[redacted]

Pulled **December PDB draft**

For the President
8 December 2016

Cyber Manipulation Of US Election Infrastructure To Remain A Challenge

We assess that Russian and criminal actors did not impact recent US election results by conducting malicious cyber activities against election infrastructure. Russian Government–affiliated actors most likely compromised an Illinois voter registration database and unsuccessfully attempted the same in other states. Election monitoring and the type of systems targeted—infrastructure not used to cast or count votes—make it highly unlikely it would have resulted in altering any state's official vote result. Criminal activity also failed to reach the scale and sophistication necessary to change election outcomes. New election technology in the future that decreases diversity in systems and expands computer-enabled functions provides additional avenues to manipulate votes, but it will remain a significant challenge to sway elections through cyber means.

- Possible Russian Government–affiliated cyber actors extracted voter data, mostly containing names and addresses of voters, from Illinois's Board of Elections registration database in July that lacked adequate security safeguards. We also observed scanning and similar efforts against Secretary of State systems and websites in up to 20 more states from servers operated by a Russian-owned company with ties to Russian military cyber actors—the same infrastructure used against Illinois. [redacted]
- We have low-to-moderate confidence in the Russian Government's involvement because of our uncertainty about its utility for a state actor, a lack of observed effects from the low-profile operation, and the actors' use of obfuscation techniques, which included substantial overlap with criminal actors using similar targeting patterns and tactics. The activities did coincide with high-profile Russian cyber-enabled data leaks during the election, which we assess probably were intended to cause psychological effects, such as undermining the credibility of the election process and candidates. [redacted]

[redacted]

[redacted]

For profit cyber criminals and criminal hackers tried to steal data and to interrupt election processes by targeting election infrastructure, but these actions did not achieve a notable disruptive effect. Several technical issues with computer-enabled infrastructure were also reported, but they probably were routine software or hardware malfunctions—such as the use of old electronic voter rolls in North Carolina and technical difficulties with electronic voting machines in Pennsylvania and Utah—and were not the result of malicious activity. [redacted]

- We assess that a probable criminal cyber actor targeted a voter database in Arizona in April, using e-mail phishing to steal a single set of administrative credentials for the system—credentials that were later used to access the system in June and were posted online by a known criminal cyber actor who collects personally identifiable information.[redacted]

- On 8 November, a cybercriminal actor posted screenshots of information on Twitter resembling voting results from Alaska's state elections website and claimed to have administrative access to the website. The actor's successful but fraudulent access was resolved that day and there is no evidence of altered voting results; however, the FBI continues to investigate the incident.[redacted]

- Unattributed distributed denial of service attacks against election infrastructure were reported on election day, including a 4-minute attack against an unspecified Illinois elections website. That attack had no impact on the website's availability, according to information from Illinois' state fusion center.[redacted] In addition, a US cyber security company observed distributed denial of service attacks on the same day directed against websites associated with the US election and press systems; however, we have no reporting of how these websites were impacted.[redacted]

We assess that US election infrastructure will remain a target of growing interest for both foreign adversaries and nonstate actors during the next four years, with designs for compromise of election-related networks, theft of data, as well as disruptive and potentially manipulative activities enabled by cyber means. We assess that actors intent on covertly altering vote outcomes would, at least in part, target electronic voting machines to achieve such goals. The most likely cyber operations will probably continue to be those designed to steal data or disrupt electoral processes.

- We judge that Russia, China, Iran, and North Korea will have the ability to steal data from election-related networks, as well as execute a variety of disruptive attacks and even data manipulation on some election infrastructure. [redacted]

[redacted]

[redacted]

[redacted] We assess foreign adversaries will likely weigh the risk of appearing to influence US elections if caught or implicated, relative to any perceived benefit.

- We assess that the introduction of new technologies in the voting process will increase vulnerabilities and decrease diversity in computer-enabled US election system in the future. These technologies include cloud-based information technology infrastructure, electronic poll-books, ballot-on-demand printers, and online voting systems. Depending on the intent and capability of a future cyber actor targeting US elections, the procurement of these new machines may present a supply-chain risk.

- Moves to create additional Internet connections to election infrastructure responsible for casting and officially counting votes could provide more vulnerability to foreign adversaries and nonstate actors. Increases in the online submission of ballots, such as in Alaska where absentee ballots are allowed through an Internet portal, provides avenues for disruptive and manipulative operations. Cyber actors could attempt a denial of service attack to prevent upload of ballots, redirect would-be voters to non-existent or fraudulent websites, or attempt to manipulate the vote through compromise of voting servers.

- Persistent difficulties anticipating decisive tipping points in a nation-wide contest, as well as the decentralized nature of the systems and the election process, will continue to limit the effectiveness of cyber operations intended to alter an outcome. However, a lack of centralized standards for voter registration and voting systems provides an opportunity to improve computer network defenses. Outreach to elections officials on security assessments and cyber defense best practices, as well as engagement with private sector companies that develop and provision election infrastructure, would likely inhibit actors' ability to compromise systems and stymie further operations.

Prepared by DHS with reporting from CIA, DIA, DHS, FBI, NSA, State, and open sources.

[redacted]

From: [redacted] (FBI) [redacted]
Sent: Thursday, December 08, 2016 4:47 PM
To: dhs ; FBI ; DHS ; -DNI-; ; -DNI-; DHS ; DHS ; DHS ; FBI ; DHS ; NSA- ; NSA- ; DIA ; ; FBI ; ; DHS ; NSA- ; NSA- ; STATE ; STATE ; DIA ; NGA ; FBI ; FBI ; FBI ; FBI ; FBI ; FBI ; DIA ; NSA- ; -DNI-; -DNI-; -DNI-; FBI ; DHS ; NSA- ; NSA- ; STATE ; STATE ; DIA ; NGA ; DIA ; NSA- ; -DNI-; -DNI-; -DNI-; ; -DNI-; -DNI-; ; DHS ; NSA- ; DIA ; NSA- ; FBI ; ; DHS ; NSA- ; NSA- ; STATE ; STATE ; DIA ; NGA ; FBI ; FBI ; FBI ; FBI ; FBI ; FBI ; DIA ; NSA- ; -DNI-; -DNI-; -DNI-; ; FBI ; DHS ; NSA- ; NSA- ; STATE ; DIA ; NGA ; DIA ; NSA- ; -DNI-; -DNI-; -DNI-; ; -DNI-; -DNI-; ; DHS ; DHS ; DHS ; FBI ; FBI ; FBI ; FBI ; FBI ; FBI ; FBI ; FBI ; FBI ; DHS ; ; FBI ; FBI ; DHS ; -DNI-; DHS ; FBI ; FBI ; FBI ; FBI ; FBI ; FBI ; FBI
Cc: DHS ; dhs ; DHS ; DHS ; -DNI-; -DNI-; ; ; ; ; ; ; ; ; ; ;

Cc: [redacted]; [redacted] FBI [redacted]
Subject: RE: PDB Coordination Request - COB 8 December --- [redacted]

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
==========

Thanks for sending the revision, we will take a closer look at it tomorrow.

[redacted]

_____
[redacted]
Supervisory Intelligence Analyst
FBI Cyber Division
Eurasia Cyber Intelligence Unit
[redacted]

-----Original Message-----
From: [redacted] DHS [redacted]
Sent: Thursday, December 08, 2016 4:32 PM
To: [redacted] (FBI); [redacted]; [redacted] -DNI-; [redacted] -DNI-; [redacted] -DNI-; [redacted]; [redacted]; [redacted] (FBI); [redacted]; [redacted]; [redacted] NSA- [redacted]; [redacted] DIA [redacted]; [redacted]; [redacted] (FBI); [redacted]; [redacted]; [redacted] NSA- [redacted]; [redacted] NSA- [redacted]; [redacted] STATE [redacted]; [redacted] STATE [redacted]; [redacted] DIA [redacted]; [redacted] NGA [redacted]; [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] DIA [redacted]; [redacted] NSA- [redacted]; [redacted] -DNI-'; [redacted] -DNI-'; [redacted] -DNI-'; [redacted]; [redacted] (FBI); [redacted]; [redacted] NSA- [redacted]; [redacted] NSA- [redacted]; [redacted] STATE [redacted]; [redacted] STATE [redacted]; [redacted] DIA [redacted]; [redacted] NGA [redacted]; [redacted] DIA [redacted]; [redacted] NSA- [redacted]; [redacted] -DNI-'; [redacted] -DNI-'; [redacted] -DNI-'; [redacted] ; 'Cc: [redacted] -DNI-'; [redacted] -DNI-'; [redacted] ; [redacted] NSA- [redacted] '; [redacted] NSA- [redacted] '; [redacted] DIA [redacted] '; [redacted] NSA- [redacted] '; [redacted] (FBI); [redacted]; [redacted] NSA- [redacted]; [redacted] NSA- [redacted]; [redacted] STATE [redacted]; [redacted] STATE [redacted]; [redacted] DIA [redacted]; [redacted] NGA [redacted]; [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] DIA [redacted]; [redacted] NSA- [redacted]; [redacted] -DNI-'; [redacted] -DNI-'; [redacted] -DNI-'; [redacted]; [redacted] (FBI); [redacted]; [redacted] NSA- [redacted]; [redacted]; [redacted] STATE [redacted]; [redacted] STATE [redacted]; [redacted] DIA [redacted]; [redacted] NGA [redacted]; [redacted] DIA [redacted]; [redacted] NSA- [redacted]; [redacted] -DNI-'; [redacted] -DNI-'; [redacted] -DNI-'; [redacted] ; 'Cc: [redacted] -DNI-'; [redacted] -DNI-'; [redacted] -DNI-'; [redacted]; [redacted]; [redacted]; [redacted]

(FBI); (FBI); (FBI); (FBI); (FBI);
(FBI); (FBI); (FBI); (FBI);
(FBI); ; ; (FBI);
(FBI); -DNI- ; (FBI); (FBI);
(FBI); (FBI); (FBI); (FBI);
(FBI); (FBI)
Cc: ; ; ; ; -DNI-;
-DNI-; ; ; ; ; ; ;
; ; ; ; ; (FBI)
Subject: RE: PDB Coordination Request - COB 8 December ---

Classification:

Classified By:
Derived From:
Declassify On:
==========

Until receiving the email below, the only difference that I was aware of between FBI and I&A over this transparently developed product was over confidence level on the attribution, which we have adjusted (to the FBI's view) upon review of the recent redacted collection. Rather than drafting a dissent, perhaps FBI could share their concerns with the most recent draft (attached). I think it goes without saying that this PDB should not go forward until the FBI has done so.

-----Original Message-----
From: (FBI)
Sent: Thursday, December 08, 2016 3:48 PM
To: ; -DNI-; -DNI-; -DNI-; ;
; ; (FBI); ; NSA- ;
NSA- ; DIA ; NSA- ;
(FBI); ; ; NSA- ; NSA-
; STATE ; STATE ; DIA ;
NGA ; (FBI); (FBI);
(FBI); (FBI); (FBI); (FBI);
DIA ; NSA- ; -DNI-'; -DNI-
'; -DNI-'; ; (FBI); ; NSA-
; NSA- ; STATE ; STATE
; DIA ; NGA ; DIA
; NSA- ; -DNI-'; -DNI-'; -DNI-
'; ; 'Cc: -DNI-'; -DNI-'; -DNI-'; ;
NSA- ; NSA- ; DIA ;
NSA- ; (FBI); ; ;
; NSA- ; STATE ; STATE
; DIA ; NGA ; (FBI);
(FBI); (FBI); (FBI);
(FBI); (FBI); DIA ; NSA- ;
-DNI-'; -DNI-'; -DNI-'; ; (FBI);
; NSA- ; NSA- ; STATE
; STATE ; DIA ; NGA
; DIA ; NSA- ; -DNI-';
-DNI-'; -DNI-'; ; 'Cc: -DNI-'; -DNI-';
-DNI-'; ; ; ; (FBI); (FBI);

(FBI); (FBI); (FBI); (FBI);
(FBI); (FBI); (FBI); (FBI);
; ; (FBI); (FBI); -DNI-;
; (FBI); (FBI); (FBI);
(FBI); ; (FBI); (FBI);
(FBI)
Cc: ; ; ; ; ;
-DNI-; -DNI-; ; ; ; ; ;
; ; ; ; ; ; ;
(FBI)
Subject: RE: PDB Coordination Request - COB 8 December ---

Classification:

Classified By:
Derived From:
Declassify On:
==========
, FBI will be drafting a dissent this afternoon. Please remove our seal an annotations of co-authorship.

-----Original Message-----
From: DHS
Sent: Thursday, December 08, 2016 2:22 PM
To: -DNI- ; -DNI- ; -DNI-
; DHS ; DHS ;
DHS ; (FBI) ;
DHS ; NSA- ; NSA-
; DIA ;
NSA- ; (FBI) ;
cia ; DHS ; NSA-
; NSA- ; STATE
; STATE ; DIA
; NGA ;
(FBI) ; (FBI) ;
(FBI) ; (FBI) ;
(FBI) ; (FBI) ; DIA
; NSA- -
DNI-' ; -DNI-' ; -DNI-'
; cia. ; (FBI) ;
DHS ; NSA- ;
; STATE ; STATE
; DIA ;
NGA ; DIA
; NSA- ; -DNI-'
; -DNI-' ; -DNI- ;
cia 'Cc: -DNI-' -DNI-'
; -DNI-' ; DHS ;
NSA- ; NSA- ;
DIA ; NSA-

; (FBI) ; cia ;
DHS ; NSA- ;
NSA- ; STATE ;
STATE ; DIA ;
NGA ; (FBI)
; (FBI) ; (FBI)
; (FBI) ; (FBI)
; (FBI) ; DIA
; NSA- ; -DNI-'
; -DNI-' ; -DNI-' ;
cia ; (FBI) ;
DHS ; NSA- ; NSA-
; STATE ; STATE
; DIA ;
NGA ; DIA
; NSA- -DNI-'
; -DNI-' ; -DNI-' ;
cia ; 'Cc: -DNI-' ; -DNI-'
; -DNI- ; DHS ;
DHS >; DHS ; (FBI)
; (FBI) ; (FBI) ;
(FBI) ; (FBI) ; (FBI)
; (FBI) ; (FBI)
; (FBI) >; (FBI)
; DHS ; DHS ;
(FBI) ; (FBI) ; (FBI)
; -DNI- ; DHS
Cc: DHS ; DHS ;
DHS ; DHS ; DHS ;
-DNI- -DNI- ;
cia ; cia
Subject: RE: PDB Coordination Request - COB 8 December ---

Classification:

Classified By:
Derived From:
Declassify On:
==========

We have so far received responses from FBI, CIA/NIC, and NGA. Please provide coordination responses ASAP if you have not been able to yet. Thank you for understanding and trying to accommodate this short coordination period, to accommodate the Administration's request for this to run tomorrow.

Thank you,

NCCIC Intelligence Support Branch
Cyber Division
DHS Office of Intelligence & Analysis

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, December 08, 2016 12:59 PM
To: [redacted]
Subject: RE: [redacted] PDB Coordination Request - COB 8 December --- [redacted]

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
==========

Hi All,

Due to high Administration interest, this piece is now scheduled to run tomorrow. Therefore, we now ask that coordination responses be sent by 2pm, so that the production process for tomorrow can be completed.

Thank you,

[redacted]
NCCIC Intelligence Support Branch
Cyber Division
DHS Office of Intelligence & Analysis
[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, December 07, 2016 4:47 PM
To: [redacted]
Cc: [redacted]
Subject: [redacted] PDB Coordination Request - COB 8 December ---

Classification: [redacted]

Classified By: [redacted]

Derived From: [redacted]
Declassify On: [redacted]
==========

[redacted]

Hi All,

DHS I&A Cyber Division is requesting coordination from all recipients by COB on 8 December for this cyber/US elections PDB. If multiple colleagues from your agency are on this email (e.g., FBI) please coordinate your response within your agency so that one unified response is sent for your agency. You can send your comments back to me, and please let me know if you have any questions.

Thank you,

[redacted]
NCCIC Intelligence Support Branch
Cyber Division
DHS Office of Intelligence & Analysis
[redacted]

==========
Classification: [redacted]

==========
Classification: [redacted]

==========
Classification: [redacted]

==========
Classification: [redacted]

==========
Classification: [redacted]

==========
Classification: [redacted]

From: [redacted]-DNI-
Sent: Thursday, December 08, 2016 4:53 PM
To: [redacted]
Cc: [redacted]
Subject: RE: [redacted] PDB Coordination Request - COB 8 December

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
==========

All,

Based on some new guidance, we are going to push back publication of the PDB. It will not run tomorrow and is not likely to run until next week.

[redacted]

[redacted]
Deputy Director / PDB / ODNI
[redacted]

==========
Classification: [redacted]

[redacted]

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20504

Summary of Conclusions for
Meeting of the Principals Committee
DATE: December 9, 2016
LOCATION: White House Situation Room
TIME: 11:30 a.m. - 1:30 p.m.

SUBJECT: Summary of Conclusions for PC Meeting on a Sensitive Topic [redacted]

Participants:

Chair
Susan Rice

OVP
No Representative

State
Secretary John Kerry (SVTS)
Victoria Nuland

Treasury
Adam Szubin

DOD
Brian McKeon

Justice
Loretta Lynch
Mary McCord

DHS
Secretary Jeh Johnson
Rob Silvers

Chief of Staff
Denis McDonough

USUN
Maher Bitar

WH Counsel
Neil Eggleston

DNI
James Clapper

FBI
Andrew McCabe

CIA
John Brennan

JCS (SVTS)
Gen Joseph Dunford

NSA
Richard Ledgett

White House
Avril Haines
Lisa Monaco
Ben Rhodes

NSC
Chris Fonzone
Caroline Tess
Brett Holmgren
Michael Daniel
Celeste Wallander
Samir Jain
Jeffrey Edmonds

[redacted]
Classified by: [redacted]
Reason: [redacted]
Declassify on: [redacted]

Summary of Conclusions

It was agreed that:

- Principals agreed to deny Russia the use of its residential and recreational compound at Pioneer Point on the Chesapeake Bay. Principals also recommended, pending the views of the U.S. Mission to the United Nations (USUN) and legal review, denying Russia the use of its residential and recreational compound in Glen Cove, New York. The Department of State noted its preference that any action against the compounds be delayed to, among other things, allow for a potential agreement on Aleppo to be implemented. State also will provide a matrix of possible Russian responses, both operationally and diplomatically, to the closure of the compounds. **(Action: State by December 13, 2016)** [redacted]

- Principals concurred with a number of measures State proposed to take with respect to Russian visas - in particular, leaving to the discretion of State and the Federal Bureau of Investigation (FBI) the issuance of U.S. visas for Russian intelligence officers, holding Russian diplomats to the 48 hour travel notification requirement, and limiting the number of exceptions provided to Russian diplomats. **(Action: State and FBI, ongoing)** [redacted]

- State and FBI will draft, for further legal and policy review, a proposal for removing a number of suspected Russian intelligence officers in the United States. **(Action: State and FBI by December 10, 2016)** [redacted]

- Principals considered the cyber options and recommended against conducting either a spearphishing campaign or a denial of service attack against certain Russian entities. [redacted]

- Principals agreed to recommend sanctioning of certain members of the Russian military intelligence and foreign intelligence chains of command responsible for cyber operations as a response to cyber activity that attempted to influence or interfere with the U.S. elections, if such activity meets the requirements for designation under Executive Order (E.O.) 13694 on *Blocking the Property of certain persons Engaging in Significant Cyber-Enabled Activities*. The Department of the

[redacted]
Classified by: [redacted]
Reason: [redacted]
Declassify on: [redacted]

Treasury will determine if such sanctions are possible under E.O. 13694. **(Action: Treasury by December 16, 2016)** [redacted]

- Principals were divided on whether to issue the designations of Belan and Bogachev under E.O. 13694 as part of the response to Russian interference in our electoral process. Some Principals opposed designations in this context because: (a) the conduct in question was unrelated to the election-related activity; and (b) absent a tie to the elections, any package of designations should include the two Chinese companies for which sanctions packages also have been developed. Other Principals support designations in this context because: (a) a failure by this Administration to use E.O. 13694 will undermine the E.O.'s utility and deterrent effect; and (b) if coupled with appropriate messaging, use of the E.O. against Russian targets would signal that future election-related activity could prompt sanctions. [redacted]

- [redacted]

- [redacted]

- To the maximum extent feasible consistent with sources and methods, Principals agreed to publicly release and attribute to Russian intelligence services technical and other information about: (a) Russian intrusion set; and (b) the recent Russian spearphishing campaign highlighted in intelligence reporting on December 9. The Cyber Response Group (CRG) will coordinate the development of the plan for public release based on input from the Central Intelligence Agency (CIA), the National Security Agency (NSA), and the FBI. **(Action: CRG in coordination with CIA, NSA, and FBI by December 19, 2016)** [redacted]

[redacted]