

(U) Foreign Influence

[redacted],[154] [redacted].[155]

[redacted][156]

[151] Department of Defense Regulation 5240 1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect U.S. Persons,* C.15.2.1, 3.1.1 (Dec. 7, 1982) (emphasis added).

[152] *Id.* at C.14.2.3.2.

[153] Important amendments to Section 2409, which took effect in July 2013, substantially altered the statute. Among other things, the updates extended reprisal protections to DoD subcontractors as well as contractors, and widened the list of persons to whom contractors and subcontractors could make disclosures. At the same time, the amendments also narrowed Section 2409's coverage by explicitly excluding employees and contractors of IC elements. However, that limitation, like other alterations to Section 2409, did not take effect until July 2013—*after* Snowden had unlawfully disclosed NSA material to journalists.

[154] *See, e.g.*, Testimony of Gen. Keith Alexander at 30, HPSCI Hearing (Jun. 13, 2013) ("It is not clear to us if there is a foreign nexus. There [are] some things; it does look odd that someone would go to Hong Kong to do this.")

[155] [redacted]

[156] [redacted]

[redacted].[157] [redacted].[158] [redacted][159]

~~(TS//HCS/OC/NF)~~ Since Snowden's arrival in Moscow, he has had, and continues to have, contact with Russian intelligence services. [redacted],[160] and in June 2016, the deputy chairman of the Russian parliament's defense and security committee asserted that "Snowden did share intelligence" with his government.[161] [redacted][162]

(U) What Did Snowden Take?

~~(S//NF)~~ [redacted].[163] In light of the volume at stake, it is likely that even Snowden does not know the full contents of all 1.5 million documents he removed.

(U) One thing that is clear, however, is that the IC documents disclosed in public are merely the tip of the iceberg.

~~(S//NF)~~ As of August 19, 2016, press outlets had published or referenced [redacted] taken by Snowden.[164] This represents less than one-tenth of one percent of the nearly 1.5 million documents the IC assesses Snowden removed. [165]

[157] [redacted]

[158] [redacted]

[159] [redacted]

[160] *Id.* Cited material classified S//OC//NF.

[161] Mary Louise Kelly, "During Tenure in Russia, Edward Snowden Has Kept A Low Profile," *National Public Radio* (June 29, 2016), *available at* http://www.npr.org/2016/06/29/483890378/during-tenure-in-russia-edward-snowden-has-kept-a-low-profile.

[162] [redacted].

[163] *See* NSA, "HPSCI Recollection Summary Paper," (Jan. 26, 2015) [redacted] Overall document classified S//NF; cited portion classified S//NF.

[164] E-mail from NSA Legislative Affairs (Aug. 22, 2016, at 4:48PM). Overall document classified S//REL TO USA, FVY; cited portion classified S//REL TO USA, FVEY.

(U) The 1.5 million documents came from two classified networks, an internal NSA network called NSANet and an IC-wide Top Secret/Sensitive Compartmented Information network called the Joint Warfighter Information Computer System (JWICS). If printed out and stacked, these documents would create a pile more than three miles high.[166]

~~(S//NF)~~ [redacted].[167] [redacted].[168] [redacted].[169] [redacted].[170]

~~(S//NF)~~ [redacted][171] [redacted].[172] [redacted][173] [redacted].[174]

[165] NSA, "HPSCI Recollection Summary Paper," (Jan. 26, 2015) Overall document classified S//NF; cited portion classified S//NF.

[166] Testimony of Mr. Scott Liard, Deputy Director for Counterintelligence, Defense Intelligence Agency, HPSCI Hearing (Jan. 27, 2014), at 7-8. The 1.5 million document count does not include 374,000 blank documents Snowden downloaded from the Department of the Army Intelligence Information Service (DAIIS) Message Processing System. *See* DIA, Information Review Task Force-2, "Fourth Quarter Report, 2014" (Dec. 31, 2014), at xvii.

[167] NSA, "HPSCI Recollection Summary Paper," (Jan. 26, 2015). Overall document classified S//NF; cited portion classified S//NF.

[168] NSA, "Timing of Recollection and Security Flags," (Mar. 14, 2016). Overall document classified S//REL TO USA, FVEY; cited portion classified S//REL.

[169] *Id.*

[170] *Id.*

[171] NSA, "HPSCI Recollection Summary Paper," (Jan. 26, 2015).

[172] *Id.*; *see also* DIA, Information Review Task Force-2, "Fourth Quarter Report, 2014" (Dec. 31, 2014), at xvii.

[173] *Id.*; *see also* DIA, Information Review Task Force-2, "Fourth Quarter Report, 2014" (Dec. 31, 2014), at xvii.

[174] *Id.*; *see also* DIA, Information Review Task Force-2, "Fourth Quarter Report, 2014" (Dec. 31, 2014), at xvii.

~~(S)~~ The vast majority of the documents Snowden removed were unrelated to electronic surveillance or any issues associated with privacy and civil liberties. [redacted][175] [redacted]

(U) What Damage Did Snowden Cause?

~~(S//NF)~~ Over the past three years, the Intelligence Community and the Department of Defense (DoD) have carried out separate reviews—with differing methodologies—of the contents of all 1.5 million documents Snowden removed. It is not clear which of the documents Snowden removed are in the hands of a foreign government. All of the documents that have been publicly disclosed—[redacted][176]—can be accessed by foreign militaries and intelligence services as well as the public. [redacted][177] [redacted][178] [redacted].

(U) Out of an abundance of caution, DoD therefore reviewed all 1.5 million documents to determine the maximum extent of the possible damage.

~~(TS//NF)~~ As of June 2016, the most recent DoD review identified 13 high-risk issues, which are identified in the following table.[179] Eight of the 13 relate to [redacted] capabilities of DoD; if the Russian or Chinese governments have access to this information, American troops will be at greater risk in any future conflict.[180]

[175] [redacted]

[176] E-mail from NSA Legislative Affairs (Aug. 22, 2016, at 4:48PM). Overall document classified S//REL TO USA, FVY; cited portion classified S//REL TO USA, FVEY.

[177] DIA, Information Review Task Force-2, "Initial Assessment" (Dec. 26, 2013), at 3. Overall document classified TS//SI//RSEN/OC/NF; cited portion classified S//NF.

[178] Mary Louise Kelly, "During Tenure in Russia, Edward Snowden Has Kept A Low Profile," *National Public Radio* (June 29, 2016), *available at* http://www.npr.org/2016/06/29/483890378/during-tenure-in-russia-edward-snowden-has-kept-a-low-profile.

[179] DoD, Mitigation Oversight Task Force, "Quarterly Report" (Oct. 2015), at 8. Overall document classified TS//SI/TK//ORCON/NF; cited portion classified TS//NF

[180] *Id.*

[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]

(U) The Intelligence Community, by contrast, has carried out a damage assessment for only a small subset of the documents Snowden removed. And unlike IC damage assessments for previous unauthorized disclosures,[181] the IC assessment on Snowden does not contain an assessment of Snowden's background and motive, an assessment of whether he was the agent of a foreign intelligence service, or recommendations for how to improve security in the IC. In its review, the National Counterintelligence and Security Center (NCSC), a component of the Office of the Director of National Intelligence, divided the documents Snowden removed into three "tiers."[182]

[181] *See, e.g.*, Office of the National Counterintelligence Executive, "Ana Belen Montes: A Damage Assessment," (July 1, 2004). Overall document classified S//NF.

[182] NCSC, "Intelligence Community Damage Assessment: Unauthorized Disclosures of Classified Information Attributed to Edward Snowden, 1 January 2015 through 31 August 2015," (Apr. 8, 2016), at 5. Overall document classified TS//HCS-P/SI-G/TK//OC/NF; cited portion classified U//FOUO.

~~(S//REL)~~ **Tier One:** Documents that have been disclosed in the media, either in whole or in part. As of August 19, 2016, press outlets had published or referenced [redacted] files taken by Snowden.[183]

~~(TS//SI//OC/NF)~~ **Tier Two:** Documents that, based on forensic analysis, Snowden would have collected in the course of collecting Tier One, but have not yet been disclosed to the public. The IC assesses these documents are likely in the hands of the media. [redacted][184]

~~(TS//SI//OC/NF)~~ **Tier Three:** The remaining [redacted] documents that Snowden accessed [redacted][185]

~~(S//NF)~~ The IC damage assessment of Tier One documents is still ongoing, but, as of late May 2016, the IC had no plans to carry out a damage assessment of the documents in Tier Two or Tier Three.[186] [redacted].[187] As a result, the IC's damage assessment cannot be considered a complete accounting of the damage Snowden caused to U.S. intelligence.

(U) However, even the IC's limited damage assessment of documents in Tier One indicates that Snowden's disclosures caused massive damage to national security. A few examples, listed below, illustrate the scale of the damage.

- ~~(TS//SI//NF)~~ [redacted][188]

[183] E-mail from NSA Legislative Affairs (Aug. 22, 2016, at 4:48PM). Overall document classified S//REL TO USA, FVEY; cited portion classified S//REL TO USA, FVEY.

[184] NCSC, "Intelligence Community Damage Assessment: Unauthorized Disclosures of Classified Information Attributed to Edward Snowden, 1 January 2015 through 31 August 2015," (Apr. 8, 2016), at 5. Overall document classified TS//HCS-P/SI-G/TK//OC/NF, cited portion classified TS//SI/OC/NF.

[185] *Id.*, cited portion classified TS//SI/OC/NF.

[186] HPSCI Staff Briefing with NCSC (May 25, 2016).

[187] NCSC, "Intelligence Community Damage Assessment: Unauthorized Disclosures of Classified Information Attributed to Edward Snowden, 1 January 2015 through 31 August 2015," (Apr. 8, 2016), at 1. Overall document classified TS//HCS-P/SI-G/TK//OC/NF; cited portion classified S//NF.

[188] HPSCI Staff Memorandum for the Record, "NSA Notification of [redacted] Resulting from Recent Media Disclosures," (July 8, 2014). Overall document classified TS//SI//NF.

  - ○ ~~(TS//SI//NF)~~ [redacted].[189]

  - ○ ~~(TS//SI//NF)~~ [redacted]

- ~~(S//SI//NF)~~ [redacted].[191]

- ~~(TS//SI//NF)~~ [redacted],[192] [redacted].[193]

  - ○ ~~(TS//SI//NF)~~ [redacted].[194]

[189] *Id.*
[190] *Id.*
[191] NCSC, "Intelligence Community Damage Assessment: Unauthorized Disclosures of Classified Information Attributed to Edward Snowden, 1 August 2014 through 31 December 2014," (Dec. 22, 2015), at 25. Overall document classified TS//HCS-P/SI-G/TK//OC/NF; cited portion classified S//SI//NF.
[192] Presidential Policy Directive 28, "Signals Intelligence Activities" (Jan. 17, 2014).
[193] Letter from Director of National Intelligence James R. Clapper to Chairman Devin Nunes and Ranking Member Adam Schiff (Jun. 23, 2015). Overall document classified TS//SI//NF, cited portion classified TS//SI//NF.
[194] NSA, "Response to Congressionally Directed Action: [redacted]," (Nov. 17, 2014), at 2-4. Overall document classified TS//SI//NF; cited portion classified TS//SI//NF.

        - ~~(TS//SI//NF)~~ [redacted]

    - ~~(TS//SI//NF)~~ [redacted].

    - ~~(TS//SI//NF)~~ [redacted].[195]

    - ~~(S//HCS-O//OC/NF)~~ Because of disclosures attributed to Snowden [redacted],[196] and in August 2015, [redacted].[197]

- ~~(S//NF)~~ [redacted]

    - ~~(TS//SI//NF)~~ [redacted].[198]

        - ~~(TS//SI//NF)~~ [redacted].[199]

[195] HPSCI Staff Briefing with ODNI (Sept. 6, 2016).

[196] HPSCI Staff Briefing with NCSC, NSA, CIA, and FBI (Jun. 17, 2016).

[197] NCSC, "Intelligence Community Damage Assessment: Unauthorized Disclosures of Classified Information Attributed to Edward Snowden, 1 August 2014 through 31 December 2014 – HCS-O Annex" (Dec. 22, 2015), . Overall document classified TS//HCS-O/SI//OC//NF; cited portion classified S//HCS-O//OC/NF.

[198] NCSC, "Intelligence Community Damage Assessment: Unauthorized Disclosures of Classified Information Attributed to Edward Snowden, 1 January 2015 through 31 August 2015," (Apr. 8, 2016), at 11. Overall document classified TS//HCS-P/SI-G/TK//OC/NF; cited portion classified TS//SI//NF.

[199] HPSCI Staff Briefing with NCSC, NSA, CIA, and FBI (Jun. 17, 2016).

  - ~~(S//HCS-P/SI//OC/NF)~~ [redacted].[200]

  - ~~(S//HCS-P/SI//OC/NF)~~ [redacted].[201]

  - ~~(TS//SI//NF)~~ [redacted].[202]

    - ~~(TS//SI//REL TO USA, FVEY)~~ [redacted].[203]

- ~~(TS//SI//OC/NF)~~ [redacted].[204] [redacted],[205] [redacted].[206]

[200] NCSC, "Intelligence Community Damage Assessment: Unauthorized Disclosures of Classified Information Attributed to Edward Snowden, 1 January 2015 through 31 August 2015," (Apr. 8, 2016), at 11. Overall document classified TS//HCS-P/SI-G/TK//OC/NF; cited portion classified S//HCS-P/SI//OC/NF.

[201] *Id.*, cited portion classified S//HCS-P/SI//OC/NF.

[202] NSA, "Response to Request for Information Re: [redacted]," (Dec. 16, 2014). Overall document classified TS//SI//NF; cited portion classified TS//SI//NF.

[203] CIA, Memorandum for Congress, "In Response to Questions on Decreased Collection Possibly Caused by Unauthorized Disclosures since June 2013," (July 20, 2016), at 2. Overall document classified TS//HCS-O-P CRD/SI//OC/NF; cited portion classified TS//SI/REL TO USA, FVEY).

[204] ODNI, Recouping Intelligence Capabilities Brief (Jun. 7, 2016), at 8. Overall document classified TS//SI//NF; cited portion classified TS//SI//NF; ODNI Briefing to HPSCI Staff on Recouping Intelligence Capabilities Brief (July 13, 2016).

[205] *Id.*

[206] ODNI, "Remediation of Unauthorized Disclosures" (June 2015), at 3. Overall document classified TS//SI//OC/NF; cited portion classified TS//SI//OC/NF.

- ○ ~~(TS//SI//NF)~~ [redacted][207] [redacted].
  - ■ [redacted][208].
- ● ~~(TS//SI//NF)~~ [redacted][209] [redacted][210].

(U) How Has the IC Recovered from Snowden?

~~(TS//SI//NF)~~ There is no IC-wide estimate for the total cost to the government of remediating Snowden's disclosures. However, a mid-2015 study by ODNI's Systems and Resources Analysis Group estimated that NSA and CIA will spend [redacted] over Fiscal Years 2016 and 2017 to recover from the damage Snowden's disclosures caused to SIGINT capabilities.[211]

~~(TS//SI//NF)~~ As a whole, the IC will undoubtedly spend even more. The [redacted] estimate represents a conservative assessment of the amount CIA and NSA will spend to rebuild SIGINT capabilities that were damaged by Snowden's disclosures. The estimate captures only two years of spending and does not reflect investments made before Fiscal Year 2016 or planned investments for Fiscal Year 2018 and beyond. Moreover, it does not capture the costs associated

[207] [redacted]

[208] [redacted].

[209] [redacted]

[210] HPSCI Staff Memorandum for the Record, "Upcoming Unauthorized Disclosures of [redacted] Overall document classified TS//SI//NF.

[211] ODNI SRA, "FY17 Major Issue Studies – Recouping Intelligence Capabilities," (June 7, 2016), at 9. Overall document classified TS//SI//NF; cited portion classified TS//SI//NF.

with the IC's damaged relationships with foreign and corporate partners, the opportunity cost of the time and resources the IC and DOD have spent mitigating the damage of the disclosures, or the costs of improved security measures across the federal government.

(U) Snowden's actions also exposed significant vulnerabilities in the IC's information security. Although it is impossible to reduce the risk of an insider threat like Snowden to zero, relatively simple changes such as automatically detecting the malicious use of scraping tools like "wget," physically disabling removable media from the workstations of NSA personnel who lack a work reason to use removable media, and implementing two-person controls to transfer data by removable media would have dramatically reduced the quantity of files Snowden could have removed or stopped him altogether.

(U) The Committee remains concerned that NSA, and the IC as a whole, have not done enough to reduce the chances of future insider threats like Snowden.

~~(C//REL TO USA, FVEY)~~ In the aftermath of Snowden's disclosures, NSA compiled a list of [redacted] security improvements for its networks. These improvements, called the "Secure the Net" initiatives, contained many steps that would have stopped Snowden, such as two-person control for transfer of data by removable media, and many broader security improvements, such as reducing the number of privileged users and authorized data transfer agents, and moving toward a continuous evaluation model for background investigations.[212] In July 2014, more than a year after Snowden's first disclosures, many of these "Secure the Net" initiatives—including some relatively simple initiatives, such as two-stage controls for systems administrators—had not been completed.[213] In August 2016, more than three years after Snowden's first disclosures, four of the [redacted] initiatives remained outstanding.[214]

(U) In the House-passed Intelligence Authorization Act for Fiscal Year 2016, the Committee directed the Department of Defense Inspector General (DOD IG) to carry out an assessment of information security at NSA, including whether NSA had successfully remediated the vulnerabilities exposed by Snowden.

(U) In August 2016, DOD IG issued its report, finding that NSA needed to take additional steps to effectively implement the privileged access-related "Secure the Net" initiatives.[215]

(U) In particular, DOD IG found that NSA had not: fully implemented technology to oversee privileged user activities; effectively reduced the number of privileged access users; or effectively reduced the number of authorized data transfer agents. In addition, contrary to the

[212] NSA, "Secure the Net Initiatives," (Aug. 22, 2016). Overall document classified C//REL TO USA, FVEY.
[213] NSA, "Secure the Net Initiatives," (July 2014). Overall document classified C//REL TO USA, FVEY.
[214] NSA, "Secure the Net Initiatives," (Aug. 22, 2016). Overall document classified C//REL TO USA, FVEY.
[215] Department of Defense Inspector General, Report 2016-129, "The National Security Agency Should Take Additional Steps in Its Privileged Access-Related Secure the Net Initiatives" (Aug. 29, 2016). Overall document classified S//NF, cited portion classified U//FOUO.

"Secure the Net" initiatives, NSA did not consistently secure server racks and other sensitive equipment in data centers, and did not extend two-stage authentication controls to all high-risk users.[216] Recent security breaches at NSA underscore the necessity for the agency to improve its security posture.

(U) And even though NSA has been the victim of recent breaches, it is not the only IC agency where information security needs to be improved. For instance, a recent CIA Inspector General report found that CIA has not yet implemented multi-factor authentication controls such as a physical token for general or privileged users of the Agency's enterprise or mission systems.[217]

(U) As a recent Committee report concluded, the introduction of the Intelligence Community Information Technology Enterprise (IC ITE) should produce an improved security environment in the IC.[218] And as that report noted, although IC data will be more secure and better protected under IC ITE than it is today, from both internal and external threats, IC ITE will also increase risks in different areas.[219] These risks will require dedicated attention to ensure IC ITE reaches its full potential for an improved security environment.

(U) Conclusion – Efforts to Improve Security

(U) Although it is impossible to reduce the chance of another Snowden to zero, more work can and should be done to improve the security of the people and computer networks that keep America's most closely held secrets.

(U) Since the beginning of Snowden's disclosures, the Committee has directed the IC to carry out a number of studies and security improvements to reduce the risk of another insider threat. Among its other oversight efforts, the Committee has:

- (U) Authorized an additional [redacted] for insider threat detection efforts in Fiscal Year 2014. Consistent with a spend plan and updated insider threat strategy provided to Congress, 60 percent of these funds were to be used for insider threat detection and the remaining 40 percent toward continuous evaluation;[220]

- (U) Directed the DNI to ensure that the President's National Insider Threat Policy and Minimum Standards were fully implemented on TS/SCI networks and all NIP-funded

[216] *Id.*, cited portion classified C//REL TO USA, FVEY.

[217] CIA Office of Inspector General, "Review of National Security Systems Required by the Cybersecurity Act of 2015," Report No. 2016-0022-AS (Aug. 2016). Overall report classified S//NF, cited portion classified S//NF.

[218] HPSCI Report, "Assessing IC ITE's Security Posture," (Feb. 4, 2016). Overall report classified S//NF, cited portion classified U.

[219] *Id.* at 25, cited portion classified U//FOUO.

[220] Classified Annex to Accompany the Report to the Intelligence Authorization Act for Fiscal Year 2014, P.L. 113-126, pp. 15-16.

networks at CIA, DIA, NSA, NGA, NRO, FBI, and DOE by October 1, 2014;[221]

- **(U)** Directed the DNI, as the Security Executive Agent, to establish a structure for a comprehensive continuous evaluation system for holders of TS/SCI within 270 days of the enactment;[222]

- **(U)** Directed the DNI, in coordination with the USD(I) to review whether the continuous evaluation process, insider threat auditing tools, and background investigation processes should consider different kinds of information to detect potential leakers than the current process collects to detect traditional security threats;[223]

- **(U)** Directed the DNI to review the management controls on privileged access, to include Systems Administrators;[224]

- **(U)** Directed the NSA to implement a "two person rule" for Tier 3 Systems Administrators and select Tier 2 Systems Administrators and directed the DNI to report to the Intelligence Committees on actions he is undertaking to lead the other IC elements in enacting a similar two person rule, or similar safeguards;[225]

- **(U)** Directed the DNI to attempt to reduce the number of Tier 3 System Administrators and ensure consistency in tier ratings across the IC;[226]

- **(U)** Directed the DNI to expand Scattered Castles to contain all TS/SCI clearance holders and list any pertinent exceptions or "flags" as close to real-time as possible;[227]

- **(U)** Directed the DNI to ensure that insider threat security measures were fully applied to contractors and contractor facilities;[228]

[221] Classified Annex to Accompany the Report to the Intelligence Authorization Act for Fiscal Year 2014, P.L. 113-126, p. 16; Classified Annex to Accompany the Report to the House-passed Intelligence Authorization Act for Fiscal Year 2014 pp. 32.

[222] Classified Annex to Accompany the Report to the Intelligence Authorization Act for Fiscal Year 2014, P.L. 113-126, p. 16; Classified Annex to Accompany the Report to the House-passed Intelligence Authorization Act for Fiscal Year 2014 pp. 32-33.

[223] Classified Annex to Accompany the Report to the Intelligence Authorization Act for Fiscal Year 2014, P.L. 113-126, p. 16; Classified Annex to Accompany the Report to the House-passed Intelligence Authorization Act for Fiscal Year 2014 p. 33.

[224] *Id.*

[225] *Id.*

[226] Classified Annex to Accompany the Report to the Intelligence Authorization Act for Fiscal Year 2014, P.L. 113-126, p. 16; Classified Annex to Accompany the Report to the House-passed Intelligence Authorization Act for Fiscal Year 2014 p. 34.

[227] *Id.*

[228] *Id.*

- **(U)** Required the IC to continuously evaluate the eligibility of personnel to access classified information, to develop procedures for automatically sharing derogatory information between agencies, and other improvements to the reinvestigation process;[229]

- **(U)** Encouraged the DNI to make a determination of how periodic reinvestigations will be handled in concert with a continuous evaluation program;[230]

- **(U)** Directed an IC analysis of private sector policies to reduce insider threats;[231]

- **(U)** Directed a DNI-led review once every three years of all U.S. government positions with access to classified information;[232]

- **(U)** Directed the DNI, in consultation with the Attorney General, the Secretary of Defense, and the Director of the Office of Personnel Management, to develop and implement procedures that govern whether and how publicly available information may be used in the security clearance process;[233]

- **(U)** Required each IC element to implement a program to enhance security reviews of individuals applying for access to classified information;[234]

- **(U)** Required the Inspector General of each federal agency that operates national security systems to report on, among other things, information security practices to detect data exfiltration and other threats;[235]

- **(U)** Directed NSA to produce a plan for completing security improvements to its networks by the end of Calendar Year 2018, including enclaves and systems used outside of NSA-controlled facilities; and[236]

[229] Intelligence Authorization Act for Fiscal Year 2014, P.L. 113-126, Title V.

[230] Classified Annex to Accompany the Report to the Intelligence Authorization Act for Fiscal Year 2014, P.L. 113-126, p. 16

[231] Intelligence Authorization Act for Fiscal Year 2015, P.L. 113-293, § 308.

[232] Classified Annex to Accompany the Report to the Intelligence Authorization Act for Fiscal Year 2015, P.L. 113-293, p. 11.

[233] Classified Annex to Accompany the Report to the Intelligence Authorization Act for Fiscal Year 2015, P.L. 113-293, pp. 11-12.

[234] Intelligence Authorization Act for Fiscal Year 2016, Division M, Consolidated Appropriations Act for Fiscal Year 2016, P.L. 114-113, § 306.

[235] Cybersecurity Act of 2015, Division N, Consolidated Appropriations Act for Fiscal Year 2016, P.L. 114-113, § 406

[236] Classified Annex to Accompany the Joint Explanatory Statement to the Intelligence Authorization Act for Fiscal Year 2016, Division M, Consolidated Appropriations Act for Fiscal Year 2016, P.L. 114-113, p. 19.

- **(U)** Directed the Intelligence Community Inspector General (IC IG) to carry out an assessment of post-Snowden information security improvements at CIA, DIA, FBI, NGA, NRO, and ODNI.[237]

(U) As the Fiscal Year 2017 Intelligence Authorization Act moves toward enactment and Congress begins its consideration of the President's Fiscal Year 2018 budget request, the Committee looks forward to working with the IC to ensure our nation's secrets receive the security they deserve.

[237] Classified Annex to Accompany the Report to the Intelligence Authorization Act for Fiscal Year 2017, H.R. 5077, p. 93.

Strzok, Peter P. (CD) (FBI)

From:	Strzok, Peter P. (CD) (FBI)
Sent:	Thursday, December 22, 2016 7:29 PM
To:	Page, Lisa C. (OGC) (FBI)
Subject:	Fwd: Media data pull

-------- Original message --------
From: "McCabe, Andrew G. (DO) (FBI) [redacted] b6 -1
Date: 12/22/2016 7:27 PM (GMT-05:00) b7C -1
To: "Strzok, Peter P. (CD) (FBI)" [redacted] b7E -6
Subject: RE: Media data pull

[redacted]

Andrew G. McCabe b6 -1
Deputy Director b7C -1
Federal Bureau of Investigation
[redacted]

-------- Original message --------
From: "Strzok, Peter P. (CD) (FBI) [redacted] b6 -1
Date: 12/22/16 7:25 PM (GMT-05:00) b7C -1
To: "McCabe, Andrew G. (DO) (FBI) [redacted] b7E -6
Cc: "Priestap, E. W. (CD) (FBI) [redacted]
Subject: Media data pull

Andy,

I received word via Jen that tomorrow morning Mike S wants to talk about whether we have opened a leak investigation into the publicity surrounding the C Foundation. He said he'd like to discuss, as the D "would like to do something."

I need guidance as to how/if you'd like me to detail the media pull we conducted. As you may recall, we have not detailed that activity other than to you and Bill.

Thanks,
Pete

Strzok, Peter P. (CD) (FBI)

From:	Strzok, Peter P. (CD) (FBI)
Sent:	Friday, December 23, 2016 10:57 AM
To:	Moffa, Jonathan C. (CD) (FBI); Page, Lisa C. (OGC) (FBI)
Subject:	I have copy 2 of 2

It was tricky hiding in SFR

Strzok, Peter P. (CD) (FBI)

From: Strzok, Peter P. (CD) (FBI)
Sent: Friday, December 23, 2016 4:40 PM
To: Page, Lisa C. (OGC) (FBI)
Subject: RE: [redacted]

b5 -1

Its deserved. You earned - fought - for it

-------- Original message --------
From: "Page, Lisa C. (OGC) (FBI)" [redacted]
Date: 12/23/2016 4:38 PM (GMT-05:00)
To: "Strzok, Peter P. (CD) (FBI)" [redacted]
Subject: RE [redacted]

b5 -1
b6 -1
b7C -1
b7E -6

Thank you. It's immodest, but I'm really really pleased with myself right now. ☺

[redacted]

b5 -1
b6 -1
b7C -1
b7E -6

Strzok, Peter P. (CD) (FBI)

From:	Strzok, Peter P. (CD) (FBI)
Sent:	Friday, December 23, 2016 6:24 PM
To:	Page, Lisa C. (OGC) (FBI)
Subject:	RE: Edits

Thanks. Curious what they are, even if I'm out.

Fucking go focus on Venezuela, I guess.

-------- Original message --------
From: "Page, Lisa C. (OGC) (FBI)[redacted] b6 -1
Date: 12/23/2016 6:10 PM (GMT-05:00) b7C -1
To: "Strzok, Peter P. (CD) (FBI)"[redacted] b7E -6
Subject: Fwd: Edits

Just FYI.

-------- Original message --------
From: "McCabe, Andrew G. (DO) (FBI)"[redacted] b6 -1
Date: 12/23/2016 5:56 PM (GMT-05:00) b7C -1
To: "Moffa, Jonathan C. (CD) (FBI)"[redacted] b7E -6
Cc: "Page, Lisa C. (OGC) (FBI)"[redacted]
Subject: Edits

John

I just spoke to the Boss following his read of the draft. He had two comments -[redacted] b5 -3
Not an emergency by any stretch.

More importantly, have a Merry Christmas.

Andrew G. McCabe
Deputy Director
Federal Bureau of Investigation
[redacted] b6 -1
b7C -1

Strzok, Peter P. (CD) (FBI)

From: Strzok, Peter P. (CD) (FBI)
Sent: Monday, December 26, 2016 2:27 PM
To: Page, Lisa C. (OGC) (FBI)
Subject: Fwd: Trump Aide Partnered With Firm Run by Man With Alleged KGB Ties - Bloomberg

See, look, I'm sharing.... ;)

-------- Original message --------
From: "Strzok, Peter P. (CD) (FBI)" [redacted]
Date: 12/26/2016 2:25 PM (GMT-05:00)
To: "Moffa, Jonathan C. (CD) (FBI)" [redacted] CD) (FBI)"
[redacted] (WF) (FBI)" [redacted]
Subject: Fwd: Trump Aide Partnered With Firm Run by Man With Alleged KGB Ties - Bloomberg

b6 -1
b7C -1
b7E -6

[redacted]

b6 -1
b7C -1

https://www.bloomberg.com/news/articles/2016-12-23/trump-aide-partnered-with-firm-run-by-man-with-alleged-kgb-ties

Trump Aide Partnered With Firm Run by Man With Alleged KGB Ties

More stories by David Kocieniewski • December 23, 2016, 5:00 AM EST

Donald Trump's national security adviser, Michael Flynn, partnered this year with a controversial technology company co-run by a man once convicted of trying to sell stolen biotech material to the Russian KGB espionage agency.

Subu Kota, who pleaded guilty in 1996 to selling the material to an FBI agent posing as a Russian spy, is one of two board directors at the company, Boston-based Brainwave

Science. During years of federal court proceedings, prosecutors presented evidence they said showed that between 1985 and 1990 Kota met repeatedly with a KGB agent and was part of a spy ring that made hundreds of thousands of dollars selling U.S. missile defense technology to Russian spies. Kota denied being part of a spy ring, reached a plea agreement in the biotech case and admitted to selling a sketch of a military helicopter to his co-defendant, who was later convicted of being a KGB operative.

Flynn served more than three decades in the military and rose to become director of the Defense Intelligence Agency before he was fired by President Barack Obama in 2014 over policy disagreements. He formed a private consulting firm, Flynn Intel Group, which has sought business with an array of cyber security firms and defense contractors. He began collaborating with Brainwave Science last spring.

Flynn, who has been widely criticized for close associations with Russia, has declined repeated requests during the past month to be interviewed about his company's business ties. A spokesman for the Trump transition team, Jason Miller, said in an email that Flynn has never met or spoken with Kota and that he has ended his association with Brainwave Science.

In a phone interview on Thursday, Kota described his criminal charges and dealings with the KGB as misunderstandings. He acknowledged selling biotech material to a federal agent posing as a Russian spy, but said the incident was a patent dispute, not espionage.

'Brain Fingerprinting'

Brainwave is seeking to develop a market for its innovative -– but broadly disputed -- technology called "brain fingerprinting" which tries to assess an interrogation subject's honesty through a brain scan. Flynn was brought onto the company's board of advisers to help sell the product to defense and law enforcement agencies, Brainwave President Krishna Ika said in an interview.

Ika said the company has not sold anything to U.S. federal agencies yet and is looking for investors. He runs the day-to-day operations while Kota brings business and technological expertise and helps make strategic decisions.

Although undercover federal agents testified that Kota bragged of his involvement in a KGB spy ring, Kota says he has never been a spy. He acknowledges meeting with Vladimir Galkin, a KGB agent, on at least four occasions and receiving hundreds of thousands of dollars in exchange for information about technology related to U.S. missile defense systems. But Kota said he thought Galkin was a businessman and that the information he provided was from public sources. Galkin was arrested at Kennedy Airport in 1996. Prosecutors were unable to build a case in the military spy ring they said he ran involving Kota and others after the U.S. State Department allowed him to leave the country.

Since pleading guilty to the biotech and tax evasion charges, Kota said he has steered clear of anything remotely illegal.

"Not even a parking ticket," he said.

Kota also runs a consulting company called The Boston Group. Federal court records show that after pleading guilty in the biotech case, he testified against his co-defendant and received a reduced sentence of four years' probation and a $50,000 fine.

Flynn has met with Brainwave officials at least 10 times, according to Ika, and signed a collaboration agreement to help drum up new business with U.S. agencies. Flynn also agreed to train any national security or law enforcement agency that purchased Brainwave products at Flynn Intel Group headquarters, Ika said. Flynn's company, based in the Washington suburb of Fairfax, Virginia, promised to provide "world-class training services led by qualified security professionals with experience in intelligence and investigation," Brainwave's website says.

Headpiece With Sensors

Flynn tested the product himself, Ika said. He put on the helmet-like headpiece fitted with sensors, which is said to read a subject's brainwaves in an attempt to detect information.

"He found it very convincing," Ika said.

Flynn's activities with the company continued after he began receiving classified intelligence briefings in mid-August as part of Trump's campaign. In late September, Ika said, he and Flynn pitched Brainwave to officials from the Bangladeshi defense forces during a meeting at Flynn's offices.

After Trump won the election in November and named Flynn his national security adviser, the collaboration stalled, Ika said. Lawyers are now negotiating how to continue Brainwave's collaboration with other partners from Flynn Intel Group.

Russia Today

Flynn has been criticized for making a paid speech at Russia Today, a state-run news agency, and sitting with President Vladimir Putin at a dinner in Moscow in 2015 to celebrate RT's anniversary. Flynn and his son also helped spread internet conspiracies on social media, and last February the elder Flynn tweeted, "Fear of Muslims is RATIONAL."

For defense employees and private-sector military contractors such as Flynn who want to check on potential business partners, the Department of Defense publishes a periodic report entitled "Espionage and Other Compromises of National Security." The 2009 edition, available online, includes a description of Kota's conviction.

Brainwave's product line is built on a technique developed by inventor Lawrence Farwell in the 1990s. The process received so much attention as a potential breakthrough for law enforcement that Congress ordered the General Accounting Office to study it. In a report released in 2001, the GAO found that its claims of effectiveness could not be validated and were not worth trying.

Ika said that after the 9/11 terror attacks, which inspired him to use his background to help fight terrorism, he heard about the technique and eventually collaborated with Farwell. Ika said he was convinced that skepticism about brain fingerprinting had been fomented by the "polygraph lobby" which did not want to lose business to a more effective technology. Brainwave now markets its product as an enhancement to polygraphs.

<ol class="noscript-footnotes"></ol>

Strzok, Peter P. (CD) (FBI)

From: Strzok, Peter P. (CD) (FBI)
Sent: Tuesday, December 27, 2016 10:30 AM
To: Priestap, E. W. (CD) (FBI); Rybicki, James E. (DO) (FBI); Kortan, Michael P. (DO) (FBI); Page, Lisa C. (OGC) (FBI); Moffa, Jonathan C. (CD) (FBI); [redacted] (OGC) (FBI)
Subject: Fwd: Did James Comey Cost Hillary Clinton The Election? We Asked The Late-Deciding Voters. | The Huffington Post

b6 -1
b7C -1

Notable that given the media outlet, they found no compelling argument the letters made a difference. And I found the quote interesting.

> "The letter itself didn't phase me or move me either way on Clinton. But her reaction to it kind of solidified it," Hernandez said. "If I wanted to say when I knew for sure, it was when they started attacking Comey for doing his job in the weekend prior to the election."
>
> http://m.huffpost.com/us/entry/us_58617933e4b0eb586486f317

NCCIC

Federal Bureau of Investigation

JOINT ANALYSIS REPORT

DISCLAIMER: *This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service referenced in this advisory or otherwise. This document is distributed as* ***TLP:WHITE:*** *Subject to standard copyright rules,* ***TLP:WHITE*** *information may be distributed without restriction. For more information on the Traffic Light Protocol, see https://www.us-cert.gov/tlp.*

Reference Number: JAR-16-20296 **December 29, 2016**

GRIZZLY STEPPE – Russian Malicious Cyber Activity

Summary

This Joint Analysis Report (JAR) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This document provides technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence Services (RIS) to compromise and exploit networks and endpoints associated with the U.S. election, as well as a range of U.S. Government, political, and private sector entities. The U.S. Government is referring to this malicious cyber activity by RIS as GRIZZLY STEPPE.

Previous JARs have not attributed malicious cyber activity to specific countries or threat actors. However, public attribution of these activities to RIS is supported by technical indicators from the U.S. Intelligence Community, DHS, FBI, the private sector, and other entities. This determination expands upon the Joint Statement released October 7, 2016, from the Department of Homeland Security and the Director of National Intelligence on Election Security.

This activity by RIS is part of an ongoing campaign of cyber-enabled operations directed at the U.S. government and its citizens. These cyber operations have included spearphishing campaigns targeting government organizations, critical infrastructure entities, think tanks, universities, political organizations, and corporations leading to the theft of information. In foreign countries, RIS actors conducted damaging and/or disruptive cyber-attacks, including attacks on critical infrastructure networks. In some cases, RIS actors masqueraded as third parties, hiding behind false online personas designed to cause the victim to misattribute the source of the attack. This JAR provides technical indicators related to many of these operations, recommended mitigations, suggested actions to take in response to the indicators provided, and information on how to report such incidents to the U.S. Government.

Description

The U.S. Government confirms that two different RIS actors participated in the intrusion into a U.S. political party. The first actor group, known as Advanced Persistent Threat (APT) 29, entered into the party's systems in summer 2015, while the second, known as APT28, entered in spring 2016.

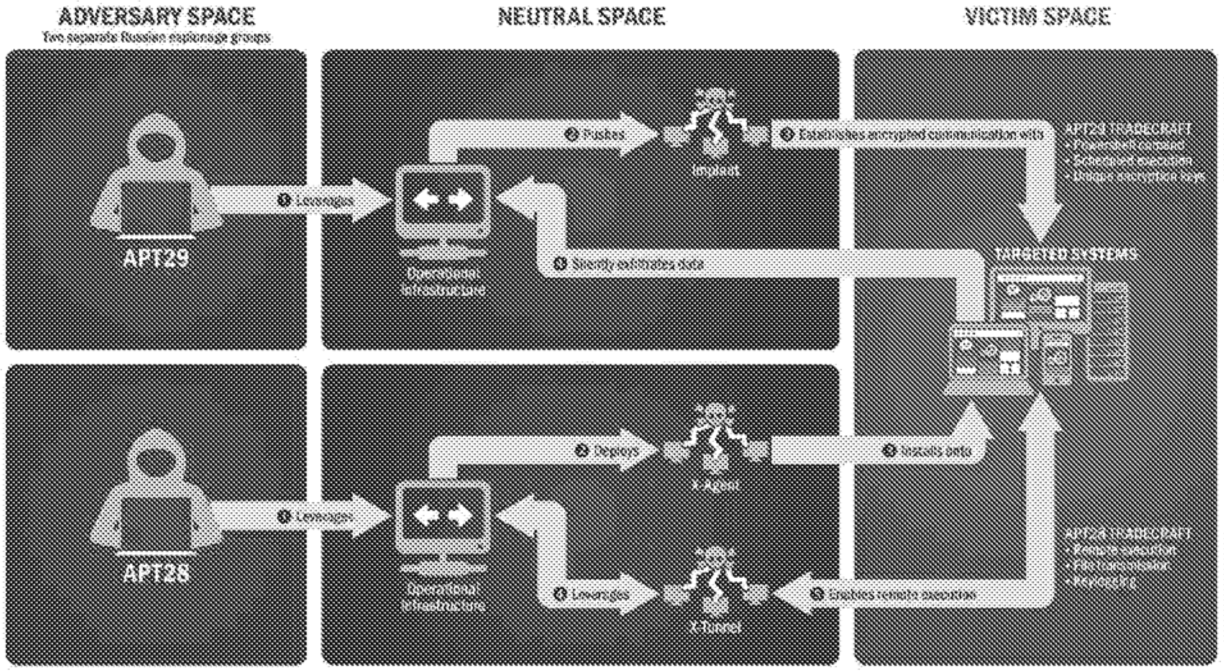


Figure 1: The tactics and techniques used by APT29 and APT 28 to conduct cyber intrusions against target systems

Both groups have historically targeted government organizations, think tanks, universities, and corporations around the world. APT29 has been observed crafting targeted spearphishing campaigns leveraging web links to a malicious dropper; once executed, the code delivers Remote Access Tools (RATs) and evades detection using a range of techniques. APT28 is known for leveraging domains that closely mimic those of targeted organizations and tricking potential victims into entering legitimate credentials. APT28 actors relied heavily on shortened URLs in their spearphishing email campaigns. Once APT28 and APT29 have access to victims, both groups exfiltrate and analyze information to gain intelligence value. These groups use this information to craft highly targeted spearphishing campaigns. These actors set up operational infrastructure to obfuscate their source infrastructure, host domains and malware for targeting organizations, establish command and control nodes, and harvest credentials and other valuable information from their targets.

In summer 2015, an APT29 spearphishing campaign directed emails containing a malicious link to over 1,000 recipients, including multiple U.S. Government victims. APT29 used legitimate domains, to include domains associated with U.S. organizations and educational institutions, to host malware and send spearphishing emails. In the course of that campaign, APT29 successfully compromised a U.S. political party. At least one targeted individual activated links to malware hosted on operational infrastructure of opened attachments containing malware. APT29 delivered malware to the political party's systems, established persistence, escalated privileges, enumerated active directory accounts, and exfiltrated email from several accounts through encrypted connections back through operational infrastructure.

In spring 2016, APT28 compromised the same political party, again via targeted spearphishing. This time, the spearphishing email tricked recipients into changing their passwords through a fake webmail domain hosted on APT28 operational infrastructure. Using the harvested credentials, APT28 was able to gain access and steal content, likely leading to the exfiltration of information from multiple senior party members. The U.S. Government assesses that information was leaked to the press and publicly disclosed.

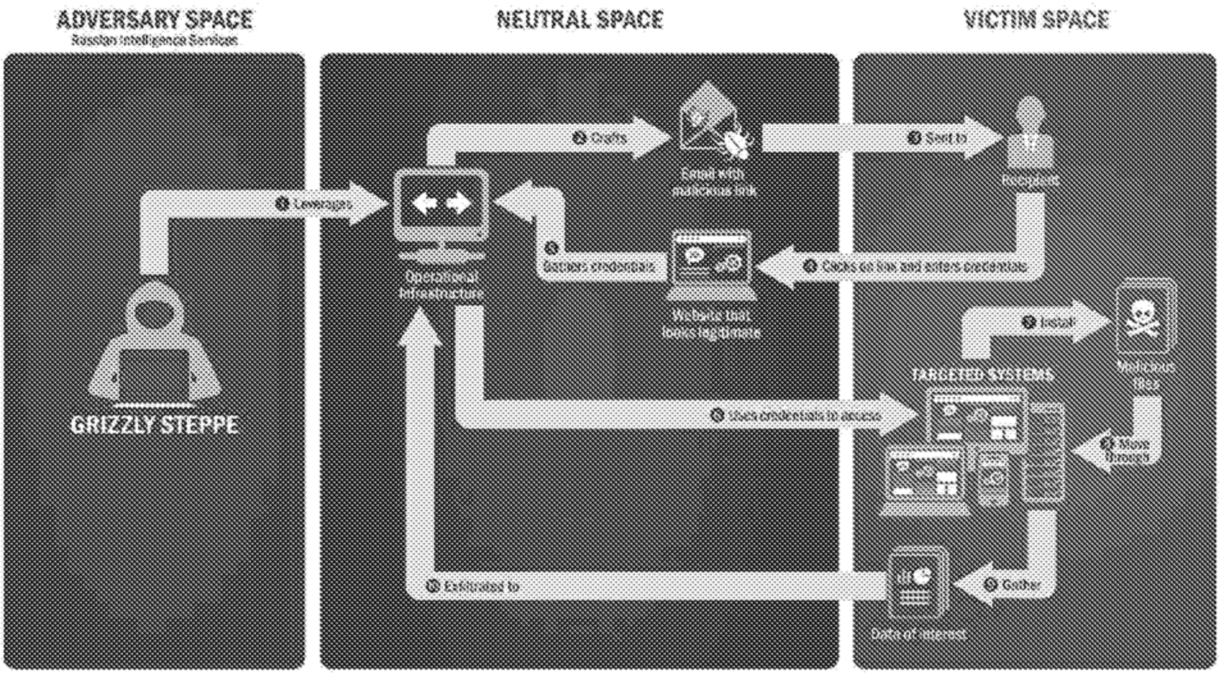


Figure 2: APT28's Use of Spearphishing and Stolen Credentials

Actors likely associated with RIS are continuing to engage in spearphishing campaigns, including one launched as recently as November 2016, just days after the U.S. election.

Reported Russian Military and Civilian Intelligence Services (RIS)

Alternate Names
APT28
APT29
Agent.btz
BlackEnergy V3
BlackEnergy2 APT
CakeDuke
Carberp
CHOPSTICK
CloudDuke
CORESHELL
CosmicDuke
COZYBEAR
COZYCAR
COZYDUKE
CrouchingYeti
DIONIS
Dragonfly
Energetic Bear
EVILTOSS
Fancy Bear
GeminiDuke
GREY CLOUD
HammerDuke
HAMMERTOSS
Havex
MiniDionis
MiniDuke
OLDBAIT
OnionDuke
Operation Pawn Storm
PinchDuke
Powershell backdoor
Quedagh
Sandworm
SEADADDY
Seaduke
SEDKIT
SEDNIT
Skipper
Sofacy
SOURFACE
SYNful Knock
Tiny Baron
Tsar Team
twain_64.dll (64-bit X-Agent implant)
VmUpgradeHelper.exe (X-Tunnel implant)
Waterbug
X-Agent

Technical Details

Indicators of Compromise (IOCs)

IOCs associated with RIS cyber actors are provided within the accompanying .csv and .stix files of JAR-16-20296.

Yara Signature

```
rule PAS_TOOL_PHP_WEB_KIT
{
meta:
description = "PAS TOOL PHP WEB KIT FOUND"
strings:
$php = "<?php"
$base64decode = /\='base'\.\(\d+\*\d+\)\.'_de'\.'code'/
$strreplace = "(str_replace("
$md5 = ".substr(md5(strrev("
$gzinflate = "gzinflate"
$cookie = "_COOKIE"
$isset = "isset"
condition:
(filesize > 20KB and filesize < 22KB) and
#cookie == 2 and
#isset == 3 and
all of them
}
```

Actions to Take Using Indicators

DHS recommends that network administrators review the IP addresses, file hashes, and Yara signature provided and add the IPs to their watchlist to determine whether malicious activity has been observed within their organizations. The review of network perimeter netflow or firewall logs will assist in determining whether your network has experienced suspicious activity.

When reviewing network perimeter logs for the IP addresses, organizations may find numerous instances of these IPs attempting to connect to their systems. Upon reviewing the traffic from these IPs, some traffic may correspond to malicious activity, and some may correspond to legitimate activity. Some traffic that may appear legitimate is actually malicious, such as vulnerability scanning or browsing of legitimate public facing services (e.g., HTTP, HTTPS, FTP). Connections from these IPs may be performing vulnerability scans attempting to identify websites that are vulnerable to cross-site scripting (XSS) or Structured Query Language (SQL) injection attacks. If scanning identified vulnerable sites, attempts to exploit the vulnerabilities may be experienced.

Network administrators are encouraged to check their public-facing websites for the malicious file hashes. System owners are also advised to run the Yara signature on any system that is suspected to have been targeted by RIS actors.

Threats from IOCs

Malicious actors may use a variety of methods to interfere with information systems. Some methods of attack are listed below. Guidance provided is applicable to many other computer networks.

- ***Injection Flaws*** are broad web application attack techniques that attempt to send commands to a browser, database, or other system, allowing a regular user to control behavior. The most common example is SQL injection, which subverts the relationship between a webpage and its supporting database, typically to obtain information contained inside the database. Another form is command injection, where an untrusted user is able to send commands to operating systems supporting a web application or database. See the United States Computer Emergency Readiness Team (US-CERT) Publication on SQL Injection for more information.
- ***Cross-site scripting (XSS) vulnerabilities*** allow threat actors to insert and execute unauthorized code in web applications. Successful XSS attacks on websites can provide the attacker unauthorized access. For prevention and mitigation strategies against XSS, see US-CERT's Alert on Compromised Web Servers and Web Shells.
- ***Server vulnerabilities*** may be exploited to allow unauthorized access to sensitive information. An attack against a poorly configured server may allow an adversary access to critical information including any websites or databases hosted on the server. See US-CERT's Tip on Website Security for additional information.

Recommended Mitigations

Commit to Cybersecurity Best Practices

A commitment to good cybersecurity and best practices is critical to protecting networks and systems. Here are some questions you may want to ask your organization to help prevent and mitigate against attacks.

1. **Backups**: Do we backup all critical information? Are the backups stored offline? Have we tested our ability to revert to backups during an incident?
2. **Risk Analysis**: Have we conducted a cybersecurity risk analysis of the organization?
3. **Staff Training**: Have we trained staff on cybersecurity best practices?
4. **Vulnerability Scanning & Patching**: Have we implemented regular scans of our network and systems and appropriate patching of known system vulnerabilities?
5. **Application Whitelisting**: Do we allow only approved programs to run on our networks?
6. **Incident Response**: Do we have an incident response plan and have we practiced it?

7. **Business Continuity**: Are we able to sustain business operations without access to certain systems? For how long? Have we tested this?
8. **Penetration Testing**: Have we attempted to hack into our own systems to test the security of our systems and our ability to defend against attacks?

Top Seven Mitigation Strategies

DHS encourages network administrators to implement the recommendations below, which can prevent as many as 85 percent of targeted cyber-attacks. These strategies are common sense to many, but DHS continues to see intrusions because organizations fail to use these basic measures.

1. **Patch applications and operating systems –** Vulnerable applications and operating systems are the targets of most attacks. Ensuring these are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker. Use best practices when updating software and patches by only downloading updates from authenticated vendor sites.
2. **Application whitelisting –** Whitelisting is one of the best security strategies because it allows only specified programs to run while blocking all others, including malicious software.
3. **Restrict administrative privileges –** Threat actors are increasingly focused on gaining control of legitimate credentials, especially those associated with highly privileged accounts. Reduce privileges to only those needed for a user's duties. Separate administrators into privilege tiers with limited access to other tiers.
4. **Network Segmentation and Segregation into Security Zones** – Segment networks into logical enclaves and restrict host-to-host communications paths. This helps protect sensitive information and critical services and limits damage from network perimeter breaches.
5. **Input validation –** Input validation is a method of sanitizing untrusted user input provided by users of a web application, and may prevent many types of web application security flaws, such as SQLi, XSS, and command injection.
6. **File Reputation** – Tune Anti-Virus file reputation systems to the most aggressive setting possible; some products can limit execution to only the highest reputation files, stopping a wide range of untrustworthy code from gaining control.
7. **Understanding firewalls –** When anyone or anything can access your network at any time, your network is more susceptible to being attacked. Firewalls can be configured to block data from certain locations (IP whitelisting) or applications while allowing relevant and necessary data through.

Responding to Unauthorized Access to Networks

Implement your security incident response and business continuity plan. It may take time for your organization's IT professionals to isolate and remove threats to your systems and restore normal operations. Meanwhile, you should take steps to maintain your organization's essential functions according to your business continuity plan. Organizations should maintain and regularly test backup plans, disaster recovery plans, and business continuity procedures.

Contact DHS or law enforcement immediately. We encourage you to contact DHS NCCIC (NCCICCustomerService@hq.dhs.gov or 888-282-0870), the FBI through a local field office or the FBI's Cyber Division (CyWatch@ic.fbi.gov or 855-292-3937) to report an intrusion and to request incident response resources or technical assistance.

Detailed Mitigation Strategies

Protect Against SQL Injection and Other Attacks on Web Services

Routinely evaluate known and published vulnerabilities, perform software updates and technology refreshes periodically, and audit external-facing systems for known Web application vulnerabilities. Take steps to harden both Web applications and the servers hosting them to reduce the risk of network intrusion via this vector.[1]

- Use and configure available firewalls to block attacks.
- Take steps to further secure Windows systems such as installing and configuring Microsoft's Enhanced Mitigation Experience Toolkit (EMET) and Microsoft AppLocker.
- Monitor and remove any unauthorized code present in any www directories.
- Disable, discontinue, or disallow the use of Internet Control Message Protocol (ICMP) and Simple Network Management Protocol (SNMP) and response to these protocols as much as possible.
- Remove non-required HTTP verbs from Web servers as typical Web servers and applications only require GET, POST, and HEAD.
- Where possible, minimize server fingerprinting by configuring Web servers to avoid responding with banners identifying the server software and version number.
- Secure both the operating system and the application.
- Update and patch production servers regularly.
- Disable potentially harmful SQL-stored procedure calls.
- Sanitize and validate input to ensure that it is properly typed and does not contain escaped code.
- Consider using type-safe stored procedures and prepared statements.
- Perform regular audits of transaction logs for suspicious activity.
- Perform penetration testing against Web services.
- Ensure error messages are generic and do not expose too much information.

[1] http://msdn.microsoft.com/en-us/library/ff648653.aspx. Web site last accessed April 11, 2016.

Phishing and Spearphishing

- Implement a Sender Policy Framework (SPF) record for your organization's Domain Name System (DNS) zone file to minimize risks relating to the receipt of spoofed messages.
- Educate users to be suspicious of unsolicited phone calls, social media interactions, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in social media or email, and do not respond to solicitations for this information. This includes following links sent in email.
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL often includes a variation in spelling or a different domain than the valid website (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org).
- Take advantage of anti-phishing features offered by your email client and web browser.
- Patch all systems for critical vulnerabilities, prioritizing timely patching of software that processes Internet data, such as web browsers, browser plugins, and document readers.

Permissions, Privileges, and Access Controls

- Reduce privileges to only those needed for a user's duties.
- Restrict users' ability (permissions) to install and run unwanted software applications, and apply the principle of "Least Privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through the network.
- Carefully consider the risks before granting administrative rights to users on their own machines.
- Scrub and verify all administrator accounts regularly.
- Configure Group Policy to restrict all users to only one login session, where possible.
- Enforce secure network authentication where possible.
- Instruct administrators to use non-privileged accounts for standard functions such as Web browsing or checking Web mail.

- Segment networks into logical enclaves and restrict host-to-host communication paths. Containment provided by enclaving also makes incident cleanup significantly less costly.
- Configure firewalls to disallow RDP traffic coming from outside of the network boundary, except for in specific configurations such as when tunneled through a secondary VPN with lower privileges.
- Audit existing firewall rules and close all ports that are not explicitly needed for business. Specifically, carefully consider which ports should be connecting outbound versus inbound.
- Enforce a strict lockout policy for network users and closely monitor logs for failed login activity. This can be indicative of failed intrusion activity.
- If remote access between zones is an unavoidable business need, log and monitor these connections closely.
- In environments with a high risk of interception or intrusion, organizations should consider supplementing password authentication with other forms of authentication such as challenge/response or multifactor authentication using biometric or physical tokens.

Credentials

- Enforce a tiered administrative model with dedicated administrator workstations and separate administrative accounts that are used exclusively for each tier to prevent tools, such as Mimikatz, for credential theft from harvesting domain-level credentials.
- Implement multi-factor authentication (e.g., smart cards) or at minimum ensure users choose complex passwords that change regularly.
- Be aware that some services (e.g., FTP, telnet, and .rlogin) transmit user credentials in clear text. Minimize the use of these services where possible or consider more secure alternatives.
- Properly secure password files by making hashed passwords more difficult to acquire. Password hashes can be cracked within seconds using freely available tools. Consider restricting access to sensitive password hashes by using a shadow password file or equivalent on UNIX systems.
- Replace or modify services so that all user credentials are passed through an encrypted channel.
- Avoid password policies that reduce the overall strength of credentials. Policies to avoid include lack of password expiration date, lack of lockout policy, low or disabled password complexity requirements, and password history set to zero.
- Ensure that users are not re-using passwords between zones by setting policies and conducting regular audits.
- Use unique passwords for local accounts for each device.

Logging Practices

- Ensure event logging (applications, events, login activities, security attributes, etc.) is turned on or monitored for identification of security issues.
- Configure network logs to provide enough information to assist in quickly developing an accurate determination of a security incident.
- Upgrade PowerShell to new versions with enhanced logging features and monitor the logs to detect usage of PowerShell commands, which are often malware-related.
- Secure logs, potentially in a centralized location, and protect them from modification.
- Prepare an incident response plan that can be rapidly implemented in case of a cyber intrusion.

How to Enhance Your Organization's Cybersecurity Posture

DHS offers a variety of resources for organizations to help recognize and address their cybersecurity risks. Resources include discussion points, steps to start evaluating a cybersecurity program, and a list of hands-on resources available to organizations. For a list of services, visit https://www.us-cert.gov/ccubedvp. Other resources include:

- **The Cyber Security Advisors (CSA)** program bolsters cybersecurity preparedness, risk mitigation, and incident response capabilities of critical infrastructure entities and more closely aligns them with the Federal Government. CSAs are DHS personnel assigned to districts throughout the country and territories, with at least one advisor in each of the 10 CSA regions, which mirror the Federal Emergency Management Agency regions. For more information, email cyberadvisor@hq.dhs.gov.
- **Cyber Resilience Review (CRR)** is a no-cost, voluntary assessment to evaluate and enhance cybersecurity within critical infrastructure sectors, as well as state, local, tribal, and territorial governments. The goal of the CRR is to develop an understanding and measurement of key cybersecurity capabilities to provide meaningful indicators of an entity's operational resilience and ability to manage cyber risk to critical services during normal operations and times of operational stress and crisis. Visit https://www.cert.org/resilience/rmm.html to learn more about the CERT Resilience Management Model.
- **Enhanced Cybersecurity Services (ECS)** helps critical infrastructure owners and operators protect their systems by sharing sensitive and classified cyber threat information with Commercial Service Providers (CSPs) and Operational Implementers (OIs). CSPs then use the cyber threat information to protect CI customers. OIs use the threat information to protect internal networks. For more information, email ECS_Program@hq.dhs.gov.
- **The Cybersecurity Information Sharing and Collaboration Program (CISCP)** is a voluntary information-sharing and collaboration program between and among critical

infrastructure partners and the Federal Government. For more information, email CISCP@us-cert.gov.

- **The Automated Indicator Sharing (AIS)** initiative is a DHS effort to create a system where as soon as a company or federal agency observes an attempted compromise, the indicator will be shared in real time with all of our partners, protecting them from that particular threat. That means adversaries can only use an attack once, which increases their costs and ultimately reduces the prevalence of cyber-attacks. While AIS will not eliminate sophisticated cyber threats, it will allow companies and federal agencies to concentrate more on them by clearing away less sophisticated attacks.
- AIS participants connect to a DHS-managed system in the NCCIC that allows bidirectional sharing of cyber threat indicators. A server housed at each participant's location allows each to exchange indicators with the NCCIC. Participants will not only receive DHS-developed indicators, but can share indicators they have observed in their own network defense efforts, which DHS will then share with all AIS participants. For more information, visit https://www.dhs.gov/ais.
- **The Cybersecurity Framework (Framework),** developed by the National Institute of Standards and Technology (NIST) in collaboration with the public and private sectors, is a tool that can improve the cybersecurity readiness of entities. The Framework enables entities, regardless of size, degree of cyber risk, or cyber sophistication, to apply principles and best practices of risk management to improve the security and resiliency of critical infrastructure. The Framework provides standards, guidelines, and practices that are working effectively today. It consists of three parts—the Framework Core, the Framework Profile, and Framework Implementation Tiers—and emphasizes five functions: Identify, Protect, Detect, Respond, and Recover. Use of the Framework is strictly voluntary. For more information, visit https://www.nist.gov/cyberframework or email cyberframework@nist.gov.

Contact Information

Recipients of this report are encouraged to contribute any additional information that they may have related to this threat. Include the JAR reference number (JAR-16-20296) in the subject line of all email correspondence. For any questions related to this report, please contact NCCIC or the FBI.

NCCIC:
Phone: +1-888-282-0780
Email: NCCICCustomerService@hq.dhs.gov

FBI:
Phone: +1-855-292-3937
Email: cywatch@ic.fbi.gov

Feedback

NCCIC continuously strives to improve its products and services. You can help by answering a few short questions about this product at the following URL: https://www.us-cert.gov/forms/feedback.

Strzok, Peter P. (CD) (FBI)

From:	Strzok, Peter P. (CD) (FBI)
Sent:	Friday, December 30, 2016 1:47 PM
To:	Page, Lisa C. (OGC) (FBI)
Subject:	RE: CALENDAR HOLD FOR TUESDAY, 01/03

Thanks. I asked Jon already, I'm hoping he can have someone leave a copy in my office, I am going in sometime over the weekend to read it before Tues.

-------- Original message --------
From: "Page, Lisa C. (OGC) (FBI [redacted]
Date: 12/30/2016 1:44 PM (GMT-05:00)
To: "Baker, James A. (OGC) (FBI)" [redacted] "Priestap, E. W. (CD) (FBI)"
[redacted] "Anderson, Trisha B. (OGC) (FBI)" [redacted]
[redacted] OGC) (FBI) [redacted] "Strzok, Peter P. (CD) (FBI)"
[redacted] "Moffa, Jonathan C. (CD) (FBI)" [redacted] "Boone, Jennifer C. (CD) (FBI)" [redacted]
Subject: CALENDAR HOLD FOR TUESDAY, 01/03

b6 -1
b7C -1
b7E -6

Folks --

An invite will likely follow later today or Tuesday, but I wanted to alert you all now that the Director would like to have a discussion about the report (in particular about those facts that are uniquely ours) and other related topics on Tuesday, January 3, probably from 1-3. Bill and I have additional detail for those at HQ today. Thanks.

Lisa

Strzok, Peter P. (CD) (FBI)

From: Strzok, Peter P. (CD) (FBI)
Sent: Saturday, December 31, 2016 8:38 AM
To: Page, Lisa C. (OGC) (FBI)
Subject: Fwd: CALENDAR HOLD FOR TUESDAY, 01/03

-------- Original message --------
From: "Moffa, Jonathan C. (CD) (FBI)" [redacted]
Date: 12/31/2016 8:34 AM (GMT-05:00)
To: "Strzok, Peter P. (CD) (FBI)" [redacted]
Subject: RE: CALENDAR HOLD FOR TUESDAY, 01/03

b6 -1
b7C -1
b7E -6

[redacted]

b5 -1

J

--

-------- Original message --------
From: "Strzok, Peter P. (CD) (FBI)" [redacted]
Date: 12/31/2016 8:09 AM (GMT-05:00)
To: "Moffa, Jonathan C. (CD) (FBI)" [redacted]
Subject: RE: CALENDAR HOLD FOR TUESDAY, 01/03

b6 -1
b7C -1
b7E -6

[redacted]

b5 -1

Anyway, I think I'm going to send him a happy new year email and ask for some time on Tuesday. Which may end up having to be at 8:00 at night.

Strzok, Peter P. (CD) (FBI)

From:	Strzok, Peter P. (CD) (FBI)
Sent:	Sunday, January 01, 2017 10:57 AM
To:	Page, Lisa C. (OGC) (FBI)
Subject:	Fwd: Trump Promises a Revelation on Hacking - NYTimes.com

Funnies

-------- Original message --------
From: [redacted](WF) (FBI)"[redacted]
Date: 01/01/2017 10:45 AM (GMT-05:00)
To: [redacted](CD) (FBI)[redacted]"Strzok, Peter P. (CD) (FBI)"
[redacted]"Moffa, Jonathan C. (CD) (FBI)[redacted]
Subject: RE: Trump Promises a Revelation on Hacking - NYTimes.com

b6 -1
b7C -1
b7E -6

To be accurate he called it a code word not a password. Ha!

...

-------- Original message --------
From: [redacted](CD) (FBI)[redacted]
Date: 01/01/2017 8:12 AM (GMT-05:00)
To: "Strzok, Peter P. (CD) (FBI)"[redacted](WF) (FBI)"
[redacted]"Moffa, Jonathan C. (CD) (FBI)[redacted]
Subject: RE: Trump Promises a Revelation on Hacking - NYTimes.com

b6 -1
b7C -1
b7E -6

[redacted]

b6 -1
b7C -1

...

-------- Original message --------
From: "Strzok, Peter P. (CD) (FBI)"[redacted]
Date: 01/01/2017 8:06 AM (GMT-05:00)
To: [redacted]WF) (FBI)"[redacted]"Moffa, Jonathan C. (CD) (FBI)"
[redacted](CD) (FBI)"[redacted]
Subject: Fwd: Trump Promises a Revelation on Hacking - NYTimes.com

b6 -1
b7C -1
b7E -6

I think the Tuesday surprise is all the stuff [redacted] told him during the CI briefing. He DID mention the stuff about his son and the computer password...

b6 -1
b7C -1

Happy New Year

"I don't care what they say, no computer is safe," he added. "I have a boy who's 10 years old; he can do anything with a computer. You want something to really go without detection, write it out and have it sent by courier."

http://mobile.nytimes.com/2016/12/31/us/politics/donald-trump-russia-hacking.html?emc=edit_th_20170101&nl=todaysheadlines&nlid=71166045&_r=0&referer=

Trump Promises a Revelation on Hacking

December 31, 2016

WEST PALM BEACH, Fla. — President-elect Donald J. Trump, expressing lingering skepticism about intelligence assessments of Russian interference in the election, said on Saturday evening that he knew "things that other people don't know" about the hacking, and that the information would be revealed "on Tuesday or Wednesday."

Speaking to a handful of reporters outside his Palm Beach, Fla., club, Mar-a-Lago, Mr. Trump cast his declarations of doubt as an effort to seek the truth.

"I just want them to be sure because it's a pretty serious charge," Mr. Trump said of the intelligence agencies. "If you look at the weapons of mass destruction, that was a disaster, and they were wrong," he added, referring to intelligence cited by the George W. Bush administration to support its march to war in 2003. "So I want them to be sure," the president-elect said. "I think it's unfair if they don't know."

He added: "And I know a lot about hacking. And hacking is a very hard thing to prove. So it could be somebody else. And I also know things that other people don't know, and so they cannot be sure of the situation."

When asked what he knew that others did not, Mr. Trump demurred, saying only, "You'll find out on Tuesday or Wednesday."

Mr. Trump, who does not use email, also advised people to avoid computers when dealing with delicate material. "It's very important, if you have something really important, write it out and have it delivered by courier, the old-fashioned way, because

I'll tell you what, no computer is safe," Mr. Trump said.

"I don't care what they say, no computer is safe," he added. "I have a boy who's 10 years old; he can do anything with a computer. You want something to really go without detection, write it out and have it sent by courier."

The comments on Saturday were a departure from a statement that Mr. Trump issued through transition officials last week, in which he said that it was time for people to "move on" from the hacking issue but that he would be briefed on the matter by intelligence officials early in the new year.

On Thursday, President Obama ordered a set of retaliatory measures against Russia over the election hacking. The United States expelled 35 Russian diplomats and shuttered two estates that it claimed had been used for intelligence-gathering.

The Russian president, Vladimir V. Putin, declined to respond in kind to the measures, a gesture that Mr. Trump appeared to view favorably. He praised it on Twitter and criticized news media coverage that had been harsh about Russia.

Mr. Trump, who has sought a warmer relationship with Mr. Putin, has repeatedly scoffed at the notion that Russia was behind the hacking, a stance at odds with members of his own party. At one point, Mr. Trump declared that the hacking may have been the work of "someone sitting on their bed weighing 400 pounds."

Strzok, Peter P. (CD) (FBI)

From:	Strzok, Peter P. (CD) (FBI)
Sent:	Wednesday, January 04, 2017 9:53 AM
To:	Page, Lisa C. (OGC) (FBI)
Attachments:	RL33265.pdf

b5 -1, 2, 3

[redacted]

Congressional
Research Service
Informing the legislative debate since 1914

Conducting Foreign Relations Without Authority: The Logan Act

Michael V. Seitzinger
Legislative Attorney

March 11, 2015

Congressional Research Service
7-5700
www.crs.gov
RL33265

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

The Logan Act, codified at 18 U.S.C. § 953, states:

> Any citizen of the United States, wherever he may be, who, without authority of the United States, directly or indirectly commences or carries on any correspondence or intercourse with any foreign government or any officer or agent thereof, in relation to any disputes or controversies with the United States, or to defeat the measures of the United States, shall be fined under this title or imprisoned not more than three years, or both.
>
> This section shall not abridge the right of a citizen to apply, himself or his agent, to any foreign government or the agents thereof for redress of any injury which he may have sustained from such government or any of its agents or subjects.

The Logan Act was intended to prohibit United States citizens without authority from interfering in relations between the United States and foreign governments. There appear to have been no prosecutions under the act in its more than 200-year history. However, there have been a number of judicial references to the act, and it is not uncommon for it to be used as a point of challenge concerning dealings with foreign officials

There has been renewed interest in the Logan Act in 2015 as the result of a letter signed by 47 U.S. Senators to Iran suggesting that negotiations about a nuclear deal between the President and the Iranian leadership would be an executive agreement that another President or Congress would be able to abrogate. Some have raised questions about the constitutionality of the act, whether it applies to Members of Congress, and its current viability. Commenters have provided arguments that both support and oppose the legality of the Senators' letter.

Although attempts have been made to repeal the act, it remains law and at least a potential sanction which could be used against anyone who without authority interferes in the foreign relations of the United States.

Contents

Contacts

Introduction

The Logan Act, designed to cover relations between private citizens of the United States and foreign governments, has prompted much controversy as to its scope and effect in its more than 200 years. Described as either a "paper dragon or sleeping giant" by one commentator, proclaimed to be possibly unconstitutional by others, it represents a combination of legal and policy factors in both domestic and international concerns.

As amended, the act states:

> Any citizen of the United States, wherever he may be, who, without authority of the United States, directly or indirectly commences or carries on any correspondence or intercourse with any foreign government or any officer or agent thereof, in relation to any disputes or controversies with the United States, or to defeat the measures of the United States, shall be fined under this title or imprisoned not more than three years, or both.
>
> This section shall not abridge the right of a citizen to apply, himself or his agent, to any foreign government or the agents thereof for redress of any injury which he may have sustained from such government or any of its agents or subjects.[1]

In 1994 the fine was changed from $5,000 to "under this title."[2] Otherwise, there do not appear to have been any substantial changes in the act since its original enactment on January 30, 1799, as 1 Stat. 613.

History of the Logan Act

After the French Revolution, difficulties developed between the Federalist Administration of the United States and the various revolutionary governments of France.[3] Because the United States had not assisted the French revolutionaries to their satisfaction and because the United States had ratified the Jay Treaty with Great Britain, the French government authorized plunderings of American merchant ships. In 1797 President Adams sent John Marshall, Charles C. Pinckney, and Elbridge Gerry as special envoys to France to negotiate and settle claims and causes of differences which existed between the French Directory and the United States. This mission resulted in the XYZ letters controversy, and its failure led to such strong anti-France feelings in the United States that preparations for war were begun by the Congress.

After the unsuccessful envoys returned from France, Dr. George Logan, a Philadelphia Quaker, a doctor, and a Republican, decided to attempt on his own to settle the controversies. Bearing a private certificate of citizenship from his friend, Thomas Jefferson, who at the time was Vice President, Logan sailed for France on June 12, 1798. In France he was hailed by the newspapers

[1] 18 U.S.C. § 953.

[2] P.L. 103-322, § 330016(1)(K). *See* 18 U.S.C. section 3571 for schedule of fines applicable to one found guilty of type of felony represented by Logan Act.

[3] For additional information on the history of the Logan Act, *see* Kearney, *Private Citizens in Foreign Affairs*, 36 EMORY L.J. 285 (1987); Vagts, *The Logan Act: Paper Tiger or Sleeping Giant?*, 60 A.J.I.L. 268 (1966); and Warren, *History of Laws Prohibiting Correspondence with a Foreign Government and Acceptance of a Commission*, S. Doc. No. 696, 64th Cong., 2d Sess. (1917).

as the envoy of peace and was received by Talleyrand. The French Directory, having concluded that it was politically wise to relax tensions with the United States, issued a decree raising the embargo on American merchant ships and freed American ships and seamen.

Logan, however, received a less friendly response from the United States after he returned. Secretary of State Timothy Pickering told him that the French decree was illusory. General Washington expressed his disapproval of Logan's actions. President Adams recommended that Congress take action to stop the "temerity and impertinence of individuals affecting to interfere in public affairs between France and the United States."[4] Representative Roger Griswold of Connecticut introduced a resolution in Congress to prevent actions similar to Logan's:

> *Resolved*, That a committee be appointed to inquire into the expediency of amending the act entitled "An act in addition to the act for the punishment of certain crimes against the United States," so far as to extend the penalties, if need be, to all persons, citizens of the United States, who shall usurp the Executive authority of this Government, by commencing or carrying on any correspondence with the Governments of any foreign prince or state, relating to controversies or disputes which do or shall exist between such prince or state, and the United States.[5]

The resolution was passed, and the committee was appointed. On January 7, 1799, Griswold introduced in the House a bill based on the resolution:

> *Be it enacted, etc.*, that if any person, being a citizen of the United States, or in any foreign country, shall, without the permission or authority of the Government of the United States, directly or indirectly, commence or carry on any verbal or written correspondence or intercourse with any foreign Government, or any officer or agent thereof, relating to any dispute or controversy between any foreign Government and the United States, with an intent to influence the measures or conduct of the Government having disputes or controversies with the United States, as aforesaid; or of any person, being a citizen of or resident within, the United States, and not duly authorized shall counsel, advise, aid or assist, in any such correspondence with intent as aforesaid, he or they shall be deemed guilty of a high misdemeanor; and, on conviction before any court of the United States having jurisdiction thereof, shall be punished by a fine not exceeding—thousand dollars, and by imprisonment during a term not less than—months, not exceeding—years.[6]

The bill was debated at length, and various amendments were proposed, some of which passed and some of which did not. The House of Representatives passed the bill on January 17, 1799, and the Senate passed it on January 25, 1799. It was signed and became a law on January 30, 1799.

[4] 1 MESSAGES AND PAPERS OF THE PRESIDENT 267 (Richardson ed., 1897).

[5] 9 ANNALS OF CONGRESS 2489, 5th Cong. (1798).

[6] *Id.* at 2565, 2583 (1799).

Judicial References to the Logan Act

There appear to have been few indictments under the Logan Act.[7] The one indictment found occurred in 1803 when a grand jury indicted Francis Flournoy, a Kentucky farmer, who wrote an article in the *Frankfort Guardian of Freedom* under the pen name of "A Western American." Flournoy advocated in the article a separate Western nation allied to France. The United States Attorney for Kentucky, an Adams appointee and brother-in-law of Chief Justice Marshall, went no further than procuring the indictment of Flournoy, and the purchase of the Louisiana Territory later that year appeared to cause the separatism issue to become obsolete.

So far as can be determined, there have been no prosecutions under the Logan Act. However, there have been a number of judicial references to the act, among which are the following.

Judge Sprague of the Circuit Court for the District of Massachusetts mentioned the Logan Act in two charges that he made to grand juries during the Civil War. On October 18, 1861, he said:

> There are other defenses to which our attention is called by the present condition of our country. A few months since a member of the British parliament declared, in the most public manner, that he had received many letters from the Northern states of America urging parliament to acknowledge the independence of the Southern confederacy. Such an announcement ought to arrest the attention of grand juries; for if any such communication has been made by a citizen of the United States, it is a high misdemeanor. St. 1799, c. 1. (1 Stat. 613) was especially designed to prevent such unwarrantable interference with the diplomacy and purposes of our government.[8]

In the second grand jury charge referring to the Logan Act, made in 1863, Judge Sprague stated:

> We have seen it stated in such form as to arrest attention, that unauthorized individuals have entered into communication with members of parliament and foreign ministers and officers in order to influence their conduct, in controversies with the United States, or to defeat the measures of our government. It ought to be known that such acts have been long prohibited by law.[9]

American Banana Co. v. United Fruit Co.[10] referred to the Logan Act as follows:

> No doubt in regions subject to no sovereign, like the high seas, or to no law that civilized countries would recognize as adequate, such countries may treat some relations between their citizens as governed by their own law and keep to some extent the old notion of personal sovereignty alive [citations omitted]. They go further, at times, and declare that they will punish anyone, subject or not, who shall do certain things if they can catch him, as in the case of pirates on the high seas. In cases immediately affecting national interests they may go further still and may make, and, if they get the chance, execute similar threats as to acts done within another recognized jurisdiction. An illustration from our statutes is found with regard to criminal correspondence with foreign governments. Rev. Stat., § 5335.[11]

[7] *See* Vagts, at 271.

[8] 30 Fed. Cas. 1049, 1050-51 (No. 18, 277).

[9] 30 Fed. Cas. 1042, 1046 (No. 18, 274).

[10] 213 U.S. 347 (1909).

[11] *Id.* at 356.

Burke v. Monumental Division, No. 52[12] was a case charging a union member with betraying the interests of his union at the time of negotiation between the union and a railroad during a labor dispute. The court compared the union's reaction toward the act of its member with Congress's feelings at the time of enactment of the Logan Act.

> [T]he plaintiff's conduct is characterized as "traitorous," and it is said that he has committed "moral perjury." This is strong language; but there is no reason to question that it is really meant, and that those responsible for its use believe it to be fully justified. The truth doubtless is that to them the Brotherhood and the roads appear to be almost distinct sovereignties. At a time when it is at grip with the companies, for a member to let one of the latter sue in his name, for the purpose of preventing the use by it of one of its most efficient means of warfare, does to them seem treasonable. Within the limits of their power, they are determined to punish any such proceeding. They feel about it as did Congress when in 1799 it enacted the so-called Logan Act ... making it a crime for any citizen to have intercourse with a foreign government with intent to defeat the measures of his own.[13]

United States v. Bryan[14]refers to 18 U.S.C. § 5, which is the predecessor of 18 U.S.C. § 953:

> That the subject of un-American and subversive activities is within the investigating power of the Congress is obvious. Conceivably, information in this field may aid the Congress in legislating concerning any one of many matters, such as correspondence with foreign governments....[15]

United States v. Peace Information Center[16] held that Congress had the power to enact the Foreign Agents Registration Act of 1938 under its inherent power to regulate external affairs as well as under its constitutional power to legislate concerning national defense and that the act is not subject to any constitutional infirmity. The court mentioned similarities between the Logan Act and the Foreign Agents Registration Act, and the language used appears to indicate that the court believed that the Logan Act, like the Foreign Agents Registration Act, is constitutional.

> Citizens of the United States are forbidden to carry on correspondence or intercourse with any foreign government with an intent to influence its measures or conduct in relation to any disputes or controversies with the United States.
>
> The Act under scrutiny in this case represents the converse of the last mentioned statute. The former deals with citizens of the United States who attempt to conduct correspondence with foreign governments. The latter affects agents of foreign principals who carry on certain specified activities in the United States. Both matters are equally within the field of external affairs of this country, and, therefore, within the inherent regulatory power of the Congress.[17]

[12] 286 F. 949 (D.Md. 1922).

[13] *Id.* at 952.

[14] 72 F. Supp. 58 (D.D.C. 1947).

[15] *Id.* at 62.

[16] 97 F. Supp. 255 (D.D.C. 1951).

[17] *Id.* at 261.

In *Martin v. Young*,[18] which concerned a petition for habeas corpus by a serviceman awaiting trial by a general court martial, the principal issue was whether the petitioner could be tried in a civil court for the offense charged against him by the Army. A part of the specification stated:

> [That petitioner while interned in a North Korean prisoner of war camp, did] without proper authority, wrongfully, unlawfully, and knowingly collaborate, communicate and hold intercourse, directly and indirectly, with the enemy by joining with, participating in, and leading discussion groups and classes conducted by the enemy reflecting views and opinions that the United Nations and the United States were illegal aggressors in the Korean conflict....[19]

The court stated that the conduct described in the specification violated at least three criminal statutes under which the petitioner could be tried in a civil court, one of which was the Logan Act, and granted the petition. However, the Department of Justice did not prosecute Martin under the Logan Act.

Pennsylvania v. Nelson[20] held that the Smith Act,[21] which prohibits the knowing advocacy of the overthrow of the United States Government by force and violence, supersedes the enforceability of the Pennsylvania Sedition Act, which proscribes the same conduct. The reason given for the pre-emption is that the federal statutes touch a field in which the federal interest is so dominant that the federal system must be assured to preclude enforcement of state laws on the same subject. The Court mentioned that "[s]tates are barred by the Constitution from entering into treaties and by 18 U.S.C. § 953 from correspondence or intercourse with foreign governments with relation to their disputes or controversies with this Nation."[22]

Briehl v. Dulles[23] upheld certain Department of State regulations which provided that no passport shall be issued to members of the Communist Party. The court referred to other valid federal statutes which restrict persons in the area of foreign relations:

> We have statutes dealing with persons who act as agents of a foreign government, or those who have "correspondence" with a foreign government with intent to influence its measures in relation to disputes or controversies with our Government or to defeat the measures of the United States.[24]

In *Waldron v. British Petroleum Co.*[25] the plaintiff sued for triple damages under the Clayton Act for alleged conspiracy of the defendants to prevent the importation and sale by the plaintiff of Iranian oil. The defendants asserted that the plaintiff had obtained his contract through a series of violations of criminal statutes including the Logan Act. The court held that, in order to maintain this defense, the defendants would have to show that the plaintiff sought to thwart some clearly and unequivocally asserted policy measures of the United States instead of merely statements of

[18] 134 F. Supp. 204 (N.D. Cal. 1955).

[19] *Id.* at 207.

[20] 350 U.S. 497 (1955).

[21] 18 U.S.C. § 2385.

[22] *Id.* at 516, fn 5.

[23] 248 F.2d 561 (D.C. Cir. 1957).

[24] *Id.* at 587.

[25] 231 F. Supp. 72 (S.D.N.Y. 1964).

opinion, attitude, and belief of government officials. The defendants were unable to show this. Further, the court noted that:

> Another infirmity in defendants' claim that plaintiff violated the Logan Act is the existence of a doubtful question with regard to the constitutionality of that statute [Logan Act] under the Sixth Amendment. That doubt is engendered by the statute's use of the vague and indefinite terms, "defeat" and "measures" [citation omitted]. Neither of these words is an abstraction of common certainty or possesses a definite statutory or judicial definition.
>
> Since, however, there are other grounds for disposing of this motion, it is not necessary to decide the constitutional question. Furthermore, any "ambiguity should be resolved in favor of lenity" [citation omitted].[26]

The court also indicates that, although Congress should perhaps eliminate the vagueness of the Logan Act, the act remains valid despite the lack of prosecutions under it.

> The Court finds no merit in plaintiff's argument that the Logan Act has been abrogated by desuetude. From the absence of reported cases, one may deduce that the statute has not been called into play because no factual situation requiring its invocation has been presented to the courts. Cf. Shakespeare, MEASURE FOR MEASURE, Act II, Scene ii ("The law hath not been dead, though it hath slept.")
>
> It may, however, be appropriate for the Court (Canons of Judicial Ethics, Judicial Canon 23) to invite Congressional attention to the possible need for amendment of Title 18 U.S.C. § 953 to eliminate this problem by using more precise words than "defeat" and "measures" and, at the same time, using language paralleling that now in § 954.[27]

United States v. Elliot[28] also refers to the Logan Act and reaffirms the statute as it is discussed in *Waldron*:

> Pertinent, too, is *Waldron* v. *British Petroleum Co.*, [citation omitted] wherein this court held vital a previously unenforced section of the Logan Act (18 U.S.C. § 953) promulgated in 1799.[29]

In *Agee v. Muskie*[30] suit was brought to revoke Agee's passport on the basis that his activities abroad were causing serious damage to the national security or foreign policy of the United States. In the Appendix to the case there are comments on various specific laws which Agee had allegedly violated. One of these was the Logan Act.

> Agee is quoted as stating that "in recent weeks" prior to December 23, 1979 he proposed to the "militants" in Iran (who obviously under 18 U.S.C. § 11 are a "faction and body of insurgents" constituting a "foreign government") that they should compel the United States to "exchange ... the C.I.A.'s files on its operations in Iran since 1950 for the Captive Americans" [citation omitted]. Such conduct violates 18 U.S.C. § 953 which prohibits any citizen of the United States from carrying on correspondence or intercourse with any foreign

[26] *Id.* at 89.

[27] *Id.* at 89, fn 30.

[28] 266 F. Supp. 318 (S.D.N.Y. 1967).

[29] *Id.* at 326.

[30] 629 F. 2d 80 (D.C. Cir. 1980), *rev'd sub nom. Haig* v. *Agee*, 453 U.S. 280 (1981), on grounds unrelated to the Logan Act reference.

> government (the Iranian terrorist faction) "with intent to influence [its] measures or conduct or [that] of any ... agent thereof [footnote omitted]. Agee's violation of this act with the Terrorists is self evident from his own uncontradicted statement.[31]

In *ITT World Communications, Inc. v. Federal Communications Commission*[32] the court found that the lower court had misread ITT's complaint concerning violation of the Logan Act.

> Under the Administrative Procedure Act, a party has standing to secure judicial review of any "agency action" that causes a "legal wrong" [footnote omitted]. The district court held that ITT has not suffered a legal wrong, reading its complaint solely to allege a violation of the Logan Act's prohibition of unauthorized negotiation with foreign governments [footnote omitted]. Because only the Department of State is aggrieved by violations of that criminal statute, the court reasoned, ITT's alleged injury is not legally cognizable.
>
> We respectfully conclude that the district court misread ITT's complaint. The gravamen of ITT's allegation is quite specific: "The activities of the FCC ... are unlawful and *ultra vires*, and in excess of the authority conferred on the Commission by the *Communications Act*" [footnote omitted]. Whether the complaint's two references to the Logan Act [footnote omitted] should be construed as an attempt to state a separate cause of action (as the Commission insists) or as mere illustrative matter not intended to assert a claim (as ITT argues), a cause of action under the Communications Act has clearly been alleged.[33]

In *Equal Employment Opportunity Commission v. Arabian American Oil Co.*,[34] suit was brought to determine whether Title VII of the Civil Rights Act of 1964[35] applied extraterritorially to regulate employment practices of United States employers who employed United States citizens abroad. The Court, in its holding that there was not sufficient evidence to indicate that the act was intended to apply abroad, stated:

> Congress' awareness of the need to make a clear statement that a statute applies overseas is amply demonstrated by the numerous occasions on which it has expressly legislated the extraterritorial application of a statute. See, *e.g.*, ... the Logan Act, 18 U.S.C. § 953 (applying Act to "any citizen ... wherever he may be ... ").[36]

United States v. DeLeon[37] concerned whether 8 U.S.C. Section 1326, which makes it a crime for an alien who has been previously deported to enter, attempt to enter, or be found in the United States unless certain conditions are met, applies to conduct occurring outside the United States. In holding that the statute does apply to conduct occurring outside the United States, the court stated:

> More important, assuming that the Convention [Convention on the Territorial Sea and the Contiguous Zone] also provides or ratifies a power to regulate certain conduct within the

[31] *Id.* at 112-113.

[32] 699 F. 2d 1219 (D.C. Cir. 1983), *rev'd on other grounds*, 466 U.S. 463 (1984).

[33] *Id.* at 1231.

[34] 499 U.S. 244 (1991).

[35] 42 U.S.C. §§ 2000e *et seq*.

[36] 499 U.S. at 258.

[37] 270 F.3d 90 (1st Cir. 2001).

> contiguous zone, that has a substantial adverse effect within the United States. That power was assumed to exist well before the Convention, e.g., Logan Act....[38]

In a series of reviews of a general court-martial, styled *United States* v. *Murphy,*[39] the appellant, who was charged with committing crimes abroad, urged the Logan Act as a basis for his being denied effective assistance of counsel.

> The appellant contends that he was denied effective assistance of counsel at a critical stage of the proceedings due to an erroneous interpretation of the Logan Act.... The Logan Act prohibits unauthorized negotiation with a foreign government.... In appellant's case, the Federal Republic of Germany declined to exercise criminal jurisdiction, in accordance with existing Status of Forces Agreements [footnote omitted]. The appellant's counsel decided, after personal research and consultation with other military lawyers, that he was prohibited from attempting to persuade the German authorities to exercise jurisdiction. The appellant now argues that his trial defense counsel's failure to negotiate with the Federal Republic of Germany, which does not allow capital punishment, denied him effective assistance of counsel. We disagree....[40]

In a 2010 case, *Strunk v. New York Province of the Society of Jesus*,[41] the plaintiff brought suit against New York City, New York State, and federal officials, asserting that government officials and agencies violated the Logan Act by acting as agents of a foreign government (presumably, the Vatican) in association with or under the direction of the Roman Catholic Church, the Society of Jesus, and the Sovereign Military Order of Malta. The plaintiff alleged that these circumstances caused him and the citizens of New York unspecified "collective spiritual and individual temporal injuries" and demanded a declaratory judgment and injunctive relief to enjoin the entities from conducting unspecified activities.

The United States District Court for the District of Columbia dismissed the action for lack of subject matter jurisdiction and plaintiff's lack of standing, stating:

> The Court concludes that plaintiff cannot establish an injury in fact, that he is without standing to bring his claims, and that this Court lacks jurisdiction to hear this matter.

The court stated that only the U.S. Department of State is aggrieved by a violation of the Logan Act and that only the U.S. Attorney General has the constitutional authority to conduct criminal litigation on behalf of the federal government.

Department of State References

A search of statements issued by the State Department concerning the Logan Act from 1975 onward has found at least two opinions. In these instances the department did not consider the activities in question to be inconsistent with the Logan Act. One opinion concerned the questioning of certain activities of Senators John Sparkman and George McGovern with respect to the government of Cuba. The department stated:

[38] *Id.* at 94.

[39] 50 M.J. 4 (1998); 36 M.J. 1137 (1993); and 30 M.J. 1040 (1990).

[40] 30 M.J. at 1047-1048.

[41] No. 09-1249, 2010 U.S. Dist. LEXIS 21957 (D.D.C. March 8, 2010).

> The clear intent of this provision [Logan Act] is to prohibit unauthorized persons from intervening in disputes between the United States and foreign governments. Nothing in section 953, however, would appear to restrict members of the Congress from engaging in discussions with foreign officials in pursuance of their legislative duties under the Constitution. In the case of Senators McGovern and Sparkman the executive branch, although it did not in any way encourage the Senators to go to Cuba, was fully informed of the nature and purpose of their visit, and had validated their passports for travel to that country.
>
> Senator McGovern's report of his discussions with Cuban officials states: "I made it clear that I had no authority to negotiate on behalf of the United States—that I had come to listen and learn...." (Cuban Realities: May 1975, 94th Cong., 1st Sess., August 1975). Senator Sparkman's contacts with Cuban officials were conducted on a similar basis. The specific issues raised by the Senators (e.g., the Southern Airways case; Luis Tiant's desire to have his parents visit the United States) would, in any event, appear to fall within the second paragraph of Section 953.
>
> Accordingly, the Department does not consider the activities of Senators Sparkman and McGovern to be inconsistent with the stipulations of Section 953.[42]

A 1976 statement by the Department of State concerned a letter written by Ambassador Robert J. McCloskey, Assistant Secretary of State for Congressional Relations, to Senator John V. Tunney in reply to a constituent's inquiry about a visit of former President Nixon to the People's Republic of China. The letter stated:

> Mr. Nixon's visit to the People's Republic of China was undertaken entirely in his capacity as a private United States citizen. In accordance with the expressed wishes of the Government of the People's Republic of China and as a normal matter of comity between governments, the U.S. Government permitted an aircraft from the People's Republic of China to land in California in connection with the visit. Aside from activities related to the Chinese special flights (including provision of an escort crew to insure safety of operations in U.S. airspace), the U.S. Government's role in the visit was limited to the provision by the Secret Service of personal protective services, as required by law, to the former President....
>
> It is the responsibility of the Department of Justice to make determinations of whether criminal statutes of this sort have been transgressed and whether individuals should be prosecuted under them. However, the Department of State is unaware of any basis for believing that Mr. Nixon acted with the intent prohibited by the Logan Act. In this connection, it should be noted that no one has ever been prosecuted under the Logan Act....[43]

In a number of instances, people have been alleged, often by political opponents, to have violated the Logan Act. For example, critics have suggested that Ross Perot's efforts to find missing American servicemen in Southeast Asia have violated the Logan Act. Critics alleged that former House Speaker Jim Wright violated the Logan Act in his relations with the Sandinista government. In 1984 while campaigning for the Democratic nomination for President, Reverend Jesse Jackson went to Syria to help in the release of a captured American military flyer and to Cuba and Nicaragua. The trips by Reverend Jackson occasioned comments from a number of people, most notably from President Reagan, that Reverend Jackson had violated the Logan Act. Other private citizens, such as Jane Fonda, have made trips which have been criticized as

[42] DIGEST OF UNITED STATES PRACTICE IN INTERNATIONAL LAW 1975, p. 750.

[43] DIGEST OF UNITED STATES PRACTICE IN INTERNATIONAL LAW 1976, pp. 75-76.

violative of the Logan Act. One of the most recent allegations involving a possible Logan Act violation focuses on a letter signed by 47 U.S. Senators to Iran suggesting that an agreement between the President and the Iranian leadership would be an executive agreement that another President or Congress would be able to abrogate.[44] There have apparently been no official sanctions taken in any of these instances.

Questions Raised Concerning a 2015 Senate Letter to Iranian Leadership

Commenters have raised questions about various issues associated with a 2015 letter signed by 47 U.S. Senators to Iran suggesting that negotiations about a nuclear deal between the President and the Iranian leadership would be an executive agreement that another President or Congress could abrogate. Three of these issues involve the constitutionality of the act, its application in this situation to Members of Congress, and its current viability.

With respect to the act's constitutionality, there is the above-discussed case, *United States v. Peace Information Center*, in which the court seemed to suggest that, because of similarities between the Logan Act and the Foreign Agents Registration Act, both acts are constitutional in that they "are equally within the field of external affairs of this country, and, therefore, within the inherent regulatory power of the Congress." Yet, there are commenters who continue to discuss whether the Logan Act is constitutional. For example, in a 1987 *Emory Law Journal* article, there is discussion about whether the act may infringe on rights involving freedom of speech and right to travel.[45]

The application of the act to Members of Congress is also a topic of discussion. In the above-discussed State Department statement concerning the questioning of Senators Sparkman and McGovern with respect to the government of Cuba, the department found that their activities did not violate the act and emphasized that nothing in the act "would appear to restrict members of the Congress in pursuance of their legislative duties under the Constitution." The State Department did not state that there is a general exemption from the act for Members of Congress; rather, it focused on the particular activities of these two Senators. Some commenters appear to believe that the 47 Senators signing the letter to Iran were acting outside permissible "pursuance of their legislative duties."[46] Others, however, believe that:

> [I]t could be argued that the letter's signatories do wield official U.S. authority and are federal officers in their capacity as U.S. senators.
>
> But even if they don't...a Logan Act prosecution would fall apart because of subsequent federal free speech cases that have taken a dim view of attempts to criminalize speech.[47]

[44] http://www.cotton.senate.gov/sites/default/files/150309%20Cotton%20Open%20Letter%20to%20Iranian%20Leaders.pdf.

[45] Kevin M. Kearney, Comment, *Private Citizens in Foreign Affairs: A Constitutional Analysis*, 36 EMORY L.J. 285 (1987).

[46] *See, e.g.*, E.J. Montini, *Did Senators Violate Federal Law with Iran Letter?*, located at: http://www.azcentral.com/story/ejmontini/2015/03/10/senators-letter-iran-president-obama-president-bush-iraq-maliki-logan-act/24710959/?hootPostID=d18760ac77dc7c1038f2e79c151c2470.

[47] Comments of Steve Vladeck, *quoted in Did 47 Republican Senators Break the Law in Plain Sight?, located at* (continued...)

The discussion of whether the act is currently viable may hinge on the fact that, despite its having been law for more than 200 years, no one has been prosecuted for violating it. Its viability may also involve constitutional issues, such as freedom of speech and right to travel, mentioned above, since these constitutional issues appear not to have been litigated with respect to the Logan Act. However, the act still remains law, and its viability should likely not be summarily dismissed.

Conclusion

Although it appears that there has never been a prosecution under the Logan Act, there have been several judicial references to it, indicating that the act has not been forgotten and that it is at least a potential point of challenge that has been used against anyone who without authority allegedly interferes in the foreign relations of the United States. There have been efforts to repeal the act, one of the most significant occurring in the late 1970s. For example, Senator Edward Kennedy proposed in the 95th Congress to delete the Logan Act from the bill to amend the United States criminal code.[48] Senator James Allen insisted on reenacting the act in exchange for promising not to prolong debate over the bill, and Senator Kennedy agreed to this. However, since the House was unable to consider the criminal reform bill in the 95th Congress, the possibility of deleting the act in a conference committee was eliminated. In early 2015, renewed interest in the act resulted from a letter sent to Iran by 47 U.S. Senators. It is possible that this interest will result in congressional consideration of whether the act should be repealed or retained.

Author Contact Information

Michael V. Seitzinger
Legislative Attorney
mseitzinger@crs.loc.gov, 7-7895

(...continued)

http://edition.cnn.com/2015/03/10/politics/tom-cotton-iran-letter-logan-act/index.html.

[48] S. 1437, 95th Cong., 2d Sess. (1978).

Strzok, Peter P. (CD) (FBI)

From: Strzok, Peter P. (CD) (FBI)
Sent: Wednesday, January 04, 2017 1:10 PM
To: Priestap, E. W. (CD) (FBI); Anderson, Trisha B. (OGC) (FBI); [redacted] OGC) (FBI); Page, Lisa C. (OGC) (FBI)
Attachments: RL33265.pdf

b6 -1
b7C -1

[redacted]

b5 -1, 2, 3

Strzok, Peter P. (CD) (FBI)

From: Strzok, Peter P. (CD) (FBI)
Sent: Wednesday, January 04, 2017 8:05 PM
To: Priestap, E. W. (CD) (FBI); Moffa, Jonathan C. (CD) (FBI) [redacted] OGC) (FBI); Page, Lisa C. (OGC) (FBI)
Subject: WSJ: Donald Trump Plans Revamp of Top U.S. Spy Agency - WSJ

b6 -1
b7C -1

Interesting. Also interesting Pompeo didn't attend the HPSCI brief...

http://www.wsj.com/articles/lawmakers-officials-frown-on-donald-trumps-dismissal-of-u-s-intelligence-1483554450

Donald Trump Plans Revamp of Top U.S. Spy Agency

President-elect works on restructuring Office of the Director of National Intelligence, tweets again his doubts that Russia hacked Democrats

By Damian Paletta and Julian E. Barnes

- Updated Jan. 4, 2017 6:35 p.m. ET

ENLARGE

President-elect Donald Trump, seen speaking in November in Hershey, Pa., is working on a plan to restructure the Office of the Director of National Intelligence, the nation's top spy agency, according to people familiar with the matter. *Photo: Evan Vucci/Associated Press*

WASHINGTON—President-elect Donald Trump, a harsh critic of U.S. intelligence agencies, is working with top advisers on a plan that would restructure and pare back the nation's top spy agency, people familiar with the planning said.

The move is prompted by his belief that the Office of the Director of National Intelligence has become bloated and politicized, these people said.

The planning comes as Mr. Trump has leveled a series of social-media attacks in recent months and the past few days against U.S. intelligence agencies, dismissing and mocking their assessment that Russia stole emails from Democratic groups and individuals and then provided them to WikiLeaks for publication in an effort to help Mr. Trump win the White House.

One of the people familiar with Mr. Trump's planning said advisers also are working on a plan to restructure the Central Intelligence Agency, cutting back on staffing at its Virginia headquarters and pushing more people out into field posts around the world. The CIA declined to comment.

ENLARGE

"The view from the Trump team is the intelligence world has become completely politicized," said the individual, who is close to the Trump transition. "They all need to be slimmed down. The focus will be on restructuring the agencies and how they interact."

In Twitter posts on Wednesday, Mr. Trump referenced an interview that WikiLeaks editor-in-chief Julian Assange gave to Fox News in which Mr. Assange denied Russia had been his source for the thousands of emails he published that had been stolen from Democratic organizations and Hillary Clinton advisers, including campaign manager John Podesta.

Mr. Trump tweeted: "Julian Assange said 'a 14 year old could have hacked Podesta'—why was DNC so careless? Also said Russians did not give him the info!"

Mr. Trump has drawn criticism from Democratic and Republican lawmakers and from intelligence and law-enforcement officials for praising Russian President Vladimir Putin, for criticizing U.S. intelligence agencies, and now for embracing Mr. Assange, long viewed with disdain by government officials and lawmakers.

"We have two choices: some guy living in an embassy on the run from the law...who has a history of undermining American democracy and releasing classified information to put our troops at risk, or the 17 intelligence agencies sworn to defend us," said Sen. Lindsey Graham (R., S.C.). "I'm going with them."

But for Mr. Trump and some supporters, the accusations that Russia hacked Democrats are seen as an effort to delegitimize his election.

Since the November election, Mr. Trump has published close to 250 Twitter posts. Of those, 11 have focused on Russia or the election-related cyberattacks. In each of those tweets, Mr. Trump either has praised Russian President Vladimir Putin—last month calling him "very smart"—or disparaged the investigation into the hacks.

This stands in sharp contrast to his posts on other issues and countries, such as North Korea or China, where his views on national-security risks line up more squarely with U.S. spy agencies.

The Office of the Director of National Intelligence was established in 2004 in large part to boost coordination between intelligence agencies following the Sept. 11, 2001, terror attacks. Many Republicans have proposed cutting the DNI before, but this has proven hard to do, in part because its mission is focused on core national security issues, such as counterterrorism, nuclear proliferation and counterintelligence.

"The management and integration that DNI focuses on allows agencies like the CIA to better hone in on its own important work," said Rep. Adam Schiff (D., Calif.), the ranking Democrat on the House intelligence panel, who believes dismantling the DNI could lead to national security problems.

Mr. Trump's advisers say he has long been skeptical of the CIA's accuracy, and the president-elect often mentions faulty intelligence in 2002 and 2003 concerning Iraq's weapons programs. But his public skepticism about the Russia assessments has jarred analysts accustomed to more cohesion with the White House.

Top officials at U.S. intelligence agencies, as well as Republican and Democratic leaders in Congress, have said Russia orchestrated the computer attacks on the Democratic Party last year. President Barack Obama ordered the intelligence agencies to produce a report on the hacking operation, and he is expected to be presented with the findings on Thursday.

Russia has long denied any involvement in the hacking operation, though Mr. Putin has said releasing the stolen emails was a public service.

The heads of the CIA, Federal Bureau of Investigation and DNI James Clapper are scheduled to brief Mr. Trump on the findings on Friday. Mr. Trump tweeted late Tuesday that this meeting had been delayed and suggested that the agencies still needed time to "build a case" against Russia. White House officials said Mr. Trump will be briefed on the hacking report as soon as it is ready.

White House officials have been frustrated by Mr. Trump's confrontations with intelligence officials. "It's appalling," an official said. "No president has ever taken on the CIA and come out looking good."

Among those helping lead Mr. Trump's plan to revamp the intelligence agencies is his national security adviser, Lt. Gen. Michael Flynn, who had served as director of the Defense Intelligence Agency until he was pushed out by Mr. Clapper and others in 2014. Also involved in the planning is Rep. Mike Pompeo (R., Kan.), whom Mr. Trump selected as CIA director.

Gen. Flynn didn't respond to a request for comment on Wednesday, and Mr. Pompeo declined to comment.

Gen. Flynn and Mr. Pompeo share Mr. Trump's view that the intelligence community's position—that Russia tried to help his campaign—is an attempt to undermine his victory or say he didn't win, the official close to the transition said.

Gen. Flynn will lead the White House's National Security Council, giving him broad influence in military and intelligence decisions throughout the government. He is also a believer in rotating senior intelligence agencies into the field and reducing headquarters staff.

ENLARGE

The lobby of the CIA Headquarters Building in Langley, Va. Donald Trump's criticism of U.S. intelligence agencies' assessments of Russian involvement in cyberattacks has some lawmakers questioning his goals. *Photo: larry downing/Reuters*

Current and former intelligence and law-enforcement officials have reacted with a mix of bafflement and outrage to Mr. Trump's continuing series of jabs at U.S. spies.

"They are furious about it," said one former senior intelligence official, adding that a retinue of senior officials who thought they would be staying on in a Hillary Clinton administration now are re-evaluating their plans following Mr. Trump's election.

Current and former officials said it was particularly striking to see Mr. Trump quote Mr. Assange in tweets

Current and former officials said it was particularly striking to see Mr. Trump quote Mr. Assange in tweets.

"It's pretty horrifying to me that he's siding with Assange over the intelligence agencies," said one former law enforcement official.

Paul Pillar, a 28-year veteran of the CIA who retired in 2005, said he was disturbed by Mr. Trump's tweets and feared much of the intelligence community's assessments could be filtered through Gen. Flynn.

"I'm rather pessimistic," he said. "This is indeed disturbing that the president should come in with this negative view of the agencies, coupled with his habits on how he absorbs information and so on that don't provide a lot of hope for change."

—Carol E. Lee, Shane Harris and Siobhan Hughes contributed to this article.

Write to Damian Paletta at damian.paletta@wsj.com and Julian E. Barnes at julian.barnes@wsj.com

Strzok, Peter P. (CD) (FBI)

From: Strzok, Peter P. (CD) (FBI)
Sent: Wednesday, January 04, 2017 10:31 PM
To: Page, Lisa C. (OGC) (FBI) [redacted] (OTD) (FBI) b6 -1
Cc: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI) b7C -1
Subject: RE: The "list"

Yes she was in the meeting where [redacted] ame to HQ. We can ask her at the prep.session.

-------- Original message --------
From: "Page, Lisa C. (OGC) (FBI)" [redacted]
Date: 01/04/2017 10:05 PM (GMT-05:00) b6 -1
To: "Strzok, Peter P. (CD) (FBI)" [redacted] (OTD) (FBI)" b7C -1
[redacted] b7E -6
Cc: [redacted] (OGC) (FBI) [redacted] (OGC) (FBI)"
[redacted]
Subject: RE: The "list"

Happy to, though I don't recall if she was in the original conversations. Was she?

-------- Original message --------
From: "Strzok, Peter P. (CD) (FBI)" [redacted] b6 -1
Date: 01/04/2017 10:01 PM (GMT-05:00) b7C -1
To [redacted] (OTD) (FBI)" [redacted] "Page, Lisa C. (OGC) (FBI)" b7E -6
[redacted]
Cc [redacted] (OGC) (FBI)" [redacted] (OGC) (FBI)"
[redacted]
Subject: RE: The "list"

We all have a prep session tomorrow at 9. I'll grab Scott along with Bill afterwards and explain. Lisa, you think it would be worth including Jim or Trisha in that? Probably Trisha, right?

-------- Original message --------
From: [redacted] (OTD) (FBI) [redacted] b6 -1
Date: 01/04/2017 9:51 PM (GMT-05:00) b7C -1
To: "Page, Lisa C. (OGC) (FBI)" [redacted] "Strzok, Peter P. (CD) (FBI)" b7E -6
[redacted]
Cc [redacted] (OGC) (FBI)" [redacted] (OGC) (FBI)"
[redacted]
Subject: RE: The "list"

Perfect. That works for me and you can mention that OTD brought it to you. My initial recommendation was for the AD to reach out to you two, but I can only assume that message did not reach him.

Thanks for the assist. b6 -1
b7C -1
[redacted]

[redacted]

b6 -1
b7C -1

[redacted]
Operational Technology Division
Federal Bureau of Investigation
[redacted] - desk
- mobile

-------- Original message --------
From: "Page, Lisa C. (OGC) (FBI)" [redacted]
Date: 01/04/2017 9:46 PM (GMT-05:00)
To: [redacted] (OTD) (FBI)" [redacted] "Strzok, Peter P. (CD) (FBI)"
[redacted]
Cc: [redacted] (OGC) (FBI)" [redacted] OGC) (FBI)"
[redacted]
Subject: RE: The "list"

b6 -1
b7C -1
b7E -6

[redacted]

Why don't you let Pete or Bill or I reach out to the AD of Cyber to let him know how we got here. [redacted] it might then be worth [redacted]

b5 -1, 3
b6 -1
b7C -1

-------- Original message --------
From: [redacted] (OTD) (FBI) [redacted]
Date: 01/04/2017 9:32 PM (GMT-05:00)
To: "Strzok, Peter P. (CD) (FBI)" [redacted] "Page, Lisa C. (OGC) (FBI)"
[redacted]
Cc: [redacted] (OGC) (FBI)" [redacted] OGC) (FBI)"
[redacted]
Subject: The "list"

b6 -1
b7C -1
b7E -6

Pete/Lisa,
I hope you guys enjoyed the holidays. It is already back to the grind.

The AD of cyber is apparently bringing up the idea of [redacted]

[redacted] ust messaged me after being pinged by SF. He asked why this was coming up again, and he wants to talk to me about it next week. Any recommendation on how to deal with this? [redacted]

b5 -1, 3
b6 -1
b7C -1

Let me know what you think.

Thanks
[redacted]

[redacted]
Operational Technology Division
Federal Bureau of Investigation
[redacted] - desk
- mobile

b6 -1
b7C -1

Strzok, Peter P. (CD) (FBI)

From:	Strzok, Peter P. (CD) (FBI)
Sent:	Thursday, January 05, 2017 6:56 PM
To:	Page, Lisa C. (OGC) (FBI)
Subject:	FW: News article: The FBI Never Asked For Access To Hacked Computer Servers

From: Baker, James A. (OGC) (FBI)
Sent: Thursday, January 05, 2017 6:41 PM
To: Smith, Scott S. (PG) (FBI[redacted] Priestap, E. W. (CD) (FBI)[redacted]
Strzok, Peter P. (CD) (FBI)[redacted] Anderson, Trisha B. (OGC) (FBI)
[redacted] OGC) (FBI) [redacted]
Subject: Fwd: News article: The FBI Never Asked For Access To Hacked Computer Servers

b6 -1
b7C -1
b7E -6

Folks,

Is this article correct?

Thanks.

Jim

--

-------- Original message --------
From: [redacted] (OGC) (FBI)" [redacted]
Date: 01/05/2017 4:23 PM (GMT-05:00)
To: "Baker, James A. (OGC) (FBI)" [redacted] (CTD) (FBI)"
[redacted] (OGC) (FBI)" [redacted]
(OGC) (FBI)" [redacted] (OGC) (FBI)" [redacted]
[redacted] (OGC) (FBI)" [redacted]
Subject: News article: The FBI Never Asked For Access To Hacked Computer Servers

b6 -1
b7C -1
b7E -6

The FBI Never Asked For Access To Hacked Computer Servers

The Democratic National Committee tells BuzzFeed News that the bureau "never requested access" to the servers the White House and intelligence community say were hacked by Russia.

Ali Watkins BuzzFeed News Reporter

.

Dmitri Lovetsky / AP

WASHINGTON — The FBI did not examine the servers of the Democratic National Committee before issuing a report attributing the sweeping cyberintrusion to Russia-backed hackers, BuzzFeed News has learned.

Six months after the FBI first said it was investigating the hack of the Democratic National Committee's computer network, the bureau has still not requested access to the hacked servers, a DNC spokesman said. No US government entity has run an independent forensic analysis on the system, one US intelligence official told BuzzFeed News.

"The DNC had several meetings with representatives of the FBI's Cyber Division and its Washington (DC) Field Office, the Department of Justice's National Security Division, and U.S. Attorney's Offices, and it responded to a variety of requests for cooperation, but the FBI never requested access to the DNC's computer servers," Eric Walker, the DNC's deputy communications director, told BuzzFeed News in an email.

The FBI has instead relied on computer forensics from a third-party tech security company, CrowdStrike, which first determined in May of last year that the DNC's servers had been infiltrated by Russia-linked hackers, the U.S. intelligence official told BuzzFeed News.

"CrowdStrike is pretty good. There's no reason to believe that anything that they have concluded is not accurate," the intelligence official said, adding they were confident Russia was behind the widespread hacks.

The FBI declined to comment.

"Beginning at the time the intrusion was discovered by the DNC, the DNC cooperated fully with the FBI and its investigation, providing access to all of the information uncovered by CrowdStrike — without any limits," said Walker, whose emails were stolen and subsequently distributed throughout the cyberattack.

It's unclear why the FBI didn't request access to the DNC servers, and whether it's common practice when the bureau investigates the cyberattacks against private entities by state actors, like when the Sony Corporation was hacked by North Korea in 2014.

BuzzFeed News spoke to three cybersecurity companies who have worked on major breaches in the last 15 months, who said that it was "par for the course" for the FBI to do their own forensic research into the hacks. None wanted to comment on the record on another cybersecurity company's work, or the work being done by a national security agency.

The hack of the DNC servers and the subsequent release of purloined emails by WikiLeaks has become a Washington scandal of proportions perhaps not seen since the Watergate era. The hacks — part of what intelligence officials, the White House, and private sector analysts say was a broader Moscow-directed effort to influence the US election — were specifically designed to undercut democratic nominee Hillary Clinton's path to the presidency and bolster Donald Trump, according to CIA and FBI analysis.

analysis.

Trump has denied that analysis and mocked the US intelligence agencies that produced it. The president-elect is due to receive an in-depth briefing on the subject on Friday.

In a 13-page report made public the last week of December, the FBI and the Department of Homeland Security confirmed in a joint analysis that Russia was behind the widespread hacks, which targeted Democrats with the intention to manipulate the US election. But the analysis was attributed to broad intelligence across both public and private sectors. Nowhere in the report does it say that the government conducted its own computer forensics on the DNC servers.

"Public attribution of these activities to [Russian Intelligence Services] is supported by technical indicators from the U.S. Intelligence Community, DHS, FBI, the private sector, and other entities," the report says.

On the heels of the report's release, the White House expelled 35 Russian diplomats, sanctioned, among other things, two of Russia's premier intelligence agencies, and shut down access to two Russian diplomatic facilities in the US.

Sheera Frenkel contributed reporting to this story.

CORRECTION

The article has been updated to reflect that CrowdStrike first discovered Russia-backed hackers had infiltrated the DNC in May 2016. A previous version of the article incorrectly said the group first discovered it in March.

Strzok, Peter P. (CD) (FBI)

From: Strzok, Peter P. (CD) (FBI)
Sent: Thursday, January 05, 2017 7:36 PM
To: Page, Lisa C. (OGC) (FBI)

[redacted] I will let Bill relay tomorrow AM. b5 -1

Strzok, Peter P. (CD) (FBI)

From: Strzok, Peter P. (CD) (FBI)
Sent: Thursday, January 05, 2017 7:46 PM
To: Page, Lisa C. (OGC) (FBI)
Subject: Fwd: Unclassified report

Fyi

-------- Original message --------
From: "Strzok, Peter P. (CD) (FBI)"[redacted]
Date: 01/05/2017 7:46 PM (GMT-05:00)
To: "Priestap, E. W. (CD) (FBI)"[redacted]
Cc: "Boone, Jennifer C. (CD) (FBI)"[redacted] "Corsi, Dina M. (CD) (FBI)"
[redacted] Moffa, Jonathan C. (CD) (FBI)"[redacted]
Subject: Unclassified report

b6 -1
b7C -1
b7E -6

FBI sent approval to ODNI for unclassified version tonight at 7:03.

Strzok, Peter P. (CD) (FBI)

Subject:	[redacted] discussion b7E -4
Location:	Mike K's office
Start:	Friday, January 06, 2017 11:30 AM
End:	Friday, January 06, 2017 12:15 PM
Show Time As:	Tentative
Recurrence:	(none)
Meeting Status:	Not yet responded
Organizer:	Strzok, Peter P. (CD) (FBI)
Required Attendees:	Kortan, Michael P. (DO) (FBI); Herring, Jason V. (CD) (FBI); Quinn, Richard P. (DO) (FBI); [redacted] (OGC) (FBI); Page, Lisa C. (OGC) (FBI) b6 -1 b7C -1

Strzok, Peter P. (CD) (FBI)

Subject: [redacted] discussion b7E -4
Location: Mike K's office

Start: Friday, January 06, 2017 11:30 AM
End: Friday, January 06, 2017 12:15 PM

Recurrence: (none)

Meeting Status: Accepted

Organizer: Strzok, Peter P. (CD) (FBI)
Required Attendees: Kortan, Michael P. (DO) (FBI); Herring, Jason V. (CD) (FBI); Quinn, Richard P. (DO) (FBI); [redacted] (OGC) (FBI); Page, Lisa C. (OGC) (FBI)

b6 -1
b7C -1

Strzok, Peter P. (CD) (FBI)

From:	Strzok, Peter P. (CD) (FBI)
Sent:	Monday, January 09, 2017 9:47 AM
To:	[redacted] DO) (FBI); Page, Lisa C. (OGC) (FBI)
Cc:	Rybicki, James E. (DO) (FBI); Priestap, E. W. (CD) (FBI)
Subject:	USIC report

b6 -1
b7C -1

[redacted]/Lisa,
Per D's request on Friday, NYO received a single copy of the influence report from ODNI's [redacted] It is being maintained in the CD SAC's safe for PEOTUS/senior staff.
Pete

b6 -1, 2
b7C -1, 2

Strzok, Peter P. (CD) (FBI)

From: Strzok, Peter P. (CD) (FBI)
Sent: Monday, January 09, 2017 4:59 PM
To: Page, Lisa C. (OGC) (FBI)
Subject: FW: Senator Cotton Question

From: Anderson, Trisha B. (OGC) (FBI)
Sent: Monday, January 09, 2017 4:52 PM
To: Strzok, Peter P. (CD) (FBI)[redacted] b6 -1
Cc[redacted](OGC) (FBI)[redacted] b7C -1
b7E -6
Subject: FW: Senator Cotton Question

See the first question below. Do you have a few minutes to discuss?

From: Herring, Jason V. (CD) (FBI)
Sent: Monday, January 09, 2017 3:13 PM
To: Rybicki, James E. (DO) (FBI)[redacted]DO) (FBI) b6 -1
[redacted]DO) (FBI)[redacted]Baker, James A. (OGC) (FBI) b7C -1
[redacted] b7E -6
Cc: Beers, Elizabeth R. (DO) (FBI)[redacted]DO) (FBI)
[redacted]Anderson, Trisha B. (OGC) (FBI)[redacted]
[redacted](OGC) (FBI[redacted]
Subject: RE: Senator Cotton Question

Adding Trisha and[redacted]from NSLB... b6 -1

OCA will work through Trisha and[redacted] b7C -1

Jason

From: Rybicki, James E. (DO) (FBI)
Sent: Monday, January 09, 2017 2:06 PM
To:[redacted](DO) (FBI)[redacted]Herring, Jason V. (CD) (FBI) b6 -1
[redacted](DO) (FBI)[redacted]Baker, James A. (OGC) (FBI) b7C -1
[redacted] b7E -6
Cc: Beers, Elizabeth R. (DO) (FBI)[redacted](DO) (FBI)
[redacted]
Subject: RE: Senator Cotton Question

Thanks,[redacted]Can OCA run down the answers to those questions this afternoon and then pass them up for the Director? b6 -1 b7C -1

Thanks!

-------- Original message --------
From[redacted](DO) (FBI)[redacted]
Date: 1/9/17 2:03 PM (GMT-05:00)
To: "Herring, Jason V. (CD) (FBI)[redacted]
Cc: "Beers, Elizabeth R. (DO) (FBI[redacted](DO) (FBI)"
[redacted]"Rybicki, James E. (DO) (FBI)"[redacted]
Subject: Senator Cotton Question

b6 -1
b7C -1
b7E -6

Jason,

Senator Cotton wants to ask ECTR related questions tomorrow at the SSCI Hearing.

First, he wonders if ECTR would have helped with the current Russian CI issues/situation. He requested to get a heads up on which way the D would answer that beforehand.

Second, is ECTR still a priority for the FBI?

So far, everyone else on the Committee is pretty quiet. If I get any further intel, I will advise.

Thanks,

[redacted]

SSA[redacted]
FBI Office of Congressional Affairs

b6 -1
b7C -1

Strzok, Peter P. (CD) (FBI)

From: Strzok, Peter P. (CD) (FBI)
Sent: Monday, January 09, 2017 5:14 PM
To: Page, Lisa C. (OGC) (FBI)
Subject: FW: Senator Cotton Question

From: Anderson, Trisha B. (OGC) (FBI)
Sent: Monday, January 09, 2017 5:13 PM
To: Herring, Jason V. (CD) (FBI) [redacted] b6 -1
Cc: Beers, Elizabeth R. (DO) (FBI) [redacted] (OGC) (FBI) b7C -1
[redacted] Strzok, Peter P. (CD) (FBI [redacted] DO) (FBI) b7E -6
Subject: RE: Senator Cotton Question

Jason,

Dropping Jim B. and the Director's office folks for purposes of working through this (and adding Pete for CD's perspective). How about something like:

[redacted] b5 -1, 3

Thoughts from others?

Trisha

From: Herring, Jason V. (CD) (FBI)
Sent: Monday, January 09, 2017 3:13 PM
To: Rybicki, James E. (DO) (FBI) [redacted] DO) (FBI) b6 -1
[redacted] DO) (FBI [redacted] Baker, James A. (OGC) (FBI) b7C -1
b7E -6
Cc: Beers, Elizabeth R. (DO) (FBI [redacted] DO) (FBI)
[redacted] Anderson, Trisha B. (OGC) (FBI) [redacted]
[redacted] OGC) (FBI) [redacted]
Subject: RE: Senator Cotton Question

Adding Trisha and [redacted] from NSLB... b6 -1
b7C -1

OCA will work through Trisha and [redacted]

b6 -1
b7C -1

Jason

From: Rybicki, James E. (DO) (FBI)
Sent: Monday, January 09, 2017 2:06 PM
To: [redacted] (DO) (FBI) [redacted] Herring, Jason V. (CD) (FBI)
[redacted] (DO) (FBI) [redacted] Baker, James A. (OGC) (FBI)
Cc: Beers, Elizabeth R. (DO) (FBI) [redacted] (DO) (FBI)
[redacted]
Subject: RE: Senator Cotton Question

b6 -1
b7C -1
b7E -6

Thanks [redacted] Can OCA run down the answers to those questions this afternoon and then pass them up for the Director?

b6 -1
b7C -1

Thanks!

--

-------- Original message --------
From: [redacted] (DO) (FBI) [redacted]
Date: 1/9/17 2:03 PM (GMT-05:00)
To: "Herring, Jason V. (CD) (FBI)" [redacted]
Cc: "Beers, Elizabeth R. (DO) (FBI) [redacted] DO) (FBI)"
[redacted] "Rybicki, James E. (DO) (FBI)" [redacted]
Subject: Senator Cotton Question

b6 -1
b7C -1
b7E -6

Jason,

Senator Cotton wants to ask ECTR related questions tomorrow at the SSCI Hearing.

First, he wonders if ECTR would have helped with the current Russian CI issues/situation. He requested to get a heads up on which way the D would answer that beforehand.

Second, is ECTR still a priority for the FBI?

So far, everyone else on the Committee is pretty quiet. If I get any further intel, I will advise.

Thanks,

[redacted]

SSA [redacted]
FBI Office of Congressional Affairs

b6 -1
b7C -1

Strzok, Peter P. (CD) (FBI)

From: Strzok, Peter P. (CD) (FBI)
Sent: Monday, January 09, 2017 5:23 PM
To: Page, Lisa C. (OGC) (FBI)
Subject: New Clinton email files detail FBI-State tussle over Benghazi message

http://www.politico.com/story/2017/01/new-clinton-emails-fbi-state-233343

"The redaction lists 'interference with foreign relations as the rationale.' The crux of States [sic] argument is they know better what will impact foreign relations and there is no longer a government in place" in Libya, the unidentified FBI official wrote to Michelle Jupina, the FBI Assistant Director for Records Management. "The more appropriate rationale is sources and methods. While the email does not name the particular official, this might be deduced and, given the threat of violence in the region, any surmise could be fatal for whoever cooperated with us. State will say no one will know if it is redacted, but that is not how classification works."

The message shows Deputy Secretary of State for Management Patrick Kennedy intervened with the FBI to dispute the classification at least three times: in a May 14, 2015, call to International Operations Division chief Brian McCauley, at an in-person meeting at the State Department five days later and in a phone conversation with the head of FBI's Counterterrorism Division, Michael Steinbach.

The unnamed FBI author of the message to Jupina said Kennedy summoned various officials to State to discuss the review of 55,000 of Clinton emails requested under FOIA. At that meeting, Kennedy asked the FBI representative and a Justice Department FOIA official to "stay behind to discuss the FBI determination" on classification in the first batch of Clinton emails, the FBI email says.

An email from Steinbach said he turned down Kennedy's request that the information be withheld solely under a FOIA provision for protection of law enforcement sources, rather than by classifying it.

"I explained to Mr. Kennedy that to only exempt for (b)(7)(D) was not appropriate as the information in the two portions in question was classified at the Secret/NOFORN level," Steinbach wrote.

Even after that decision, the FBI got another high-level contact on the issue from State that same day, with Secretary of State John Kerry's chief of staff Jon Finer calling Jim Rybicki, then-deputy chief of staff to FBI Director James Comey.

"Finer...stated that he was not attempting to change [Steinbach's] classification decision, and said that he just wanted to make sure that FBI leadership was aware of the decision and the procedural process and media attention it would likely trigger," Rybicki wrote in an email to several colleagues. "I relayed back to the State Department that leadership is aware of the review process and decision."

Rybicki said Finer asked if the FBI could classify the information rather than State doing so at FBI's request. When the email was released, State officials said they were withholding it at FBI's request.

Strzok, Peter P. (CD) (FBI)

From: Strzok, Peter P. (CD) (FBI)
Sent: Tuesday, January 10, 2017 12:31 PM
To: [redacted] OGC) (FBI); Priestap, E. W. (CD) (FBI); Moffa, Jonathan C. (CD) (FBI); Page, Lisa C. (OGC) (FBI)
b6 -1
b7C -1
Subject: RE: MYE - Timeline re Statements

Thanks and will do

-------- Original message --------
From: [redacted] (OGC) (FBI)" [redacted]
Date: 01/10/2017 10:26 AM (GMT-05:00)
To: "Priestap, E. W. (CD) (FBI)" [redacted] "Moffa, Jonathan C. (CD) (FBI)" [redacted] "Strzok, Peter P. (CD) (FBI)" [redacted] "Page, Lisa C. (OGC) (FBI)" [redacted]
Subject: MYE - Timeline re Statements

b6 -1
b7C -1
b7E -6

All -
Trisha asked me to put together the attached chart re the meetings/discussions we had with (or without) the Director about his July statement and subsequent letters to Congress. In particular, we are highlighting discussions which we would assert are privileged. This will be provided to EOUSA to inform their representation of the FBI in the matter with OSC.

Please review the attached and check your notes, calendars, etc to see if I missed anything. We're hoping to get something to EOUSA by the end of the week, so I'd appreciate any feedback by Thursday.

Please let me know if you'd like to discuss.

Thanks,
[redacted]

[redacted]
Assistant General Counsel
National Security Law Branch
Office of the General Counsel
Federal Bureau of Investigation
[redacted]

b6 -1
b7C -1

Confidentiality Statement:
This message is transmitted to you by the Office of the General Counsel of the Federal Bureau of Investigation. The message, along with any attachments, may be confidential and legally privileged. If you are not the intended recipient of this message, please destroy it promptly without further retention or dissemination (unless otherwise required by law). Please notify the sender of the error by a separate e-mail or by calling [redacted]

Strzok, Peter P. (CD) (FBI)

From: Strzok, Peter P. (CD) (FBI)
Sent: Tuesday, January 10, 2017 2:42 PM
To: Page, Lisa C. (OGC) (FBI)
Subject: RE: RE:

Ha. I believe you. ☺

From: Page, Lisa C. (OGC) (FBI)
Sent: Tuesday, January 10, 2017 2:34 PM
To: Strzok, Peter P. (CD) (FBI) [redacted] b6 -1 b7C -1 b7E -6
Subject: RE:

I honestly don't know!

-------- Original message --------
From: "Strzok, Peter P. (CD) (FBI)" [redacted] b6 -1 b7C -1 b7E -6
Date: 01/10/2017 1:56 PM (GMT-05:00)
To: "Page, Lisa C. (OGC) (FBI)" [redacted]
Subject: RE:

Hi. Just called, but have to go into ANOTHER meeting. Btw, heard why [redacted] is here...not sure if you claimed ignorance on purpose... ;) b6 -1 b7C -1

-----Original Message-----
From: Page, Lisa C. (OGC) (FBI) b6 -1 b7C -1 b7E -6
Sent: Tuesday, January 10, 2017 1:01 PM
To: Strzok, Peter P. (CD) (FBI) [redacted]
Subject: RE:

On a call now; hopefully after.

-----Original Message-----
From: Strzok, Peter P. (CD) (FBI) b6 -1 b7C -1 b7E -6
Sent: Tuesday, January 10, 2017 1:00 PM
To: Page, Lisa C. (OGC) (FBI) [redacted]
Subject:

Hey are you going to be able to listen to the link [redacted] sent, even in the background? I know you're working on comments/response to the other thing - I just have my 1:00 Div mtg (with Jon and Jen) and none of us will be listening.... b6 -1 b7C -1

Peter P. Strzok II
Deputy Assistant Director, Branch I
Counterintelligence Division
[redacted] (O) b6 -1 b7C -1
(C)

Strzok, Peter P. (CD) (FBI)

From:	Strzok, Peter P. (CD) (FBI)
Sent:	Tuesday, January 10, 2017 3:25 PM
To:	Page, Lisa C. (OGC) (FBI)
Subject:	RE: CNN update

Can I maybe get a read out vis a vis relationship with Brits etc?

-------- Original message --------
From: "Page, Lisa C. (OGC) (FBI)" [redacted]
Date: 01/10/2017 3:20 PM (GMT-05:00)
To: "Strzok, Peter P. (CD) (FBI)" [redacted] "Priestap, E. W. (CD) (FBI)"
[redacted] "Moffa, Jonathan C. (CD) (FBI) [redacted]
Cc: "Boone, Jennifer C. (CD) (FBI) [redacted]
Subject: RE: CNN update

b6 -1
b7C -1
b7E -6

We have lots of details from kortan. He will brief at the 3:45.

-------- Original message --------
From: "Strzok, Peter P. (CD) (FBI)" [redacted]
Date: 01/10/2017 3:01 PM (GMT-05:00)
To: "Priestap, E. W. (CD) (FBI) [redacted] "Moffa, Jonathan C. (CD) (FBI)"
[redacted]
Cc: "Boone, Jennifer C. (CD) (FBI)" [redacted] "Page, Lisa C. (OGC) (FBI)"
[redacted]
Subject: CNN update

b6 -1
b7C -1
b7E -6

Per Rich, CNN to publish C material today between 4 and 5

Strzok, Peter P. (CD) (FBI)

From:	Strzok, Peter P. (CD) (FBI)
Sent:	Tuesday, January 10, 2017 3:33 PM
To:	Page, Lisa C. (OGC) (FBI)
Subject:	RE: Fwd:

thx

From: Page, Lisa C. (OGC) (FBI)
Sent: Tuesday, January 10, 2017 3:23 PM
To: Priestap, E. W. (CD) (FBI) [redacted] Strzok, Peter P. (CD) (FBI [redacted]
Subject: Fwd:

b6 -1
b7C -1
b7E -6

Fyi.

-------- Original message --------
From [redacted] (DO) (FBI)" [redacted]
Date: 01/10/2017 2:51 PM (GMT-05:00)
To: "McCabe, Andrew G. (DO) (FBI)" [redacted] "Kortan, Michael P. (DO) (FBI)" [redacted] "Page, Lisa C. (OGC) (FBI)" [redacted] "Bowdich, David L. (DO) (FBI)" [redacted]
Subject

b6 -1
b7C -1
b7E -6

FYI - Just got word that SSCI is just now moving into closed session. Thanks [redacted]

[redacted]
Deputy Chief of Staff
Office of the Director
[redacted]

b6 -1
b7C -1

Strzok, Peter P. (CD) (FBI)

From:	Strzok, Peter P. (CD) (FBI)
Sent:	Tuesday, January 10, 2017 6:37 PM
To:	Priestap, E. W. (CD) (FBI); Baker, James A. (OGC) (FBI); Moffa, Jonathan C. (CD) (FBI); Page, Lisa C. (OGC) (FBI)
Subject:	Mother Jones article

http://www.motherjones.com/politics/2017/01/fbi-information-investigation-trump-russia-wyden

Senate Intelligence Committee Member Suggests FBI Is Sitting on Information on Trump-Russia Ties

At a hearing, Sen. Ron Wyden pushed FBI Director James Comey to release it by Inauguration Day.

David CornJan. 10, 2017 2:54 PM

It was only a couple of questions in the middle of a hearing, but the queries posed to FBI Director James Comey by Sen. Ron Wyden (D-Ore.) during a Senate Intelligence Committee gathering on Tuesday afternoon had potentially explosive implications, because they suggested that Wyden believes the FBI has been sitting on information regarding ties between Donald Trump's inner circle and Russia.

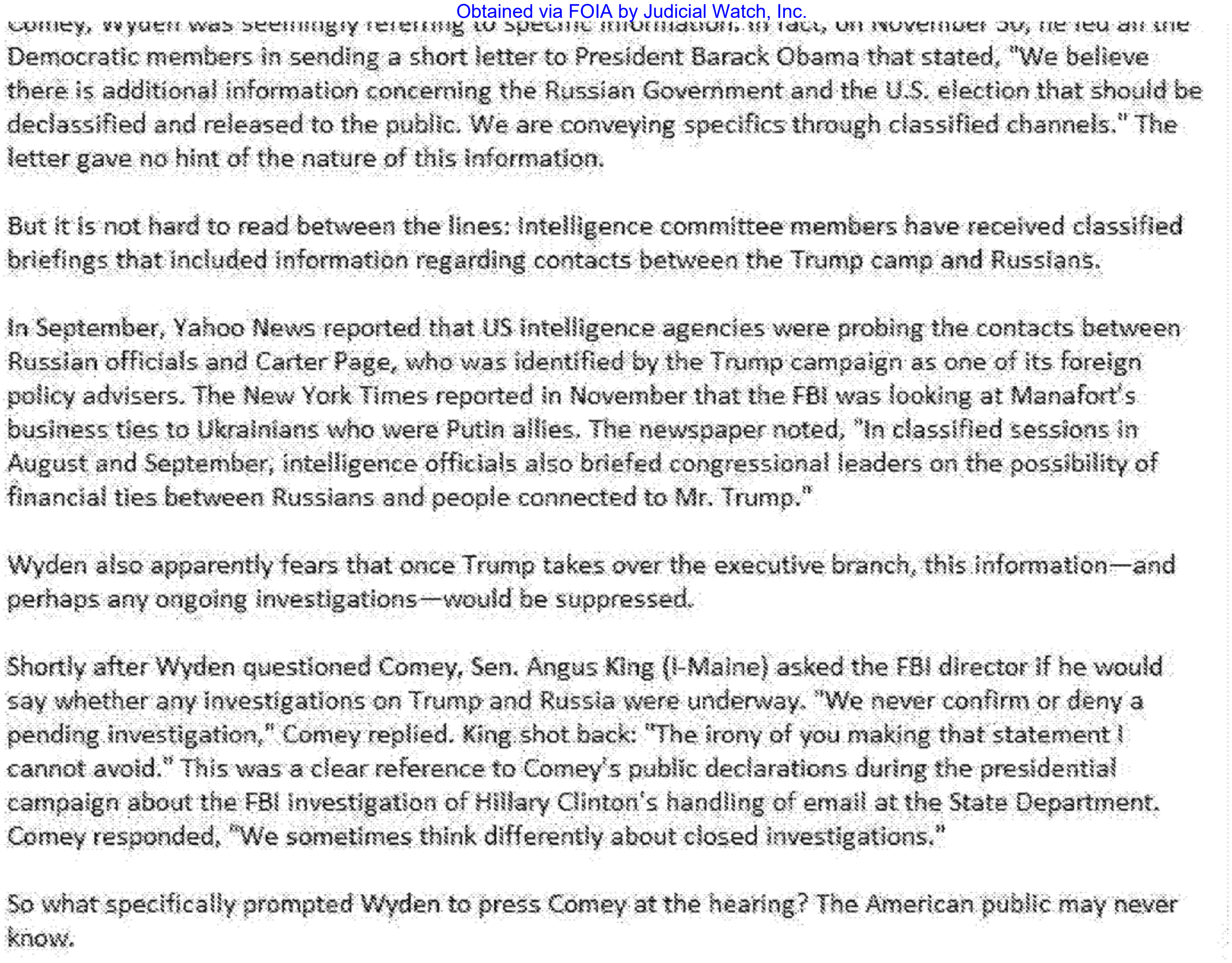
The hearing was focused on the intelligence community's recently released report concluding that Vladimir Putin's regime had mounted an extensive secret operation to influence the US election in order to help Trump. At the start of the hearing, outgoing Director of National Intelligence James Clapper emphasized that the report did not assess whether the Russian meddling had affected the outcome of the election. This was an indirect rebuke to Trump and his partisans, who have repeatedly said the report concluded the Russian intervention did not affect the results. Comey also noted that Russian hackers had targeted Republican targets but that the FBI had not found evidence that Moscow had penetrated the Trump campaign or current accounts of the Republican National Committee.

The most dramatic exchange came with Wyden's questions. He noted that several media outlets have reported that Trump campaign associates, including Paul Manafort, Trump's former campaign chairman, had maintained connections with Russians tied to Putin. He asked Comey, "Has the FBI investigated these reported relationships?" Comey answered, "I would never comment on investigations...in an open forum."

Wyden pushed Comey further. He asked whether the FBI chief would declassify information related to this matter and "release it to the American people" by January 20. No, Comey said, adding, "I can't talk about it."

Wyden then declared, "The American people have a right to know this." He continued: "If it doesn't happen by January 20, I'm not sure it's going to happen."

Wyden's line of questioning indicated that he believes (or knows) the FBI has collected information on Trump ties to Moscow. And Wyden is in a position to know. As a member of the committee, he can see classified material gathered by the FBI and other national security agencies. With these questions to Comey, Wyden was seemingly referring to specific information. In fact, on November 30, he led all the



Comey, Wyden was seemingly referring to specific information. In fact, on November 30, he led all the Democratic members in sending a short letter to President Barack Obama that stated, "We believe there is additional information concerning the Russian Government and the U.S. election that should be declassified and released to the public. We are conveying specifics through classified channels." The letter gave no hint of the nature of this information.

But it is not hard to read between the lines: Intelligence committee members have received classified briefings that included information regarding contacts between the Trump camp and Russians.

In September, Yahoo News reported that US intelligence agencies were probing the contacts between Russian officials and Carter Page, who was identified by the Trump campaign as one of its foreign policy advisers. The New York Times reported in November that the FBI was looking at Manafort's business ties to Ukrainians who were Putin allies. The newspaper noted, "In classified sessions in August and September, intelligence officials also briefed congressional leaders on the possibility of financial ties between Russians and people connected to Mr. Trump."

Wyden also apparently fears that once Trump takes over the executive branch, this information—and perhaps any ongoing investigations—would be suppressed.

Shortly after Wyden questioned Comey, Sen. Angus King (I-Maine) asked the FBI director if he would say whether any investigations on Trump and Russia were underway. "We never confirm or deny a pending investigation," Comey replied. King shot back: "The irony of you making that statement I cannot avoid." This was a clear reference to Comey's public declarations during the presidential campaign about the FBI investigation of Hillary Clinton's handling of email at the State Department. Comey responded, "We sometimes think differently about closed investigations."

So what specifically prompted Wyden to press Comey at the hearing? The American public may never know.

Strzok, Peter P. (CD) (FBI)

From: Strzok, Peter P. (CD) (FBI)
Sent: Tuesday, January 10, 2017 7:48 PM
To: Page, Lisa C. (OGC) (FBI); Priestap, E. W. (CD) (FBI); Moffa, Jonathan C. (CD) (FBI); Kortan, Michael P. (DO) (FBI); Baker, James A. (OGC) (FBI); [redacted] (OGC) (FBI); Rybicki, James E. (DO) (FBI); [redacted] (DO) (FBI)
Cc: McCabe, Andrew G. (DO) (FBI)
Subject: RE: Buzzfeed published some of the reports

b6 -1
b7C -1

Our internet system is blocking the site. I have the pdf via iPhone, but it's 25.6 MB. Comparing now. The set is only identical to what McCain had (it has differences from what was given to us by Corn and Simpson).

[redacted]

b5 -1, 3
b6 -1
b7C -1
b7E -6

Strzok, Peter P. (CD) (FBI)

From:	Strzok, Peter P. (CD) (FBI)
Sent:	Tuesday, January 10, 2017 8:23 PM
To:	Priestap, E. W. (CD) (FBI); Moffa, Jonathan C. (CD) (FBI); Baker, James A. (OGC) (FBI); Anderson, Trisha B. (OGC) (FBI)[redacted](OGC) (FBI); Kortan, Michael P. (DO) (FBI); Quinn, Richard P. (DO) (FBI); Page, Lisa C. (OGC) (FBI)
Subject:	Guardian: FBI chief given dossier by John McCain alleging secret Trump-Russia contacts

b6 -1
b7C -1

https://www.theguardian.com/us-news/2017/jan/10/fbi-chief-given-dossier-by-john-mccain-alleging-secret-trump-russia-contacts

Nb - "The Guardian has learned that the FBI applied for a warrant from the foreign intelligence surveillance (Fisa) court over the summer in order to monitor four members of the Trump team suspected of irregular contacts with Russian officials. The Fisa court turned down the application asking FBI counter-intelligence investigators to narrow its focus. According to one report, the FBI was finally granted a warrant in October, but that has not been confirmed, and it is not clear whether any warrant led to a full investigation."

FBI chief given dossier by John McCain alleging secret Trump-Russia contacts

Julian Borger in Washington

Tuesday 10 January 2017 19.29 EST Last modified on Tuesday 10 January 2017 20.03 EST

Senator John McCain passed documents to the FBI director, James Comey, last month alleging secret contacts between the Trump campaign and Moscow and that Russian intelligence had personally compromising material on the president-elect himself.

The material, which has been seen by the Guardian, is a series of reports on Trump's relationship with Moscow. They were drawn up by a former western counter-intelligence official, now working as a private consultant.

The Guardian has not been able to confirm the veracity of the documents' contents, and the Trump team has consistently denied any hidden contacts with the Russian government.

But an official in the US administration who spoke to the Guardian described the source who wrote the intelligence report as consistently reliable, meticulous and well-informed, with a reputation for having extensive Russian contacts.

Some of the reports - which are dated from 20 June to 20 October last year - also proved to be prescient, predicting events that happened after they were sent.

One report, dated June 2016, claims that the Kremlin has been cultivating, supporting and assisting Trump for at least five years, with the aim of encouraging "splits and divisions in western alliance".

It claims that Trump had declined "various sweetener real estate deals offered him in Russia" especially in developments linked to the 2018 World Cup finals but that "he and his inner circle have accepted a regular flow of intelligence from the Kremlin, including on his Democratic and other political rivals."

Most explosively, the report alleges: "FSB has compromised Trump through his activities in Moscow sufficiently to be able to blackmail him."

CNN reported on Tuesday that the FBI was still investigating the credibility of the documents but added that the intelligence chiefs had included a summary of the material in a secret briefing on Russian interference in the election delivered last week to Barack Obama and Donald Trump.

The emergence of the documents is potentially explosive, 10 days before Trump's inauguration and on the eve of his first planned press conference since July last year.

Despite glowing references from US and foreign officials who have worked with the source, there are some errors in the reports. One describes the Moscow suburb of Barvikha as "reserved for the residences of the top leadership and their close associates", but although it is a very expensive neighbourhood, there are no restrictions on who can own property there. The document also misspells the name of a Russian banking corporation.

The FBI does not normally make any comment on ongoing counter-intelligence investigations but was under increasing pressure from Democrats and some Republicans to act before the inauguration, particularly because of Comey's announcement of a continuing investigation into Hillary Clinton's email server 11 days before the election, which many of her supporters believe cost her the presidency.

The reports were initially commissioned as opposition research during the presidential campaign, but its author was sufficiently alarmed by what he discovered to send a copy to the FBI. It is unclear who within the organisation they reached and what action the bureau took. The former Democratic Senate leader, Harry Reid, has lambasted Comey for publicising investigations into Hillary Clinton's private server, while allegedly sitting on "explosive" material on Trump's ties to Russia.

Another Democratic senator, Ron Wyden, questioned Comey insistently at a Senate intelligence committee hearing on Tuesday on whether the FBI was pursuing leads on Trump campaign contacts with Russia.

"Has the FBI investigated these reported relationships?" Wyden asked.

Comey replied: "I would never comment on investigations ... in a public forum.

The Guardian can confirm that the documents reached the top of the FBI by December. Senator John McCain, who was informed about the existence of the documents separately by an intermediary from a western allied state, dispatched an emissary overseas to meet the source and then decided to present the material to Comey in a one-on-one meeting on 9 December, according to a source aware of the meeting. The documents, which were first reported on last year by Mother Jones, are also in the hands of officials in the White House.

McCain is not thought to have made a judgment on the reliability of the documents but was sufficiently impressed by the source's credentials to feel obliged to pass them to the FBI.

The Senate armed services committee, which Senator McCain chairs, launched an inquiry last week into Russian cyber-attacks during the election, and the intelligence services are due to complete a final assessment of Russian electoral meddling for President Obama this week.

Russian intelligence allegedly gathered compromising material from his stay in Moscow in November 2013, when he was in the city to host the Miss Universe pageant.

Another report, dated 19 July last year said that Carter Page, a businessman named by Trump as one of his foreign policy advisers, had held a secret meeting that month with Igor Sechin, head of the Rosneft state-owned oil company and a long-serving lieutenant of Vladimir Putin. Page also allegedly met Igor Divyekin, an internal affairs official with a background in intelligence, who is said to have warned Page that Moscow had "kompromat" (compromising material) on Trump.

Two months later, allegations of Page's meetings surfaced in the US media, attributed to intelligence sources, along with reports that he had been under FBI scrutiny.

Page, a vociferous supporter of the Kremlin line, was in Moscow in July to make a speech decrying western policy towards Russia. At the time he declined to say whether he had been in contact with Russian officials, but in September he rejected the reports as "garbage".

The Guardian has learned that the FBI applied for a warrant from the foreign intelligence surveillance (Fisa) court over the summer in order to monitor four members of the Trump team suspected of irregular contacts with Russian officials. The Fisa court turned down the application asking FBI counter-intelligence investigators to narrow its focus. According to one report, the FBI was finally granted a warrant in October, but that has not been confirmed, and it is not clear whether any warrant led to a full investigation.

A month after Trump's surprise election victory, Page was back in Moscow saying he was meeting with "business leaders and thought leaders", dismissing the FBI investigation as a "witch-hunt" and suggesting the Russian hacking of the Democratic Party alleged by US intelligence agencies, could be a false flag operation to incriminate Moscow.

Another of the reports compiled by the former western counter-intelligence official in July said that members of Trump's team, which was led by campaign manager Paul Manafort (a former consultant for pro-Russian politicians in Ukraine), had knowledge of the DNC hacking operation, and in return "had agreed to sideline Russian intervention in Ukraine as a campaign issue and to raise US/Nato defence commitments in the Baltics and Eastern Europe to deflect attention away from Ukraine".

A few days later, Trump raised the possibility that his administration might recognise Russia's annexation of Crimea and openly called on Moscow to hack Hillary Clinton's emails.

In August, officials from the Trump campaign intervened in the drafting of the Republican party platform, specifically to remove a call for lethal assistance to Ukraine for its battle against Moscow-backed eastern rebels.

Manafort stepped down in August as campaign manager and the campaign steadily distanced itself from Page. However, Trump's praise of Putin and defence of Moscow's actions in Ukraine and Syria remained one of the few constants in his campaign talking points.

Manafort has denied secret links with Moscow calling the allegation "an outrageous smear being

Manafort has denied secret links with Moscow calling the allegation "an outrageous smear being driven by Harry Reid and the Clinton campaign".

Since then, Trump has consistently cast doubt on Russian culpability for hacking the Democratic National Committee, defying a consensus of 17 national intelligence agencies. After Obama deported 35 Russian diplomats in retaliation for Moscow's intervention, Trump praised Putin for not carrying out tit-for-tat deportations of US diplomats. "I always knew he was very smart," he tweeted.

An FBI spokesman declined to comment after the CNN report.

Peter P. Strzok II
Deputy Assistant Director, Branch I
CounterIntelligence Division
[redacted] (O)
(C)

b6 -1
b7C -1