# National Security Council

~~TOP SECRET~~

**Document Referral**

## Memorandum For:

Name: (b)(3)
Agency: DNI
Address:

Package Number: 4416004907
Action Date: 12/2/2016 11:50:40 AM

## Document Description:

To: PRESIDENT
From: WYDEN, RON HEINRICH, MARTIN REED, JACK KING, ANGUS WARNER, MARK HIRONO, MAZIE MIKULSKI, BARBARA
Date: 11/29/2016
Subject: LETTER FROM SENATORS WYDEN ET AL RE DECLASSIFYING INFORMATION REGARDING RUSSIAN INTERFERENCE IN 2016 U.S. ELECTION

Action Required: DIRECT REPLY / FURNISH INFO COPY
Due Date: 12/09/2016
Comments: Please reply on behalf of the President. Obtain NSC clearance before returning response to the Hill. Thank you.

**For:** Corey Nightengale
Director of Records Management

## CLASSIFICATION:

~~TOP SECRET~~

Please Return Signed and Dated Receipt to:
NSC Records Management
Room 5013, NEOB
Washington, D.C. 20504
or fax to(202) 456-9230

~~TOP SECRET//(b)(3) //SI//NOFORN~~

# United States Senate

SELECT COMMITTEE ON INTELLIGENCE
WASHINGTON, DC 20510-6475

November 29, 2016

The President
The White House
1600 Pennsylvania Avenue, NW
Washington, DC 20500

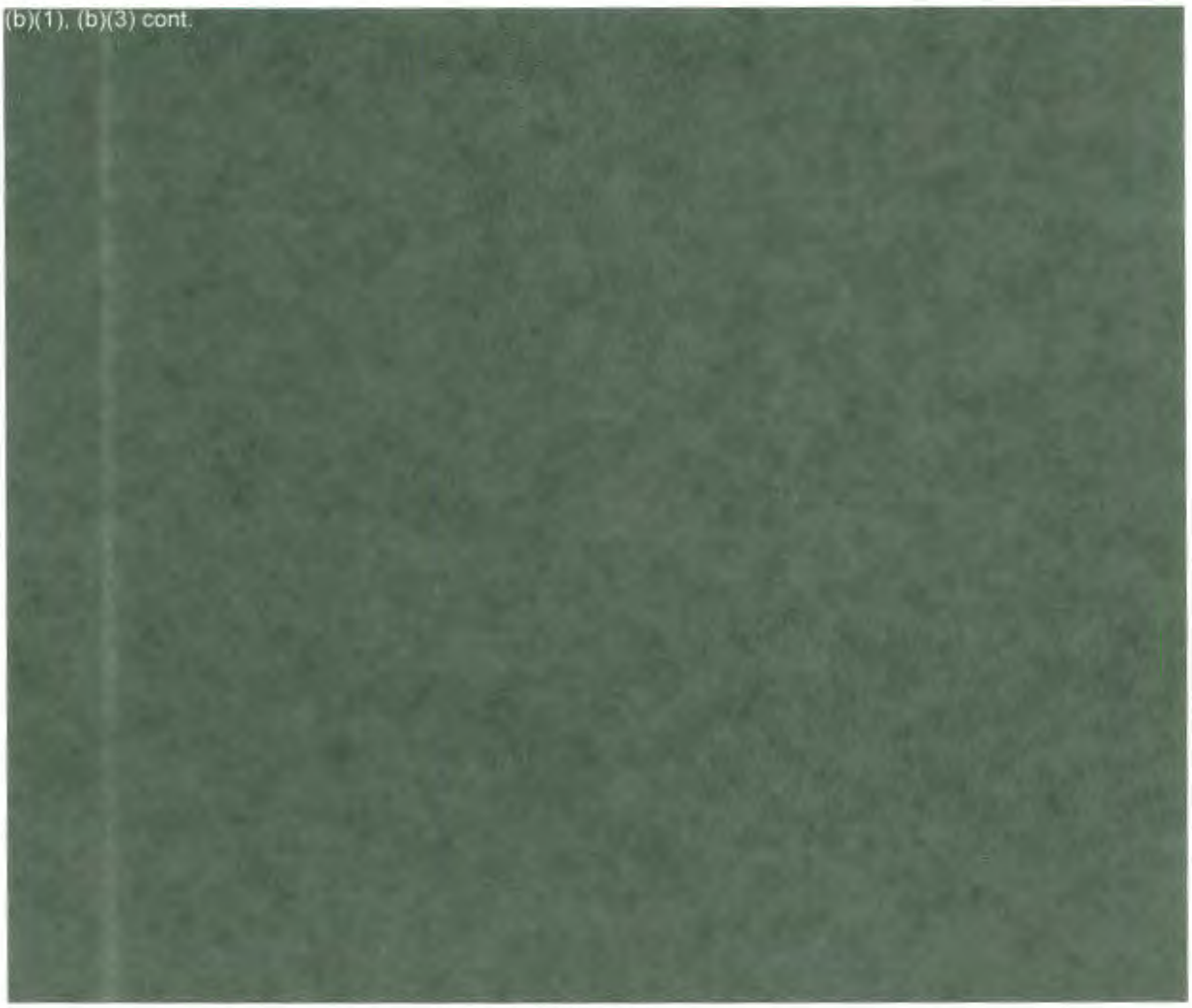
SSCI# 2016-3775

Dear Mr. President:

We write to request that, to the extent possible, you declassify and release to the public additional information related to the Russian Government and the U.S. election. Specifically, we have serious concerns about information recently provided to the Senate Select Committee on Intelligence regarding Russian Active Measures and election related cyber activity associated with the Russian intelligence services. Despite the broad national interest in this topic, this new information has not been provided to the American people. Accordingly, we request the declassification and release of the information enclosed in quotations below.


~~TOP SECRET//(b)(3) //SI//NOFORN~~

(b)(1), (b)(3) cont.



In addition, on November 7, 2016, the FBI made the following assessment in a summary of 2016 general election related cyber activity within the United States:

(b)(1), (b)(3), (b)(7)(A), (b)(7)(E)

(b)(3), (b)(7)(A), (b)(7)(E) cont.

[redacted]

Thank you for your attention to this important matter.

Sincerely,

Ron Wyden

Jack Reed

Angus King

Barbara Mikulski

Mark R Warner

# ENCLOSURE

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

JAN 27 2017

The Honorable Richard J. Durbin
United States Senate
Washington DC, 20510

Dear Senator Durbin:

Thank you for your letter to President Obama on 13 December 2016 requesting a National Intelligence Estimate regarding Russian efforts to manipulate the recent U.S. Presidential election. President Obama asked former Director of National Intelligence (DNI) Clapper to respond on his behalf.

The Office of the DNI (ODNI) shares your concerns regarding Russian actions in the run-up to the election. The Intelligence Community (IC), at the President's request, completed a comprehensive review of all intelligence related to Russian efforts to influence the recent Presidential election. That report, an Intelligence Community Assessment entitled *Assessing Russian Activities and Intentions in Recent US Elections,* was delivered to the Senate in both classified and unclassified formats on 6 January 2017.

The Department of Homeland Security and ODNI also issued an unprecedented joint public statement on 7 October 2016 assessing that the Russian Government directed the recent compromises of e-mails from U.S. persons and institutions, including from the Democratic National Committee and other U.S. political organizations. The IC also furnished a coordinated, unclassified assessment of these threats to Federal partners with responsibility for engaging with state, local, tribal, and territorial authorities on cybersecurity matters.

Thank you for your interest in this important matter. If you have any further questions, please contact Ms. Deirdre M. Walsh, Director of Legislative Affairs, at (703) 275-2474.

Sincerely,

Michael P. Dempsey

Michael P. Dempsey
Acting Director of National Intelligence

Enclosure:
1. National Intelligence Council Assessment: Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution

The Honorable Richard J. Durbin

cc: The Honorable Patrick Leahy
The Honorable Ben Cardin
The Honorable Al Franken
The Honorable Brian Schatz
The Honorable Gary Peters
The Honorable Tom Udall
The Honorable Robert P. Casey, Jr.
The Honorable Edward Markey

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

JAN 27 2017

The Honorable Ron Wyden
United States Senate
Washington DC, 20510

Dear Senator Wyden:

Thank you for your letter to President Obama on 29 November 2016 regarding Russian activities and intentions during the recent U.S. Presidential election. President Obama asked former Director of National Intelligence (DNI) Clapper to respond on his behalf.

The Office of the DNI (ODNI) shares your concerns regarding Russian actions in the run-up to the election. The Intelligence Community (IC), at the President's request, completed a comprehensive review of all intelligence related to Russian efforts to influence the recent Presidential election. That report, an IC Assessment entitled *Assessing Russian Activities and Intentions in Recent US Elections,* was delivered to the Senate in both classified and unclassified formats on 6 January 2017.

The Department of Homeland Security and ODNI also issued an unprecedented joint public statement on 7 October 2016 assessing that the Russian Government directed the recent compromises of e-mails from U.S. persons and institutions, including from the Democratic National Committee and other U.S. political organizations. The IC also furnished a coordinated, unclassified assessment of these threats to Federal partners with responsibility for engaging with state, local, tribal, and territorial authorities on cybersecurity matters. The briefings former DNI Clapper provided the week of 9 January 2017 were intended to provide additional insights and an opportunity for an interactive dialogue.

Thank you for your interest in this important matter. If you have any further questions, please contact Ms. Deirdre M. Walsh, Director of Legislative Affairs, at (703) 275-2474.

Sincerely,

Michael P. Dempsey
Acting Director of National Intelligence

Enclosure:
1. National Intelligence Council Assessment: Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution

The Honorable Ron Wyden

cc: The Honorable Dianne Feinstein
The Honorable Mark Warner
The Honorable Martin Heinrich
The Honorable Mazie Hirono
The Honorable Jack Reed
The Honorable Angus King

The U.S. Intelligence Community (USIC) is confident that the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations. The recent disclosures of alleged hacked e-mails on sites like DCLeaks.com and WikiLeaks and by the Guccifer 2.0 online persona are consistent with the methods and motivations of Russian-directed efforts. These thefts and disclosures are intended to interfere with the US election process. Such activity is not new to Moscow—the Russians have used similar tactics and techniques across Europe and Eurasia, for example, to influence public opinion there. We believe, based on the scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorized these activities.

Some states have also recently seen scanning and probing of their election-related systems, which in most cases originated from servers operated by a Russian company. However, we are not now in a position to attribute this activity to the Russian Government. The USIC and the Department of Homeland Security (DHS) assess that it would be extremely difficult for someone, including a nation-state actor, to alter actual ballot counts or election results by cyber attack or intrusion. This assessment is based on the decentralized nature of our election system in this country and the number of protections state and local election officials have in place. States ensure that voting machines are not connected to the Internet, and there are numerous checks and balances as well as extensive oversight at multiple levels built into our election process.

Nevertheless, DHS continues to urge state and local election officials to be vigilant and seek cybersecurity assistance from DHS. A number of states have already done so. DHS is providing several services to state and local election officials to assist in their cybersecurity. These services include cyber "hygiene" scans of Internet-facing systems, risk and vulnerability assessments, information sharing about cyber incidents, and best practices for securing voter registration databases and addressing potential cyber threats. DHS has convened an Election Infrastructure Cybersecurity Working Group with experts across all levels of government to raise awareness of cybersecurity risks potentially affecting election infrastructure and the elections process. Secretary Johnson and DHS officials are working directly with the National Association of Secretaries of State to offer assistance, share information, and provide additional resources to state and local officials.

# Background Questions

***What activities related to the US election does the USIC attribute to Russia?***

- The IC has high confidence in its attribution of the intrusions into the DNC and DCCC, based on the forensic evidence identified by a private cyber-firm and the IC's own review and understanding of cyber activities by the Russian Government.

***What about the disclosures that occurred after the DNC and DCCC intrusions?***

The U.S. Intelligence Community (USIC) is confident that the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations. At least some of the disclosures, including the disclosures of DNC and DCCC documents by Guccifer 2.0, DCLeaks, and WikiLeaks from June to August 2016, are consistent with the methods and motivations of Russian-directed efforts, thus suggesting Moscow is at least providing the information or is possibly directly responsible for the leaks.

- The disclosure of White House e-mails by DCLeaks also appears to be consistent with tactics and motivations of the Russian Government.

- Similarly, the disclosures of medical information from the World Anti-Doping Agency by a hacker group calling itself "Fancy Bear" are consistent with the cyber tactics and motivations of the Russian Government.

***How did the US IC attribute the DNC and DCCC intrusions to the Russian Government?***

- The IC independently observed technical activity that is consistent with the forensic evidence identified by a private cyber-firm and is consistent with our general understanding of cyber activities by the Russian Government.

***Does the USIC believe additional Russian action to interfere with our elections is imminent?***

- We expect that Russia will continue its efforts up to Election Day.

***Has the USIC concluded that Russia is behind the "Shadow Brokers" disclosures?***

- We are not in a position to comment on Shadow Brokers at this time.

***Was Hal Martin, the recently arrested former NSA contractor, part of this Russia-sponsored effort?***

- We are not able to comment on ongoing criminal investigations, so we would refer you to the Department of Justice.

***Do you assess that Putin ordered these operations?***

- We believe that authorization to conduct these operations could only have come from the most senior levels of the Russian Government.

***Has the US concluded that Russia is responsible for the intrusions into state election systems?***

- We are not definitively attributing the intrusions into state elections systems to the Russian Government, but the fact that they are consistent with Russian motivations and intent behind the DNC and DCCC intrusions, strongly suggests that Russia is responsible.

***Is Russia trying to alter the outcome of the US election?***

- The Kremlin probably expects that publicity surrounding the disclosures will raise questions about the integrity of the election process and would undermine the legitimacy of the President-elect.

***What is the USG doing about this?***

- The American public and our democracy are resilient to foreign attempts to manipulate public opinion. The U.S. Government is committed to ensuring a secure election process and has robust capabilities to detect efforts to interfere with our elections.

- The President has made it clear that we will take action to protect our interests, including in cyberspace, and we will do so at a time and place of our choosing. Consistent with the practice we have adopted in the past, the

public should not assume that they will necessarily know what actions have been taken or what actions we will take.

***What options are you considering for your response?***

- We are not going to discuss potential responses except to say that as we implement our responses, some responses you may see, and others you may not.

***Why is the USG publicly attributing these actions now? Why didn't the USG attribute this sooner?***

- In this instance, we have applied the framework we have used in the past—the IC and FBI worked together to evaluate information gathered through intelligence sources, FBI investigations, and other sources in order to determine attribution. As the IC gathered new information, it was able to reach higher degrees of confidence about which actors are responsible and then determine what could be disclosed publicly, consistent with law enforcement equities, while appropriately protecting sources and methods.

- We also worked as quickly as possible to release as much information as possible in order to provide state and local officials sufficient time to fortify their infrastructure.

***When was the President apprised of this conclusion?***

- The President has been regularly updated on the analysis and the IC's conclusions.

***Is the Russian effort intended to assist the Trump campaign?***

- Whatever the Russian Government's motivation, its interference is a source of concern.

***The U.S. Government does not make attribution determinations very often. Does this mean you have changed your position on attribution?***

- As the IC gathered new information, it was able to reach higher degrees of confidence about which actors are responsible and then determine what

could be disclosed publicly, while appropriately protecting sources and methods.

- Publicly identifying those actors is a step that the government considers when we have confidence in the attribution and can make the information public, consistent with U.S. national security interests, including the protection of sources and methods, and when doing so advances U.S. national interests.

***What is DHS doing to help state and local governments raise their cybersecurity protections ahead of the elections?***

- DHS is providing several services to state and local election officials to assist in their cybersecurity. These include cyber "hygiene" scans of Internet-facing systems, risk and vulnerability assessments, information sharing about cyber incidents, and best practices for securing voter registration databases and addressing potential cyber threats. As of October 6, more than half of the states have contacted DHS and are in discussions about receiving one or more of these services.

- DHS has convened an Election Infrastructure Cybersecurity Working Group with experts across all levels of government to raise awareness of cybersecurity risks potentially affecting voting infrastructure and the elections process.

- Secretary Johnson and DHS officials are working directly with the National Association of Secretaries of State to offer assistance, share information, and provide additional resources to state and local officials.

***Why hasn't DHS designated the election system to be a critical infrastructure sector?***

- At this point, we do not believe that designating election systems as a critical infrastructure sector would provide significant new authorities or resources to safeguard these systems in the near term. We have committed that we will not take any action on this issue until after the election and we have had sufficient opportunity to consult with the states. Right now, our priority is to help state officials ensure the security of their systems. In the longer term, we want to work with state officials to help them understand the practical

benefits of being designated as critical infrastructure and to seek their input on whether or not designation is appropriate.

***What is included in or meant by election infrastructure?***

- While there is no generally accepted definition of election infrastructure, DHS understands this term as the collection of systems and processes, administered by state and local governments, used to conduct elections. This collection includes information technology systems to register voters, maintain and disseminate accurate rolls of registered voters, create and disseminate ballots, enable voters to cast ballots, and accurately count and report on cast ballots in a timely manner. It covers all modes of voting, including in-person, early, absentee, vote-by-mail, and Internet voting.

***Who is responsible for the systems?***

- The responsibility for administering these systems varies widely by jurisdiction, but typically resides with the Secretary of State or Governor.

***What is DHS doing to secure voting infrastructure?***

- DHS is providing risk assessments and conducting hygiene scans, and has deployed cybersecurity advisors and protective security advisors throughout the country to provide support to state election officials. The DHS National Cybersecurity and Communications Integration Center serves as a 24x7 incident response center and can provide on-site assistance to identify and remediate a cyber incident.

- In addition to the work already being done by states and the operational cybersecurity support being provided through the National Protection & Programs Directorate, DHS stood up an Election Infrastructure Cybersecurity Working Group with experts from all levels of government to raise awareness of cybersecurity risks potentially affecting voting infrastructure and promote the security and resilience of the electoral process.

***Given these revelations, do you still have confidence in the U.S. electoral system?***

- Yes, we remain confident in the integrity of the U.S. election system for several reasons:

- The diverse and diffuse nature of our voting infrastructure makes it very difficult to manipulate the outcome of an election.

- States ensure that voting machines are not connected to the Internet.

- There are numerous checks and balances as well as extensive oversight at multiple levels built into our electoral process.

***Since you have not designated the election infrastructure as a critical infrastructure sector, does that mean it is not important or that you will not take steps to defend it?***

- Free and fair elections are a hallmark of our democracy, and we would consider any action that interferes with the right of Americans to participate in our election process as an attack on our democratic way of life.

- Regardless of whether the election infrastructure is designed as a critical infrastructure sector, we will take all necessary steps to sustain the integrity of our elections.

- The primary responsibility for protecting our election infrastructure resides with the states and local governments that administer elections, and that's the way it should be. However, the Federal government, and DHS in particular, stands ready to assist states and local governments if they request it.

***Has Congress been consulted regarding this incident?***

- Congress is regularly briefed about significant cyber threats and other intelligence reporting concerning the numerous and expanding range of malicious cyber actors threatening the United States and its interests around the world.

- Consistent with this practice, appropriate Congressional leadership were informed about these incidents, has been kept informed about this matter, and we intend to continue to update them on the incident as the situation warrants.

## Brian P. Hale-DNI-

**From:** Robert Litt-DNI-
**Sent:** Tuesday, December 27, 2016 2:09 PM
**To:** [redacted] DNI-; Brian P. Hale-DNI-; (b)(3) [redacted] Deirdre M. Walsh-DNI-; (b)(3) [redacted]
**Subject:** RE: (U) RE: First Draft - Executive Brief [~~SECRET~~, Record]

******* This message has been archived. Double-Click the message to view the contents. *******

Classification: ~~SECRET~~

Classified By: (b)(3) [redacted]
Derived From: Multiple Sources
Declassify On: 20411231
==========

My only question is (b)(5) [redacted] Otherwise looks good to me.

-----Original Message-----
From: (b)(3) [redacted] -DNI-
Sent: Tuesday, December 27, 2016 1:40 PM
To: Brian P. Hale-DNI- (b)(3) [redacted]; Robert Litt-DNI- <(b)(3) [redacted]>; (b)(3) [redacted] Deirdre M. Walsh-DNI- (b)(3) [redacted]; (b)(3) [redacted]
Subject: RE: (U) RE: First Draft - Executive Brief [~~SECRET~~, Record]

Classification: ~~SECRET~~

Classified By: (b)(3) [redacted]
Derived From: Multiple Sources
Declassify On: 20411231
==========

Here is a draft ODNI edit version. Thoughts? The main question would be (b) (5) [redacted].

(b) (5) [redacted]

~ (b) [redacted]

[redacted]
Deputy National Intelligence Officer for Cyber Issues
(b)(3) [redacted]

-----Original Message-----
From: Brian P. Hale-DNI-
Sent: Tuesday, December 27, 2016 9:36 AM
To: Robert Litt-DNI- (b)(3) >; (b)(3)
[redacted] Deirdre M. Walsh-DNI- (b)(3)
[redacted]
Subject: RE: (U) RE: First Draft - Executive Brief [~~SECRET~~, Record]

Classification: ~~SECRET~~

Classified By: (b)(3)
Derived From: Multiple Sources
Declassify On: 20411231
==========

I agree with Bob that (b) (5)
[redacted]

-----Original Message-----
From: Robert Litt-DNI-
Sent: Tuesday, December 27, 2016 8:49 AM
To: (b)(3)
[redacted] Brian P. Hale-DNI- (b)(3) ; Deirdre M. Walsh-DNI- (b)(3)
[redacted]
Subject: RE: (U) RE: First Draft - Executive Brief [~~SECRET~~, Record]

Classification: ~~SECRET~~

Classified By: (b)(3)
Derived From: Multiple Sources
Declassify On: 20411231
==========

(b) (5)
[redacted]

-----Original Message-----
From: (b)(3) -
Sent: Tuesday, December 27, 2016 8:42 AM
To: (b)(3)
[redacted] Robert Litt-DNI- (b)(3)
[redacted] Brian P. Hale-DNI- (b)(3) ; Deirdre M. Walsh-DNI- <(b)(3)
[redacted]
Subject: FW: (U) RE: First Draft - Executive Brief [~~SECRET~~, Record]

Classification: ~~SECRET~~

Classified By: (b)(3)
Derived From: Multiple Sources
Declassify On: 20411231
==========

New version of the DHS statement that I just responded to.

~ (b)

[redacted]
Deputy National Intelligence Officer for Cyber Issues
(b)(3) [redacted]

-----Original Message-----
From: (b)(3) [redacted]
Sent: Monday, December 26, 2016 2:10 PM
To: (b)(3) [redacted]
Cc: (b)(3) [redacted]
Subject: (U) RE: First Draft - Executive Brief [~~SECRET~~, Record] ---~~SECRET~~

Classification: ~~SECRET~~

Classified By: (b)(3) [redacted]
Derived From: Multiple Sources
Declassify On: 20411231
==========

All,

Please see attached for the updated Joint Press Statement and DHS comments and edits on the Exec Brief. (b) (5)

[redacted]

(b)

-----Original Message-----
From: (b)(3)
Sent: Friday, December 23, 2016 3:20 PM
To: (b)(3)

[redacted]

Subject: First Draft - Executive Brief [~~SECRET~~, Record]

Classification: ~~SECRET~~

Colleagues,

As promised, attached is a first draft of the (b) (5)

[redacted]

Please review and provide input/comments by Tuesday, December 26 at 2pm.

Thanks,

(b)

E.O. Categories: 1.4(b);1.c)(d)
Classified on: 12/13/2016
Declassify on: 12/13/2036

Classification:

Classification:

Classification:

Classification:

Classification:

Classification:

**Brian P. Hale-DNI-**

**From:** (b)(3) -DNI-
**Sent:** Wednesday, December 28, 2016 8:15 AM
**To:** Robert Litt-DNI-
**Cc:** Brian P. Hale-DNI-; Sellitto Michael EOP USA GOV; (b)(3) DHS USA GOV
**Subject:** RE: (U) RE: First Draft - Executive Brief [~~SECRET~~, Record]

******* This message has been archived. Double-Click the message to view the contents. *******

Classification: ~~SECRET~~

Classified By: (b)(3)
Derived From: ODNI CG v3.0 31 May 2016
Declassify On: 20411231
==========

I don't have a current draft. My understanding is a new package of (b) coming this morning? (b) (5)

~ (b)

Deputy National Intelligence Officer for Cyber Issues
(b)(3)

-----Original Message-----
From: Robert Litt-DNI-
Sent: Wednesday, December 28, 2016 8:07 AM
To: (b)(3)
Cc: Brian P. Hale-DNI- (b)(3)
Subject: RE: (U) RE: First Draft - Executive Brief [~~SECRET~~, Record]

Classification: ~~SECRET~~

Classified By: (b)(3)
Derived From: ODNI CG v3.0 31 May 2016
Declassify On: 20411231
==========
Can I see what the document looks like at this point, with these changes?

-----Original Message-----
From: (b)(3) DNI-
Sent: Wednesday, December 28, 2016 7:51 AM
To: Sellitto Michael EOP USA GOV <MSellitto@nsc.eop.ic.gov>
Cc: Brian P. Hale-DNI- (b)(3) >; Robert Litt-DNI-
<(b)(3) >
Subject: RE: (U) RE: First Draft - Executive Brief [~~SECRET~~, Record]

Classification: ~~SECRET~~

Classified By: (b)(3)

Derived From: ODNI CG v3.0 31 May 2016
Declassify On: 20411231
==========

Brian or Bob correct me if not, but this seems fine to me.

~ (b)

[redacted]
Deputy National Intelligence Officer for Cyber Issues
(b)(3) [redacted]

-----Original Message-----
From: Sellitto, Michael P. [mailto:MSellitto@nsc.eop.ic.gov]
Sent: Tuesday, December 27, 2016 3:50 PM
To: (b)(3) [redacted]
Subject: RE: (U) RE: First Draft - Executive Brief [~~SECRET~~, Record]

Classification: ~~SECRET~~

(b) (5) [redacted]

-----Original Message-----
From: (b)(3) [redacted]
Sent: Tuesday, December 27, 2016 2:28 PM
To: (b)(3) [redacted]

(b)(3) [redacted]

Subject: RE: (U) RE: First Draft - Executive Brief [~~SECRET~~, Record]

Classification: ~~SECRET~~

Classified By: (b)(3) [redacted]
Derived From: Multiple Sources
Declassify On: 20411231

==========

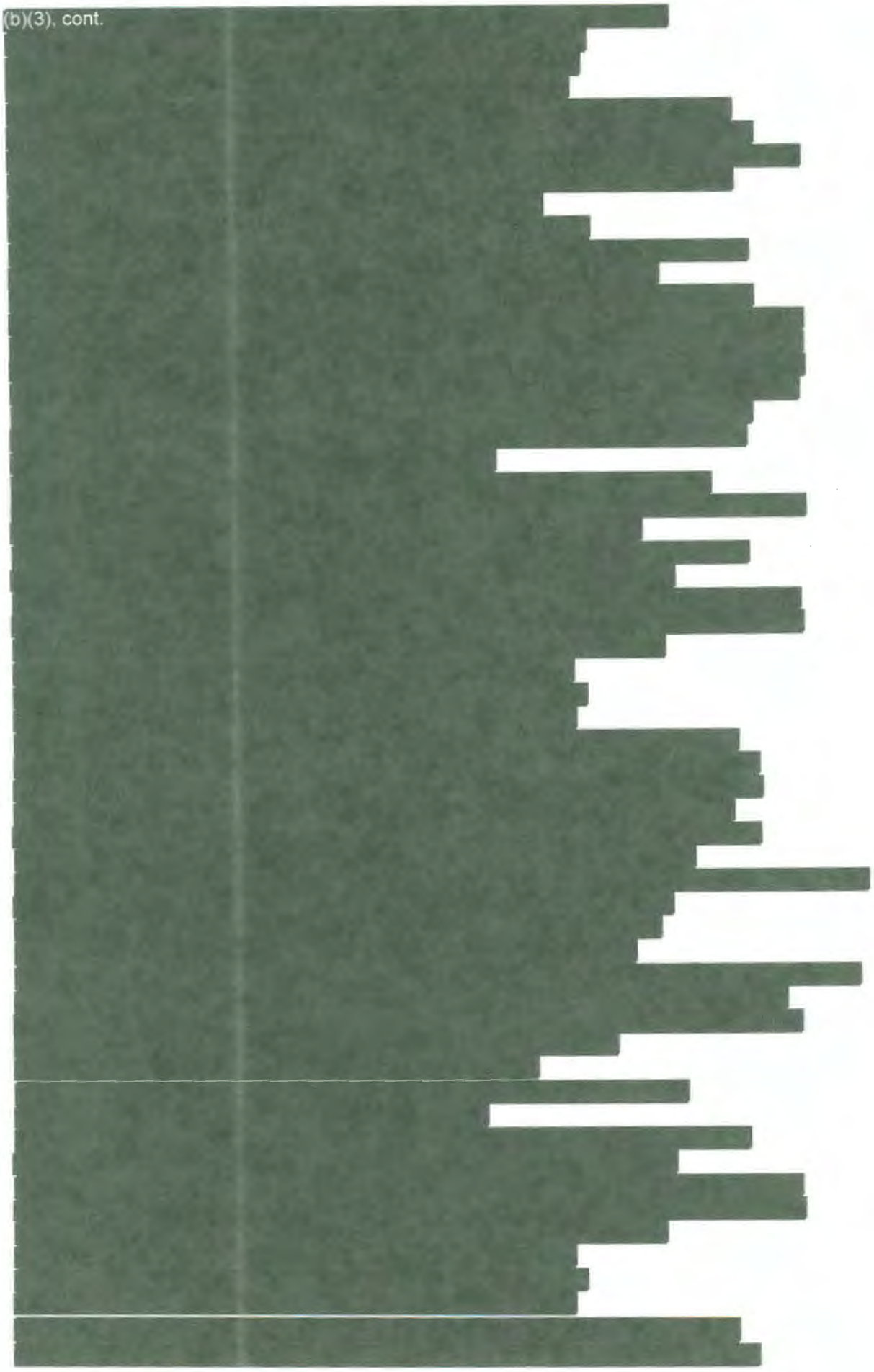
Attached is what ODNI proposes for this. It basically (b) (5) [redacted]

~ (b) [redacted]

[redacted]
Deputy National Intelligence Officer for Cyber Issues
(b)(3) [redacted]

-----Original Message-----
From: (b)(3) [redacted]
Sent: Tuesday, December 27, 2016 10:04 AM
To: (b)(3) [redacted]

(b)(3), cont.



(b)(3), cont.

[redacted]

Subject: RE: (U) RE: First Draft - Executive Brief [~~SECRET~~, Record] ---
~~SECRET~~

Classification: ~~SECRET~~

Classified By: (b)(3)
Derived From: Multiple Sources
Declassify On: 20411231
==========

(b)

(b) (5)

[redacted]

(b)

-----Original Message-----
From: (b)(3)
Sent: Tuesday, December 27, 2016 8:42 AM
To: (b)(3)

[redacted]

(b)(3)

[redacted]

Subject: RE: (U) RE: First Draft - Executive Brief [~~SECRET~~, Record]

Classification: ~~SECRET~~

Classified By: (b)(3)
Derived From: Multiple Sources
Declassify On: 20411231

==========

Thanks (b), looking better, but can we get some clarification on a couple points?

(b) (5)

[redacted]

(b)(5), cont.

[redacted]

~(b)

[redacted]
Deputy National Intelligence Officer for Cyber Issues
(b)(3)
[redacted]

-----Original Message-----
From: (b)(3)
Sent: Monday, December 26, 2016 2:10 PM
To: (b)(3)
[redacted]
Subject: (U) RE: First Draft - Executive Brief [~~SECRET~~, Record] --- ~~SECRET~~

Classification: ~~SECRET~~

Classified By: (b)(3)
Derived From: Multiple Sources
Declassify On: 20411231

All,

(b) (5)

[redacted]

(b)

----- Original Message-----
From: (b)(3)
Sent: Friday, December 23, 2016 3:20 PM
To: (b)(3)

[redacted]

Subject: First Draft - Executive Brief [~~SECRET~~, Record]

Classification: ~~SECRET~~

Colleagues,

As promised, attached is a first draft of the (b) (5)

[redacted]

Please review and provide input/comments by Tuesday, December 26 at 2pm.

Thanks,

(b)

E.O. Categories: 1.4(b,(c)(d)
Classified on: 12/23/2015
Declassify on: 12/23/2025

Classification: SECRET

Classification: SECRET

Classification: SECRET

Classification: SECRET

>E.O. Categories: 1.4(b)(c)(d)
Classified on: 12/27/2016
Declassify on: 12/27/2026

Classification: SECRET

Classification: SECRET

Classification: SECRET

## Brian P. Hale-DNI-

**From:** Brian P. Hale-DNI-
**Sent:** Tuesday, December 27, 2016 4:27 PM
**To:** (b)(3)
**Cc:**
**Subject:** RE: (U) RE: First Draft - Executive Brief [~~SECRET~~, Record]

******* This message has been archived. Double-Click the message to view the contents. *******

Classification: ~~SECRET~~

Classified By: (b)(3)
Derived From: Multiple Sources
Declassify On: 20411231
==========

Will do. Have a good trip.

(b)(3), (b)(5)

-----Original Message-----
From: Brian P. Hale-DNI-
Sent: Tuesday, December 27, 2016 3:13 PM
To: Ronald D. Boyd (b)(3)
Subject: FW: (U) RE: First Draft - Executive Brief [~~SECRET~~, Record]

Classification: ~~SECRET~~

Classified By: (b)(3)
Derived From: Multiple Sources
Declassify On: 20411231
==========

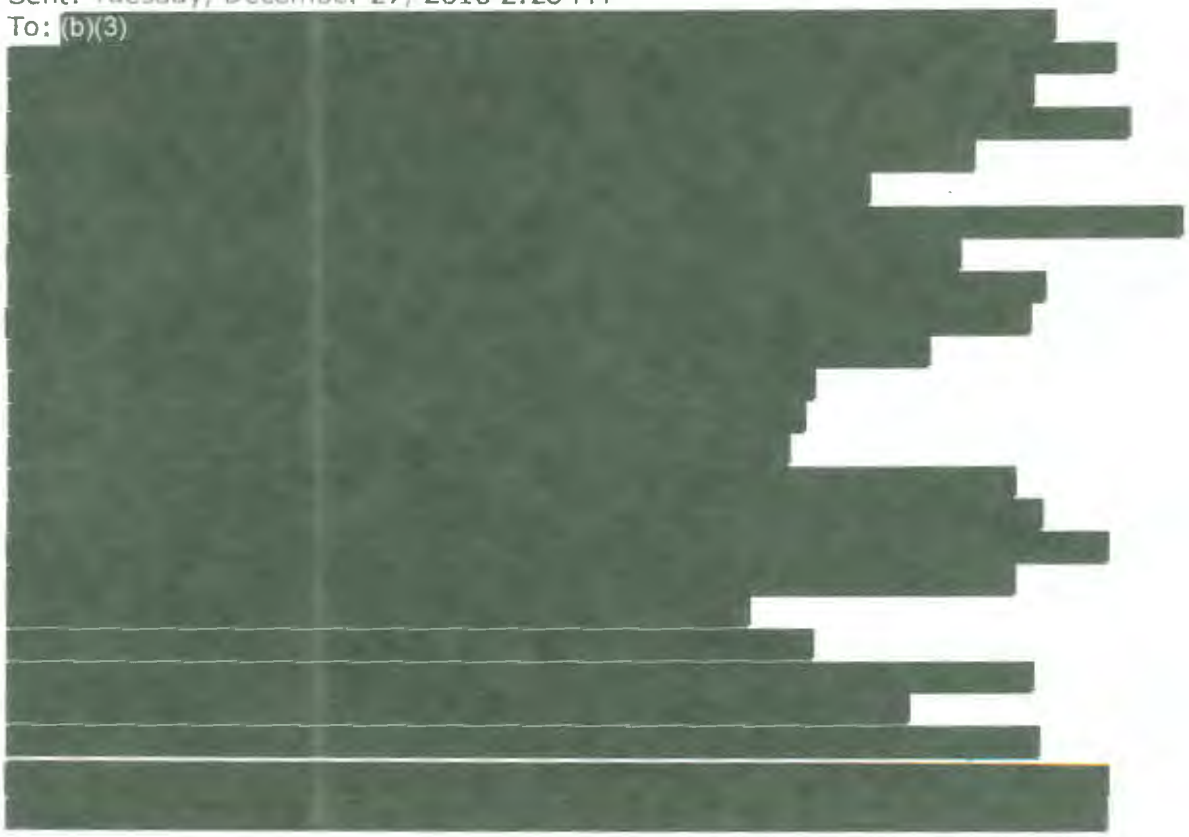
-----Original Message-----
From: Brian P. Hale-DNI-
Sent: Tuesday, December 27, 2016 2:42 PM
To: 'Stroh, Mark E.' <MStroh@nsc.eop.ic.gov>; Timothy L. Barrett-DNI-
<(b)(3) (b)(3)
(b)(3)
Subject: FW: (U) RE: First Draft - Executive Brief [~~SECRET~~, Record]

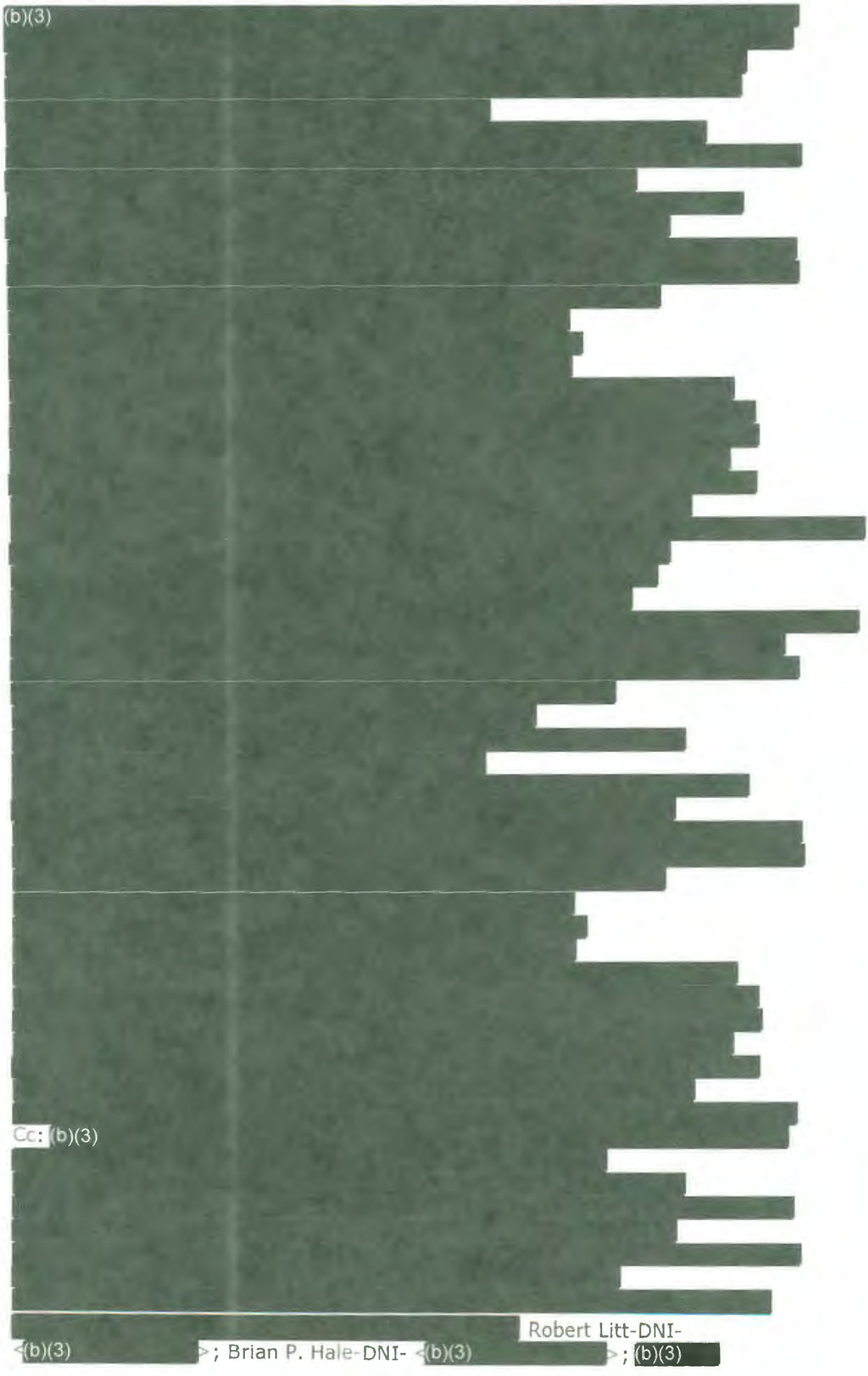
Classification: ~~SECRET~~

Classified By: (b)(3)
Derived From: Multiple Sources
Declassify On: 20411231
==========

We just got this alternate version that has been circulating within among other channels. Sending forward for your awareness.

-----Original Message-----
From: (b)(3) -DNI-
Sent: Tuesday, December 27, 2016 2:28 PM
To: (b)(3)





(b)(3), cont.

Subject: RE: (U) RE: First Draft - Executive Brief [~~SECRET~~, Record]

Classification: ~~SECRET~~

Classified By: (b)(3)
Derived From: Multiple Sources
Declassify On: 20411231
==========

Attached is what ODNI proposes for this. (b) (5)

(b)(3)

Deputy National Intelligence Officer for Cyber Issues
(b)(3)

-----Original Message-----
From: (b)(3)
Sent: Tuesday, December 27, 2016 10:04 AM
To: (b)(3)

(b)(3)

[redacted] Robert Litt-DNI- <[redacted]>; Brian P.

Hale-DNI- <(b)(3) >; (b)(3)

Subject: RE: (U) RE: First Draft - Executive Brief [~~SECRET~~, Record] ---
~~SECRET~~

Classification: ~~SECRET~~

Classified By: (b)(3)
Derived From: Multiple Sources
Declassify On: 20411231

(b)

(b) (5)

(b)

-----Original Message-----
From: (b)(3) (b)(3)
Sent: Tuesday, December 27, 2016 8:42 AM
To: (b)(3)

(b)(3)

Robert Litt-DNI-; Brian P. Hale-DNI-; (b)(3) Deirdre M. Walsh-DNI-; (b)(3)
Subject: RE: (U) RE: First Draft - Executive Brief [~~SECRET~~, Record]

Classification: ~~SECRET~~

Classified By: (b)(3)
Derived From: Multiple Sources
Declassify On: 20411231
==========

Thanks (b), looking better, but can we get some clarification on a couple points?

(b) (5)

~(b)

Deputy National Intelligence Officer for Cyber Issues
(b)(3)

-----Original Message-----
From: (b)(3)
Sent: Monday, December 26, 2016 2:10 PM
To: (b)(3)

Cc: (b)(3)
Subject: (U) RE: First Draft - Executive Brief [~~SECRET~~, Record] --- ~~SECRET~~

Classification: ~~SECRET~~

Classified By: (b)(3)
Derived From: Multiple Sources
Declassify On: 20411231
==========

All,

Please see attached for the updated Joint Press Statement and DHS comments and edits on the Exec Brief. (b) (5)

(b)(5), cont.

[redacted]

(b)

-----Original Message-----
From: (b)(3) [redacted]
Sent: Friday, December 23, 2016 3:20 PM
To: (b)(3) [redacted]

Subject: First Draft - Executive Brief [~~SECRET~~, Record]

Classification: ~~SECRET~~

Colleagues,

As promised, attached is a first draft of (b) (5) [redacted]

Please review and provide input/comments by Tuesday, December 26 at 2pm.

Thanks,

(b)

---

E.O. Categories: 1.4(b)(c)(d)
Classified on: 12/23/2016
Declassify on: 12/23/2026

Classification: [redacted]

Classification: [redacted]

Classification: [redacted]

Classification: [redacted]

Classification: [redacted]

Classification: [redacted]

Classification: [redacted]

Classification: [redacted]

SSCI# 2016-377

# United States Senate

November 29, 2016

The President
The White House
1600 Pennsylvania Avenue, NW
Washington, DC 20500

Dear Mr. President:

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.

Thank you for your attention to this important matter.

Sincerely,

Ron Wyden

Martin Heinrich

Jack Reed

Angus King

Mark R. Warner

Maize K. Hirono

Barbara A. Mikulski

**Michael G Birmingham**

**From:** Timothy L Barrett
**Sent:** Friday, December 09, 2016 1:29 PM
**To:** 'Price, Ned C. EOP/NSC'; Stroh, Mark E. EOP/NSC; 'John Francis Kirby (kirbyj@state.gov)'; 'tonermc2@state.gov'; Trudeau, Elizabeth K
**Cc:** Media; DNI-Media; Raimondi, Marc A. EOP/NSC
**Subject:** RE: Russia Review

thanks

**From:** Price, Ned C. EOP/NSC [mailto:Edward_C_Price@nsc.eop.gov]
**Sent:** Friday, December 09, 2016 1:20 PM
**To:** Stroh, Mark E. EOP/NSC <Mark_E_Stroh@nsc.eop.gov>; 'John Francis Kirby (kirbyj@state.gov)' <kirbyj@state.gov>; 'tonermc2@state.gov' <tonermc2@state.gov>; Trudeau, Elizabeth K <trudeauek@state.gov>
**Cc:** (b)(3) [redacted]; DNI-Media <DNI-Media@dni.gov>; Raimondi, Marc A. EOP/NSC <Marc_A_Raimondi@nsc.eop.gov>
**Subject:** RE: Russia Review

Adding the IC

**From:** Stroh, Mark E. EOP/NSC
**Sent:** Friday, December 9, 2016 1:10 PM
**To:** 'John Francis Kirby (kirbyj@state.gov)' <kirbyj@state.gov>; 'tonermc2@state.gov' <tonermc2@state.gov>; Trudeau, Elizabeth K <trudeauek@state.gov>; Price, Ned C. EOP/NSC <Edward_C_Price@nsc.eop.gov>
**Subject:** Russia Review

Feel free to refer to s but this is what we have for Schultz.

## ELECTION HACKING

**The President has instructed the Intelligence Community conduct a full review of the pattern of malicious cyber activity related to our Presidential election cycle. He has requested this report be completed and submitted to him before the end of his term.**

- **As you know, in 2008, there were intrusions into both the Obama and McCain campaigns.**

- **And there haven't been any noted episodes in 2012, but the President asked to go back – with what we now know – to make sure we're using every detection too possible as a means of due diligence.**

- **And of course in 2016, our IC determined there had been malicious cyber activity intended to interfere in our elections. In the high-confidence assessment they released, the IC made clear this was activity directed by the highest levels of the Russian government.**

  - Such activity wasn't new to Moscow. They have been engaging in similar tactics and techniques across Europe and Eurasia to influence public opinion.

**As we have made clear, we are committed to ensuring the integrity of our elections – and this report will dig into this pattern of malicious cyber activity timed to our elections, take stock of our defensive capabilities, and capture lessons-learned to brief members of Congress and stakeholders as appropriate** (like political campaigns and state and local offices responsible for administering elections).

**Q: Disputing election?**

- This is not an effort to challenge the outcome of the election.
  - To the contrary, the President has gone to great lengths to proceed with a seamless transition of power.
- We are not calling into question election results – we are taking seriously our responsibility to protect the integrity of our elections.

**Q: Public report?**

- The President has requested this report before he leaves office and you can imagine there could be classified or otherwise sensitive material included. I think you can expect that we'll get you as much of it as we can.

- But the President has instructed the report be shared with Members of Congress and other stakeholders.

**Q: Why now?**

- Obviously this is something we've been focused on for a while. That's why the President's Department of Homeland Security worked with nearly all 50 states how best to bolster cyber defenses in the lead-up to the election.

- Just to get real specific about this – we had noticed in the summer and fall an increase in scanning and probing of some states election related systems.

- In response, DHS engaged in rigorous outreach.
  - Deployed experts all across the country
  - Convened conference calls to share latest information
  - Briefed best practices

- As a result, we can confirm that the Federal Gov't did not observe any increased level of malicious cyber activity aimed at disrupting our electoral process on election day.

**Q: Which agencies?**

- As you know, the October statement that was released was announced by DNI and DHS. Obviously there are other agencies who work on these issues including the FBI, DOJ, and State.

(b)(3)

From: Timothy L Barrett
Sent: Friday, December 09, 2016 1:33 PM
To: (b)(6), (b)(7)(C) (b)(3)
Cc: DNI-Media
Subject: RE: WH Investigation of Russian hacking

Hi (b)(6), (b)(7)(C) and (b),

We are referring all calls to NSC. For your awareness, the below is what we just received from NSC, the guidance they are using for these queries:

## ELECTION HACKING

**The President has instructed the Intelligence Community conduct a full review of the pattern of malicious cyber activity related to our Presidential election cycle. He has requested this report be completed and submitted to him before the end of his term.**

- **As you know, in 2008, there were intrusions into both the Obama and McCain campaigns.**

- **And there haven't been any noted episodes in 2012, but the President asked to go back – with what we now know – to make sure we're using every detection too possible as a means of due diligence.**

- **And of course in 2016, our IC determined there had been malicious cyber activity intended to interfere in our elections. In the high-confidence assessment they released, the IC made clear this was activity directed by the highest levels of the Russian government.**

  - Such activity wasn't new to Moscow. They have been engaging in similar tactics and techniques across Europe and Eurasia to influence public opinion.

**As we have made clear, we are committed to ensuring the integrity of our elections – and this report will dig into this pattern of malicious cyber activity timed to our elections, take stock of our defensive capabilities, and capture lessons-learned to brief members of Congress and stakeholders as appropriate** (like political campaigns and state and local offices responsible for administering elections).

**Q: Disputing election?**

- This is not an effort to challenge the outcome of the election
  - To the contrary, the President has gone to great lengths to proceed with a seamless transition of power.
- We are not calling into question election results – we are taking seriously our responsibility to protect the integrity of our elections.

**Q: Public report?**

- The President has requested this report before he leaves office and you can imagine there could be classified or otherwise sensitive material included. I think you can expect that we'll get you as much of it as we can.

- But the President has instructed the report be shared with Members of Congress and other stakeholders.

**Q: Why now?**

- Obviously this is something we've been focused on for a while. That's why the President's Department of Homeland Security worked with nearly all 50 states how best to bolster cyber defenses in the lead-up to the election

- Just to get real specific about this – we had noticed in the summer and fall an increase in scanning and probing of some states election related systems.

- In response, DHS engaged in rigorous outreach.
  - Deployed experts all across the country
  - Convened conference calls to share latest information
  - Briefed best practices

- As a result we can confirm that the Federal Gov't did not observe any increased level of malicious cyber activity aimed at disrupting our electoral process on election day.

**Q: Which agencies?**

- As you know, the October statement that was released was announced by DNI and DHS. Obviously there are other agencies who work on these issues including the FBI, DOJ, and State.

**From:** (b)(6), (b)(7)(C) [redacted]
**Sent:** Friday, December 09, 2016 1:30 PM
**To:** (b)(3) [redacted]>; Timothy L Barrett <Tim.Barrett@dni.gov>
**Subject:** FW: WH Investigation of Russian hacking

Hello again (b) and Tim

Are you all receiving inquiries on the below? Are you saying anything? At this point, it does not look like we are.

Thank you,

(b)(6), (b)(7)(C)

**From:** (b)(6)
**Sent:** Friday, December 09, 2016 12:03 PM
**To:** (b)(6), (b)(7)(C)
**Subject:** WH Investigation of Russian hacking

Good afternoon.
Wondering if FBI has any comment on this - http://www.reuters.com/article/us-usa-election-cyber-idUSKBN13Y1U7

Any details of how this is going to work? Is this going to be a coordinated report or are agencies each doing their own? Would appreciate any available comments about how FBI will be approaching this investigation and if there are specific areas FBI will be focusing on in the investigation. This is for this afternoon.
Cheers,
(b)(6)

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

Ryan Shapiro
Jason Leopold
c/o Law Office of Jeffrey L. Light
1712 Eye St., NW, Suite 915
Washington, DC 20006

October 25, 2018

Re: Litigation 16-cv-02517-CKK, ODNI FOIA Case DF-2017-00093

Dear Mr. Shapiro and Mr. Leopold:

This is the 10th interim response provided by the Office of the Director of National Intelligence (ODNI) to your Freedom of Information Act (FOIA) request dated Dec 14, 2016, in which you requested, among other things, records about allegations of Russian-directed interference with the United States 2016 elections. On December 23, 2016, the ODNI's Information Management Division (IMD) acknowledged receipt of your request.

Your request is being processed in accordance with the FOIA, 5 U.S.C. § 552, as amended. With this response, 3 documents are being released in full and 6 documents are being released in part. All reasonably segregable, non-exempt information has been released. We have determined that the following exemptions apply:

- (b)(1), which applies to information that is currently and properly classified pursuant to Executive Order 13526, Section 1.4 (c) and (d).

- (b)(3), which applies to information exempt from disclosure by statute. The relevant statutes are the National Security Act of 1947, as amended, 50 U.S.C. § 3024(i) and 50 U.S.C. § 3024(m), which protect intelligence sources and methods and identifying information of ODNI personnel, respectively; 50 U.S.C. § 3605; and 18 U.S.C. § 798.

- (b)(5), which applies to intra or interagency communications that are pre-decisional and deliberative in nature. Disclosure in this instance would harm the Agency's deliberative process.

- (b)(6), which applies to information, the release of which, would constitute a clearly unwarranted invasion of personal privacy.

- (b)(7)(A), (C), and (E), which apply to certain records compiled for law enforcement purposes.

In addition, 4 documents are being withheld in full. The documents are comprised of multiple responsive and non-responsive records. The responsive records are being withheld under FOIA Exemption (b)(5) and the deliberative process privilege, which applies to interagency or intra-agency memorandums or letters that are pre-decisional and deliberate in nature. There is no meaningful responsive, non-exempt information that can be segregated from

these records. Portions of the records are also exempt from disclosure under (b)(1) and (b)(3) as described above.

If you have any questions, your attorney may contact Attorney Amy Powell of the Department of Justice at (919) 856-4013.

Sincerely,

Stephen Kelley
Deputy Director
Information Management Division

Enclosures