Withdrawn/Redacted Material
Obama Presidential Library

DOCUMENT NO.	FORM	SUBJECT/TITLE	PAGES	DATE	RESTRICTION(S)
001	Note	[Handwritten notes]	3	N.D.	P1/b1;
002	Draft	[Outline]	2	N.D.	P1/b1;
003	Email	From Ned C. Price to DL-WHO-Press et al., re: Fwd: JOINT DHS, ODNI, FBI STATEMENT ON RUSSIAN MALICIOUS CYBER ACTIVITY	2	12/29/2016	
004	Report	Joint Analysis Report, re: Grizzly Steppe - Russian Malicious Cyber Activity	13	12/29/2016	
005	Email	From Graham H. Brookie to Graham H. Brookie, re: FW: TREASURY SANCTIONS TWO INDIVIDUALS FOR MALICIOUS CYBER-ENABLED ACTIVITIES	3	12/29/2016	
006	Article	U.S. Punishes Russia for Election hacking, Ejecting Operatives	3	12/29/2016	

COLLECTION TITLE:
National Security Council - Homeland Security and Counter-Terrorism Directorate

SERIES:
Monaco, Lisa - Subject Files

FOLDER TITLE:
Russia Response Rollout

FRC ID:
70724

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

Deed of Gift Restrictions

A. Closed by Executive Order 13526 governing access to national security information.
B. Closed by statute or by the agency which originated the document.
C. Closed in accordance with restrictions contained in donor's deed of gift.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Records Not Subject to FOIA

Court Sealed - The document is withheld under a court seal and is not subject to the Freedom of Information Act.

Withdrawn/Redacted Material
Obama Presidential Library

DOCUMENT NO.	FORM	SUBJECT/TITLE	PAGES	DATE	RESTRICTION(S)
007	Timeline	[Timeline of events for December 27th to December 31st]	3	N.D.	P1/b1;
008	Tab Divider	POTUS / Fact Sheet	1	N.D.	
009	Statement	Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment	1	12/29/2016	
010	Fact Sheet	FACT SHEET: Actions in Response to Russian Malicious Cyber Activity and Harassment	3	N.D.	
011	Email	From Ned C. Price to DL-WHO-Press et al., re: FW: STATEMENT: Department of State Actions in Response to Russian Harassment	2	12/29/2016	
012	Tab Divider	Q/A	1	N.D.	

COLLECTION TITLE:
National Security Council - Homeland Security and Counter-Terrorism Directorate

SERIES:
Monaco, Lisa - Subject Files

FOLDER TITLE:
Russia Response Rollout

FRC ID:
70724

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

Deed of Gift Restrictions

A. Closed by Executive Order 13526 governing access to national security information.
B. Closed by statute or by the agency which originated the document.
C. Closed in accordance with restrictions contained in donor's deed of gift.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Records Not Subject to FOIA

Court Sealed - The document is withheld under a court seal and is not subject to the Freedom of Information Act.

Withdrawn/Redacted Material
Obama Presidential Library

DOCUMENT NO.	FORM	SUBJECT/TITLE	PAGES	DATE	RESTRICTION(S)
013	Draft	Cyber: Response to Russian Malicious Cyber Activity and Harassment	16	12/29/2016	P5;
014	Email	From Avril D. Haines to Lisa O. Monaco et al., re: Per the Q/A discussed	1	12/29/2016	P5;
015	Draft	Cyber: Response to Russian Malicious Cyber Activity and Harassment	14	N.D.	P5;
016	Tab Divider	DNI / DHS / FBI	1	N.D.	
017	Draft	Draft Joint DHS/DNI/FBI Press Statement	2	12/27/2016	P1/b1;
018	Tab Divider	JAR / Exc. Summary	1	N.D.	

COLLECTION TITLE:
National Security Council - Homeland Security and Counter-Terrorism Directorate

SERIES:
Monaco, Lisa - Subject Files

FOLDER TITLE:
Russia Response Rollout

FRC ID:
70724

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

Deed of Gift Restrictions

A. Closed by Executive Order 13526 governing access to national security information.
B. Closed by statute or by the agency which originated the document.
C. Closed in accordance with restrictions contained in donor's deed of gift.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Records Not Subject to FOIA

Court Sealed - The document is withheld under a court seal and is not subject to the Freedom of Information Act.

Withdrawn/Redacted Material
Obama Presidential Library

DOCUMENT NO.	FORM	SUBJECT/TITLE	PAGES	DATE	RESTRICTION(S)
019	Draft	Joint Analysis Report, re: Operation Grizzly Steppe - Russian Malicious Cyber Activity	12	12/29/2016	P5;
020	Draft	Operation Grizzly Steppe	6	12/27/2016	P1/b1; P5;
021	Tab Divider	Prior Statements	1	N.D.	
022	Speech	Remarks as delivered by the Honorable James R. Clapper Director of National Intelligence	5	02/09/2016	
023	Transcript	Aspen Security Forum 2016 The View from the West Wing	35	07/30/2016	
024	Webpage	Readout of Secretary Johnson's Call with State Election Officials on Cybersecurity	2	08/15/2016	

COLLECTION TITLE:
National Security Council - Homeland Security and Counter-Terrorism Directorate

SERIES:
Monaco, Lisa - Subject Files

FOLDER TITLE:
Russia Response Rollout

FRC ID:
70724

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

Deed of Gift Restrictions

A. Closed by Executive Order 13526 governing access to national security information.
B. Closed by statute or by the agency which originated the document.
C. Closed in accordance with restrictions contained in donor's deed of gift.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Records Not Subject to FOIA

Court Sealed - The document is withheld under a court seal and is not subject to the Freedom of Information Act.

Withdrawn/Redacted Material
Obama Presidential Library

DOCUMENT NO.	FORM	SUBJECT/TITLE	PAGES	DATE	RESTRICTION(S)
025	Article	Comey: FBI takes election tampering 'very seriously'	2	08/30/2016	
026	Press Release	Joint DHS and ODNI Election Security Statement	1	10/07/2016	
027	Article	DHS official: Half of U.S. states have sought help to thwart election hackers	2	10/05/2016	
028	Tab Divider	Presss Call TPs	1	N.D.	
029	Draft	Talking Points for Cyber Validator Calls	3	N.D.	P5;
030	Tab Divider	E.O.	1	N.D.	
031	Executive Order	Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities	5	12/28/2016	

COLLECTION TITLE:
National Security Council - Homeland Security and Counter-Terrorism Directorate

SERIES:
Monaco, Lisa - Subject Files

FOLDER TITLE:
Russia Response Rollout

FRC ID:
70724

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

Deed of Gift Restrictions

A. Closed by Executive Order 13526 governing access to national security information.
B. Closed by statute or by the agency which originated the document.
C. Closed in accordance with restrictions contained in donor's deed of gift.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Records Not Subject to FOIA

Court Sealed - The document is withheld under a court seal and is not subject to the Freedom of Information Act.

Withdrawn/Redacted Material
Obama Presidential Library

DOCUMENT NO.	FORM	SUBJECT/TITLE	PAGES	DATE	RESTRICTION(S)
032	List	Annex	1	N.D.	
033	List	Annex [duplicate of 032]	1	N.D.	
034	Press Release	Text of a Letter from the President to the Speaker of the House of Representatives and the President of the Senate	1	12/28/2016	
035	Email	From Ned C. Price to #SUITE et al., re: [Readouts]	3	12/29/2016	P5;
036	Email	From Ned C. Price to #SUITE et al., re: [Readout]	2	12/29/2016	P5;
037	Email	From Graham H. Brookie to Lisa O. Monaco et al., re: Confirmed Participants - White House Call - (12/29) at 1:30 pm ET	2	12/29/2016	P5;
038	List	[List]	1	N.D.	

COLLECTION TITLE:
National Security Council - Homeland Security and Counter-Terrorism Directorate

SERIES:
Monaco, Lisa - Subject Files

FOLDER TITLE:
Russia Response Rollout

FRC ID:
70724

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

Deed of Gift Restrictions

A. Closed by Executive Order 13526 governing access to national security information.
B. Closed by statute or by the agency which originated the document.
C. Closed in accordance with restrictions contained in donor's deed of gift.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Records Not Subject to FOIA

Court Sealed - The document is withheld under a court seal and is not subject to the Freedom of Information Act.

Withdrawn/Redacted Material
Obama Presidential Library

DOCUMENT NO.	FORM	SUBJECT/TITLE	PAGES	DATE	RESTRICTION(S)
039	Statement	Joint DHS and ODNI Election Security Statement	2	10/07/2016	
040	Email	From Joe "Michael" Daniel to Lisa O. Monaco et al.	1	12/28/2016	P1/b1;

COLLECTION TITLE:
National Security Council - Homeland Security and Counter-Terrorism Directorate

SERIES:
Monaco, Lisa - Subject Files

FOLDER TITLE:
Russia Response Rollout

FRC ID:
70724

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

Deed of Gift Restrictions

A. Closed by Executive Order 13526 governing access to national security information.
B. Closed by statute or by the agency which originated the document.
C. Closed in accordance with restrictions contained in donor's deed of gift.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Records Not Subject to FOIA

Court Sealed - The document is withheld under a court seal and is not subject to the Freedom of Information Act.

Withdrawal Marker
Obama Presidential Library

FORM	SUBJECT/TITLE	PAGES	DATE	RESTRICTION(S)
Note	[Handwritten notes]	3	N.D.	P1/b1;

This marker identifies the original location of the withdrawn item listed above. For a complete list of items withdrawn from this folder, see the Withdrawal/Redaction Sheet at the front of the folder.

COLLECTION:
National Security Council - Homeland Security and Counter-Terrorism Directorate

SERIES:
Monaco, Lisa - Subject Files

FOLDER TITLE:
Russia Response Rollout

FRC ID:
70724

OA Num.:
W1100

NARA Num.:

FOIA IDs and Segments:

22-26844-F

22-26842-F

22-26841-F

22-26840-F 3

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

Deed of Gift Restrictions

A. Closed by Executive Order 13526 governing access to national security information.
B. Closed by statute or by the agency which originated the document.
C. Closed in accordance with restrictions contained in donor's deed of gift.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Records Not Subject to FOIA

Court Sealed - The document is withheld under a court seal and is not subject to the Freedom of Information Act.

Withdrawal Marker
Obama Presidential Library

FORM	SUBJECT/TITLE	PAGES	DATE	RESTRICTION(S)
Draft	[Outline]	2	N.D.	P1/b1;

This marker identifies the original location of the withdrawn item listed above. For a complete list of items withdrawn from this folder, see the Withdrawal/Redaction Sheet at the front of the folder.

COLLECTION:
National Security Council - Homeland Security and Counter-Terrorism Directorate

SERIES:
Monaco, Lisa - Subject Files

FOLDER TITLE:
Russia Response Rollout

FRC ID:
70724

OA Num.:
W1100

NARA Num.:

FOIA IDs and Segments:

22-26844-F

22-26842-F

22-26841-F

22-26840-F 3

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

Deed of Gift Restrictions

A. Closed by Executive Order 13526 governing access to national security information.
B. Closed by statute or by the agency which originated the document.
C. Closed in accordance with restrictions contained in donor's deed of gift.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Records Not Subject to FOIA

Court Sealed - The document is withheld under a court seal and is not subject to the Freedom of Information Act.

Alpha, Avery M. EOP/NSC

From: Price, Ned C. EOP/NSC
Sent: Thursday, December 29, 2016 3:05 PM
To: DL-WHO-Press; #CYBER; #RUSSIA; #SUITE; #INTEL
Subject: Fwd: JOINT DHS, ODNI, FBI STATEMENT ON RUSSIAN MALICIOUS CYBER ACTIVITY

Press Office
U.S. Department of Homeland Security

Press Release

December 29, 2016
Contact: DHS Press Office, 202-282-8010

JOINT DHS, ODNI, FBI STATEMENT ON RUSSIAN MALICIOUS CYBER ACTIVITY

On October 7, 2016, Secretary Johnson and Director Clapper issued a joint statement that the intelligence community is confident the Russian Government directed the recent compromises of e-mails from U.S. persons and institutions, including from U.S. political organizations, and that the disclosures of alleged hacked e-mails on sites like DCLeaks.com and WikiLeaks are consistent with the Russian-directed efforts. The statement also noted that the Russians have used similar tactics and techniques across Europe and Eurasia to influence public opinion there.

Today, DHS and FBI released a Joint Analysis Report (JAR) which further expands on that statement by providing details of the tools and infrastructure used by Russian intelligence services to compromise and exploit networks and infrastructure associated with the recent U.S. election, as well as a range of U.S. government, political and private sector entities.

This activity by Russian intelligence services is part of a decade-long 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, think tanks, universities, political organizations, and corporations; theft of information from these organizations; and the recent public release of some of this stolen information. In other countries, Russian intelligence services have also undertaken damaging and disruptive cyber-attacks, including on critical infrastructure, in some cases masquerading as third parties or hiding behind false online personas designed to cause victim to misattribute the source of the attack. The Joint Analysis Report provides technical indicators related to many of these operations, recommended mitigations and information on how to report such incidents to the U.S. Government.

A great deal of analysis and forensic information related to Russian government activity has been published by a wide range of security companies. The U.S. Government can confirm that the Russian government, including Russia's civilian and military intelligence services, conducted many of the activities generally described by a number of these security companies. The Joint Analysis Report recognizes the excellent work undertaken by security companies and private sector network owners and operators, and provides new indicators of compromise and malicious infrastructure identified during the course of investigations and incident response. The U.S. Government seeks to arm network defenders with the tools they need to identify,, detect and disrupt Russian malicious cyber activity that is targeting our country's and our allies' networks.

We encourage security companies and private sector owners and operators to look back within their network traffic for signs of the malicious activity described in the Joint Analysis Report. We also encourage such entities to utilize these indicators in their proactive defense efforts to block malicious cyber activity before it occurs. DHS has already added these indicators to its Automated Indicator Sharing service, which provides indicators of malicious cyber activity at machine speed. Entities that are participating in this service have already implemented these indicators for the network protection activities.

Entities that find signs of this malicious cyber activity should report it to the FBI through CyWatch or its local field offices or to DHS's National Cybersecurity and Communications Integration Center (NCCIC).

###

TLP:WHITE

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.

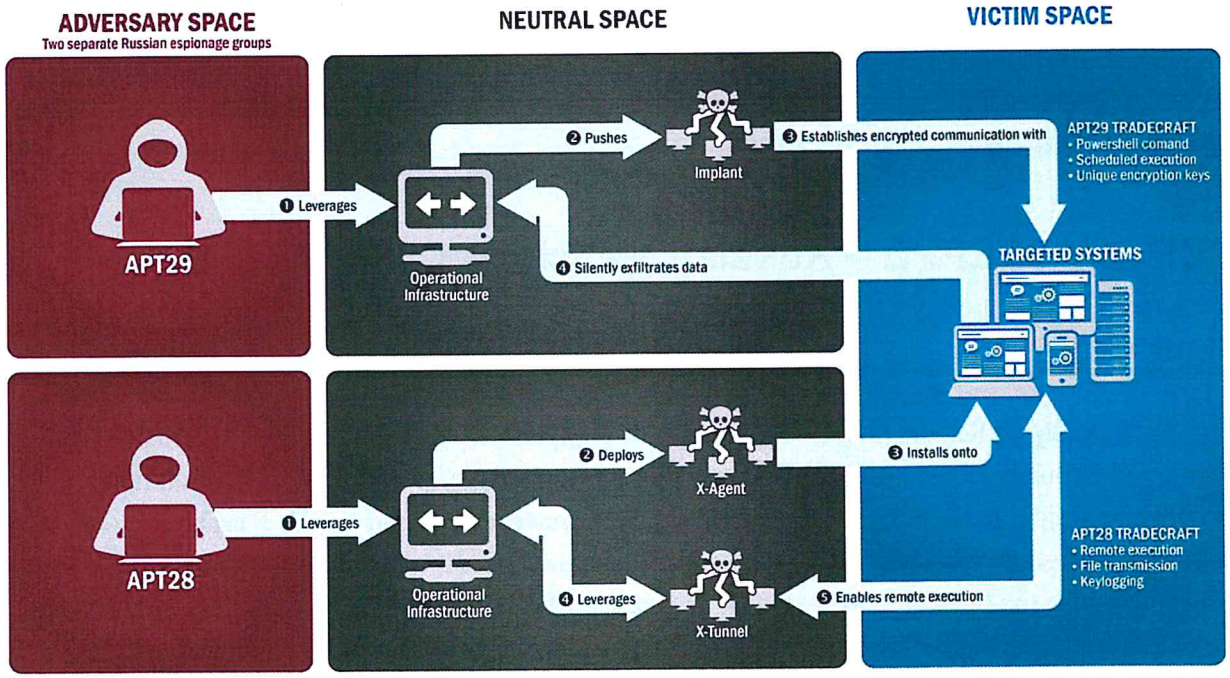


Figure 1: The tactics and techniques used by APT29 and APT 28 to conduct cyber intrusions against target systems

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.

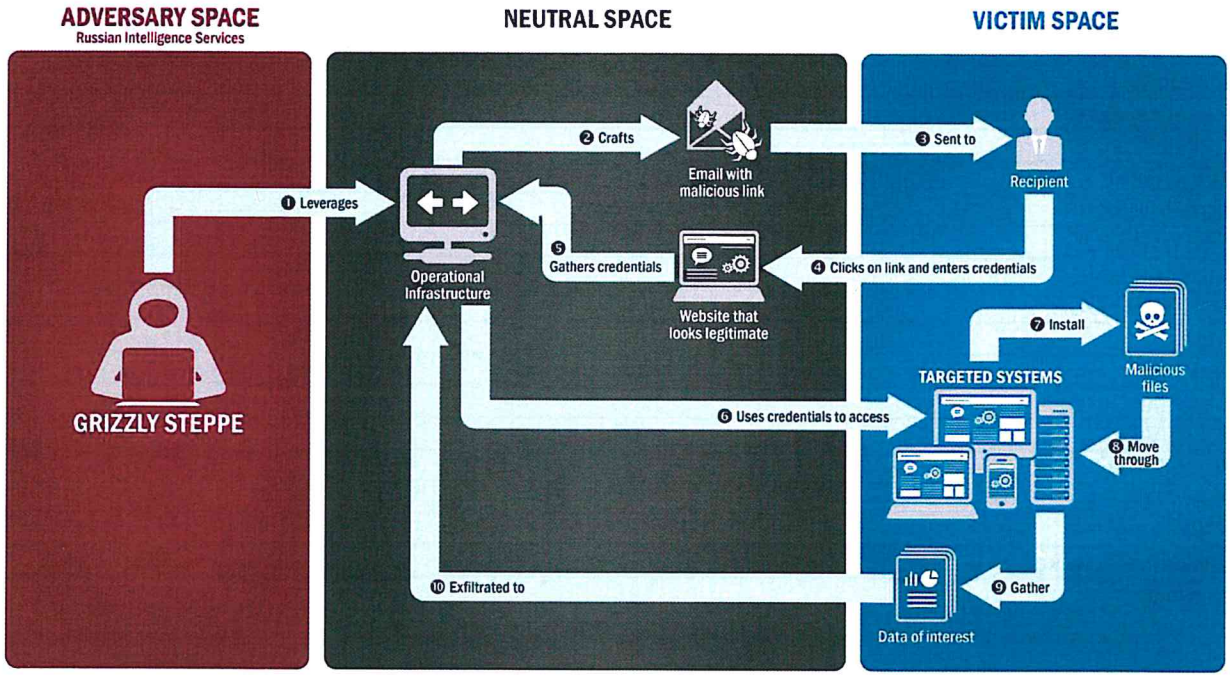


Figure 2: APT28's Use of Spearphishing and Stolen Credentials

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

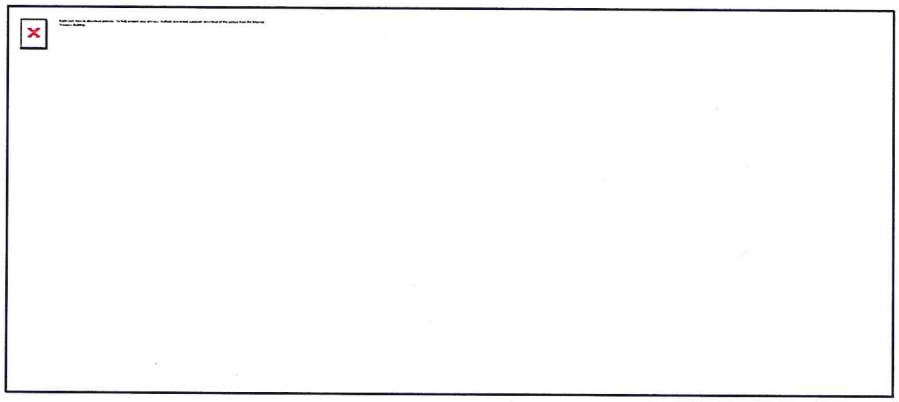
Feedback

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.

Pietranton, Kelsey L. EOP/NSC

From: Brookie, Graham H. EOP/NSC
nt: Thursday, December 29, 2016 3:05 PM
: Brookie, Graham H. EOP/NSC
Subject: FW: TREASURY SANCTIONS TWO INDIVIDUALS FOR MALICIOUS CYBER-ENABLED ACTIVITIES

From: U.S. Department of the Treasury <subscriptions@ustreas.service.govdelivery.com>
Sent: Thursday, December 29, 2016 2:26 PM
Subject: TREASURY SANCTIONS TWO INDIVIDUALS FOR MALICIOUS CYBER-ENABLED ACTIVITIES



U.S. TREASURY DEPARTMENT
OFFICE OF PUBLIC AFFAIRS

FOR IMMEDIATE RELEASE: December 29, 2016
CONTACT: Dawn Selak, Treasury Public Affairs, (202) 622-6490

TREASURY SANCTIONS TWO INDIVIDUALS FOR MALICIOUS CYBER-ENABLED ACTIVITIES

WASHINGTON – Building on the authority previously provided to the Secretary of the Treasury, the President amended Executive Order 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," which was issued by President Obama on April 1, 2015 to authorize sanctions against individuals and entities that threaten the national security, foreign policy, or economic health or financial stability of the United States through involvement in malicious cyber-enabled activities that constitute tampering with, altering, or causing a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions. In an Annex to the amended E.O., the President imposed sanctions on five entities and four individuals in response to the Government of Russia's interference with U.S. elections and processes in recent months.

'n a parallel action, today, the Treasury Department's Office of Foreign Assets Control (OFAC) imposed sanctions on two Russian individuals for engaging in malicious cyber-enabled activities pursuant to E.O. 13694. Specifically, Evgeniy Mikhailovich Bogachev and Aleksey Alekseyevich Belan are being designated for their activities related to the significant misappropriation of funds or economic resources, trade secrets,

personal identifiers, or financial information for private financial gain. As a result of today's action, any property or interests in property of the designated persons within U.S. jurisdiction must be blocked and U.S. persons are generally prohibited from engaging in transactions with them.

"The integrity and stability of our electronic systems are of utmost importance to our national security and we will hold accountable those who seek to compromise or tamper with those systems," said Treasury Secretary Jacob J. Lew. "Treasury will use all of its financial tools as part of the U.S. Government's effort to counter those who engage in malicious cyber activities against our financial system or our national institutions."

Today's actions are the first sanctions imposed under this authority. These measures reflect the continuing commitment of the United States Government to counter and deter the most significant cyber threats we face, including those who use cyber means to undermine democratic processes or institutions or to steal the financial and personal information of innocent individuals.

Evgeniy Mikhailovich Bogachev

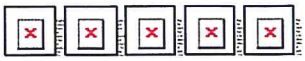
Evgeniy Mikhailovich Bogachev was designated for having engaged in significant malicious cyber-enabled misappropriation of financial information for private financial gain. Bogachev directly benefited from and enabled other cybercriminals to conduct their malicious cyber-enabled activities utilizing the Zeus malware, which he played a significant role in developing. He managed the distribution and sales of the Zeus malware, as well as tailoring subsequent versions of Zeus to meet his clients' needs.

Bogachev is also directly responsible for the development and use of Cryptolocker, a form of ransomware, which is known to have held over 120,000 U.S. victims' data hostage for financial gain. Bogachev and his cybercriminal associates are responsible for the theft of over $100 million from U.S. financial institutions and government agencies.

Aleksey Alekseyevich Belan

Aleksey Alekseyevich Belan engaged in the significant malicious cyber-enabled misappropriation of personal identifiers for private financial gain. Belan compromised the computer networks of at least three major United States-based e-commerce companies. Belan used his unauthorized access on the e-commerce company networks to steal user data, including email addresses, customer names, and encrypted passwords, belonging to approximately 200 million accounts worldwide. Belan actively engaged in successful efforts to sell the stolen information for private financial gain.

###



SUBSCRIBER SERVICES:
Manage Preferences | Unsubscribe | Help

U.S. Punishes Russia for Election Hacking, Ejecting Operatives
By DAVID E. SANGER DECEMBER 29, 2016

WASHINGTON — The Obama administration struck back at Russia on Thursday for its efforts to influence the 2016 election, ejecting 35 Russian intelligence operatives from the United States and imposing sanctions on Russia's two leading intelligence services, including four top officers of the military intelligence unit the White House believes ordered the attacks on the Democratic National Committee and other political organizations.

In a sweeping set of announcements, the United States was also expected to release evidence linking the cyberattacks to computer systems used by Russian intelligence. Taken together, the actions would amount to the strongest American response ever taken to a state-sponsored cyberattack aimed at the United States.

The sanctions were also intended to box in President-elect Donald J. Trump. Mr. Trump has consistently cast doubt that the Russian government had anything to do with the hacking of the D.N.C. or other political institutions, saying American intelligence agencies could not be trusted and suggesting that the hacking could have been the work of a "400-pound guy" lying in his bed.

Mr. Trump will now have to decide whether to lift the sanctions on the Russian intelligence agencies when he takes office next month, with Republicans in Congress among those calling for a public investigation into Russia's actions. Should Mr. Trump do so, it would require him to effectively reject the findings of his intelligence agencies.

Asked on Wednesday night at his Mar-a-Lago estate in Palm Beach, Fla., about reports of the impending sanctions, Mr. Trump said: "I think we ought to get on with our lives. I think that computers have complicated lives very greatly. The whole age of computer has made it where nobody knows exactly what is going on. We have speed, we have a lot of other things, but I'm not sure we have the kind, the security we need."

The Obama administration is also planning to release a detailed "joint analytic report" from the Federal Bureau of Investigation and the Department of Homeland Security that is clearly based in part on intelligence gathered by the National Security Agency. A more detailed report on the intelligence, ordered by President Obama, will be published in the next three weeks, though much of the detail — especially evidence collected from "implants" in Russian computer systems, tapped conversations and spies — is expected to remain classified.

Despite the fanfare and political repercussions surrounding the announcement, it is not clear how much real effect the sanctions may have, although they go well beyond the modest sanctions imposed against North Korea for its attack on Sony Pictures Entertainment two years ago.

Starting in March 2014, the United States and its Western allies levied sanctions against broad sectors of the Russian economy and blacklisted dozens of people, some of them close friends of President Vladimir V. Putin, after the Russian annexation of Crimea and its activities to destabilize Ukraine. Mr. Trump suggested in an interview with The New York Times earlier this year that he believed those sanctions were useless, and left open the possibility he might lift them.

Mr. Obama and his staff have debated for months when and how to impose what they call "proportionate" sanctions for the remarkable set of events that took place during the election, as well as how much of them to announce publicly. Several officials, including Vice President Joseph R. Biden Jr., have suggested that there may also be a covert response, one that would be obvious to Mr. Putin but not to the public.

While that may prove satisfying, many outside experts have said that unless the public response is strong enough to impose a real cost on Mr. Putin, his government and his vast intelligence apparatus, it might not deter further activity.

"They are concerned about controlling retaliation," said James A. Lewis, a cyberexpert at the Center for Strategic and International Studies in Washington.

The Obama administration was riven by an internal debate about how much of its evidence to make public. Although the announcement risks revealing sources and methods, it was the best way, some officials inside the administration argued, to make clear to a raft of other nations – including China, Iran and North Korea – that their activities can be tracked and exposed.

In the end, Mr. Obama decided to expand an executive order that he issued in April 2015, after the Sony hacking. He signed it in Hawaii on Thursday morning, specifically giving himself and his successor the authority to issue travel bans and asset freezes on those who "tamper with, alter, or cause a misappropriation of information, with a purpose or effect of interfering with or undermining election processes or institutions."

Mr. Obama used that order to immediately impose sanctions on four Russian intelligence officials: Igor Valentinovich Korobov, the current chief of a military intelligence agency, the G.R.U., and three deputies: Sergey Aleksandrovich Gizunov, the deputy chief of the G.R.U.; Igor Olegovich Kostyukov, a first deputy chief, and Vladimir Stepanovich Alekseyev, also a first deputy chief of the G.R.U.

But G.R.U. officials rarely travel to the United States, or keep their assets here, so the effects may be largely symbolic. It is also unclear if any American allies will impose parallel sanctions on Russia.

The administration also put sanctions on three companies and organizations that it said supported the hacking operations: the Special Technologies Center, a signals intelligence operation in St. Petersburg; a firm called Zor Security that is also known as Esage Lab; and the "Autonomous Non-commercial Organization Professional Association of Designers of Data Processing Systems," whose lengthy name, American officials said, was cover for a group that provided specialized training for the hacking.

"It is hard to do business around the world when you are named like this," a senior administration official with long experience in Russia sanctions said on Thursday morning. The official spoke on the condition of anonymity because of the sensitive nature of the intelligence.

But the question will remain whether the United States acted too slowly – and then, perhaps, with not enough force. Members of Hillary Clinton's election campaign argue that the distractions caused by the leakage of emails, showing infighting in the D.N.C., and later the private communications of John D. Podesta, the campaign chairman, absorbed an American press corps more interested in the leaks than in the phenomena of a foreign power marrying new cybertechniques with old-style information warfare.

Certainly the United States had early notice. The F.B.I. first informed the D.N.C. that it saw evidence that the committee's email systems had been hacked in the fall of 2015. Months of fumbling and slow responses followed. Mr. Obama said at a new conference he was first notified early this summer. But one of his top cyberaides met Russian officials in Geneva to complain about cyberactivity in April.

By the time the leadership of the D.N.C. woke up to what was happening, the G.R.U. had not only obtained those emails through a hacking group that has been closely associated with it for years, but, investigators say, also allowed them to be published on a number of websites, from a newly created one called "DC Leaks" to the far more established WikiLeaks. Meanwhile, several states reported the "scanning" of their voter databases – which American intelligence agencies also attributed to Russian hackers. But there is no evidence, American officials said, that Russia sought to manipulate votes or voter rolls on Nov. 8.

Mr. Obama decided not to issue sanctions ahead of the elections, for fear of Russian retaliation ahead of election day. Some of his aides now believe that was a mistake. But the president made clear before leaving for Hawaii that he planned to respond.

The question now is whether the response he has assembled will be more than just symbolic, deterring not only Russia but others who might attempt to influence future elections.

Withdrawal Marker
Obama Presidential Library

FORM	SUBJECT/TITLE	PAGES	DATE	RESTRICTION(S)
Timeline	[Timeline of events for December 27th to December 31st]	3	N.D.	P1/b1;

This marker identifies the original location of the withdrawn item listed above. For a complete list of items withdrawn from this folder, see the Withdrawal/Redaction Sheet at the front of the folder.

COLLECTION:
National Security Council - Homeland Security and Counter-Terrorism Directorate

SERIES:
Monaco, Lisa - Subject Files

FOLDER TITLE:
Russia Response Rollout

FRC ID:
70724

OA Num.:
W1100

NARA Num.:

FOIA IDs and Segments:

22-26844-F

22-26842-F

22-26841-F

22-26840-F 3

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

Deed of Gift Restrictions

A. Closed by Executive Order 13526 governing access to national security information.
B. Closed by statute or by the agency which originated the document.
C. Closed in accordance with restrictions contained in donor's deed of gift.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Records Not Subject to FOIA

Court Sealed - The document is withheld under a court seal and is not subject to the Freedom of Information Act.

POTUS / FACT SHEET

12/29/2016
~~11:15 am~~ 11 6pm FINAL

Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment

Today, I have ordered a number of actions in response to the Russian government's aggressive harassment of U.S. officials and cyber operations aimed at the U.S. election. These actions follow repeated private and public warnings that we have issued to the Russian government, and are a necessary and appropriate response to efforts to harm U.S. interests in violation of established international norms of behavior.

All Americans should be alarmed by Russia's actions. In October, my Administration publicized our assessment that Russia took actions intended to interfere with the U.S. election process. These data theft and disclosure activities could only have been directed by the highest levels of the Russian government. Moreover, our diplomats have experienced an unacceptable level of harassment in Moscow by Russian security services and police over the last year. Such activities have consequences. Today, I have ordered a number of actions in response.

I have issued an executive order that provides additional authority for responding to certain cyber activity that seeks to interfere with or undermine our election processes and institutions, or those of our allies or partners. Using this new authority, I have sanctioned nine entities and individuals: the GRU and the FSB, two Russian intelligence services; four individual officers of the GRU; and three companies that provided material support to the GRU's cyber operations. In addition, the Secretary of the Treasury is designating two Russian individuals for using cyber-enabled means to cause misappropriation of funds and personal identifying information. The State Department is also shutting down two Russian compounds, in Maryland and New York, used by Russian personnel for intelligence-related purposes, and is declaring "persona non grata" 35 Russian intelligence operatives. Finally, the Department of Homeland Security and the Federal Bureau of Investigation are releasing declassified technical information on Russian civilian and military intelligence service cyber activity, to help network defenders in the United States and abroad identify, detect, and disrupt Russia's global campaign of malicious cyber activities.

These actions are not the sum total of our response to Russia's aggressive activities. We will continue to take a variety of actions at a time and place of our choosing, some of which will not be publicized. In addition to holding Russia accountable for what it has done, the United States and friends and allies around the world must work together to oppose Russia's efforts to undermine established international norms of behavior, and interfere with democratic governance. To that end, my Administration will be providing a report to Congress in the coming days about Russia's efforts to interfere in our election, as well as malicious cyber activity related to our election cycle in previous elections.

12/29/2016
~~9:30 am~~ 1:10pm FINAL

FACT SHEET: Actions in Response to Russian Malicious Cyber Activity and Harassment

Today, President Obama authorized a number of actions in response to the Russian government's aggressive harassment of U.S. officials and cyber operations aimed at the U.S. election in 2016. Russia's cyber activities were intended to influence the election, erode faith in U.S. democratic institutions, sow doubt about the integrity of our electoral process, and undermine confidence in the institutions of the U.S. government. These actions are unacceptable and will not be tolerated.

Sanctioning Malicious Russian Cyber Activity

In response to the threat to U.S. national security posed by Russian interference in our elections, the President has approved an amendment to Executive Order 13964. As originally issued in April 2015, this **Executive Order** created a new, targeted authority for the U.S. government to respond more effectively to the most significant of cyber threats, particularly in situations where malicious cyber actors operate beyond the reach of existing authorities. The original Executive Order focused on cyber-enabled malicious activities that:

- Harm or significantly compromise the provision of services by entities in a critical infrastructure sector;
- Significantly disrupt the availability of a computer or network of computers (for example, through a distributed denial-of-service attack); or
- Cause a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain (for example, by stealing large quantities of credit card information, trade secrets, or sensitive information).

The increasing use of cyber-enabled means to undermine democratic processes at home and abroad, as exemplified by Russia's recent activities, has made clear that a tool explicitly targeting attempts to interfere with elections is also warranted. As such, the President has approved amending Executive Order 13964 to authorize sanctions on those who:

- Tamper with, alter, or cause a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions.

Using this new authority, the President has sanctioned nine entities and individuals: two Russian intelligence services (the GRU and the FSB); four individual officers of the GRU; and three companies that provided material support to the GRU's cyber operations.

- The Main Intelligence Directorate (a.k.a. Glavnoe Razvedyvatel'noe Upravlenie) (a.k.a. GRU) is involved in external collection using human intelligence officers and a variety of technical tools, and is designated for tampering, altering, or causing a misappropriation of

information with the purpose or effect of interfering with the 2016 U.S. election processes.

- The Federal Security Service (a.k.a. Federalnaya Sluzhba Bezopasnosti) (a.k.a FSB) assisted the GRU in conducting the activities described above.

- The three other entities include the Special Technology Center (a.k.a. STLC, Ltd. Special Technology Center St. Petersburg) assisted the GRU in conducting signals intelligence operations; Zorsecurity (a.k.a. Esage Lab) provided the GRU with technical research and development; and the Autonomous Noncommercial Organization "Professional Association of Designers of Data Processing Systems" (a.k.a. ANO PO KSI) provided specialized training to the GRU.

- Sanctioned individuals include Igor Valentinovich Korobov, the current Chief of the GRU; Sergey Aleksandrovich Gizunov, Deputy Chief of the GRU; Igor Olegovich Kostyukov, a First Deputy Chief of the GRU; and Vladimir Stepanovich Alexseyev, also a First Deputy Chief of the GRU.

In addition, the Department of the Treasury is designating two Russian individuals, Evgeniy Bogachev and Aleksey Belan, under a pre-existing portion of the Executive Order for using cyber-enabled means to cause misappropriation of funds and personal identifying information.

- Evgeniy Mikhailovich Bogachev is designated today for having engaged in significant malicious cyber-enabled misappropriation of financial information for private financial gain. Bogachev and his cybercriminal associates are responsible for the theft of over $100 million from U.S. financial institutions, Fortune 500 firms, universities, and government agencies.

- Aleksey Alekseyevich Belan engaged in the significant malicious cyber-enabled misappropriation of personal identifiers for private financial gain. Belan compromised the computer networks of at least three major United States-based e-commerce companies.

Responding to Russian Harassment of U.S. Personnel

Over the past two years, harassment of our diplomatic personnel in Russia by security personnel and police has increased significantly and gone far beyond international diplomatic norms of behavior. Other Western Embassies have reported similar concerns. In response to this harassment, the President has authorized the following actions:

- Today the State Department declared 35 Russian government officials from the Russian Embassy in Washington and the Russian Consulate in San Francisco "persona non grata." They were acting in a manner inconsistent with their diplomatic status. Those individuals and their families were given 72 hours to leave the United States.

- In addition to this action, the Department of State has provided notice that as of noon on Friday, December 30, Russian access will be denied to two Russian government-owned compounds, one in Maryland and one in New York.

Raising Awareness About Russian Malicious Cyber Activity

The Department of Homeland Security and Federal Bureau of Investigation are releasing a Joint Analysis Report (JAR) that contains declassified technical information on Russian civilian and military intelligence services' malicious cyber activity, to better help network defenders in the United States and abroad identify, detect, and disrupt Russia's global campaign of malicious cyber activities.

- The JAR includes information on computers around the world that Russian intelligence services have co-opted without the knowledge of their owners in order to conduct their malicious activity in a way that makes it difficult to trace back to Russia. In some cases, the cybersecurity community was aware of this infrastructure, in other cases, this information is newly declassified by the U.S. government.

- The report also includes data that enables cybersecurity firms and other network defenders to identify certain malware that the Russian intelligence services use. Network defenders can use this information to identify and block Russian malware, forcing the Russian intelligence services to re-engineer their malware. This information is newly de-classified.

- Finally, the JAR includes information on how Russian intelligence services typically conduct their activities. This information can help network defenders better identify new tactics or techniques that a malicious actor might deploy or detect and disrupt an ongoing intrusion.

This information will allow network defenders to take specific steps that can often block new activity or disrupt on-going intrusions by Russian intelligence services. DHS and FBI are encouraging security companies and private sector owners and operators to use this JAR and look back within their network traffic for signs of malicious activity. DHS and FBI are also encouraging security companies and private sector owners and operators to leverage these indicators in proactive defense efforts to block malicious cyber activity before it occurs. DHS has already added these indicators to their Automated Indicator Sharing service.

Cyber threats pose one of the most serious economic and national security challenges the United States faces today. For the last eight years, this Administration has pursued a comprehensive strategy to confront these threats. And as we have demonstrated by these actions today, we intend to continue to employ the full range of authorities and tools, including diplomatic engagement, trade policy tools, and law enforcement mechanisms, to counter the threat posed by malicious cyber actors, regardless of their country of origin, to protect the national security of the United States.

Monaco, Lisa O. EOP/WHO

From: Price, Ned C. EOP/NSC
Sent: Thursday, December 29, 2016 2:23 PM
To: DL-WHO-Press; #SUITE; #RUSSIA
Subject: FW: STATEMENT: Department of State Actions in Response to Russian Harassment

From: State Department Press Office [mailto:usstatebpa@subscriptions.fcg.gov]
Sent: Thursday, December 29, 2016 2:20 PM
To: Price, Ned C. EOP/NSC <Edward_C_Price@nsc.eop.gov>
Subject: STATEMENT: Department of State Actions in Response to Russian Harassment

U.S. DEPARTMENT OF STATE

Office of the Spokesperson

For Immediate Release

STATEMENT BY MARK TONER, DEPUTY SPOKESPERSON

December 29, 2016

Department of State Actions in Response to Russian Harassment

The State Department today declared persona non grata 35 Russian officials operating in the United States who were acting in a manner inconsistent with their diplomatic or consular status. The Department also informed the Russian Government that it would deny Russian personnel access to two recreational compounds in the United States owned by the Russian Government.

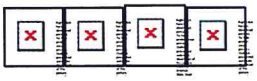
The Department took these actions as part of a comprehensive response to Russia's interference in the U.S. election and to a pattern of harassment of our diplomats overseas that has increased over the last four years, including a significant increase in the last 12 months. This harassment has involved arbitrary police stops, physical assault, and the broadcast on State TV of personal details about our personnel that put them at risk. In addition, the Russian Government has impeded our diplomatic operations by, among other actions: forcing the closure of 28 American corners which hosted cultural programs and English-language teaching; blocking our efforts to begin the construction of a new, safer

facility for our Consulate General in St. Petersburg; and rejecting requests to improve perimeter security at the current, outdated facility in St. Petersburg.

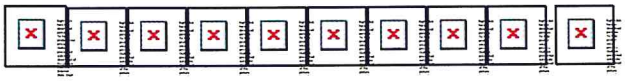
Today's actions send a clear message that such behavior is unacceptable and will have consequences.

###

Stay connected with the State Department Office of Press Relations:



Stay connected with the State Department:



Q/A

012

Withdrawal Marker
Obama Presidential Library

FORM	SUBJECT/TITLE	PAGES	DATE	RESTRICTION(S)
Draft	Cyber: Response to Russian Malicious Cyber Activity and Harassment	16	12/29/2016	P5;

This marker identifies the original location of the withdrawn item listed above. For a complete list of items withdrawn from this folder, see the Withdrawal/Redaction Sheet at the front of the folder.

COLLECTION:
National Security Council - Homeland Security and Counter-Terrorism Directorate

SERIES:
Monaco, Lisa - Subject Files

FOLDER TITLE:
Russia Response Rollout

FRC ID:
70724

OA Num.:
W1100

NARA Num.:

FOIA IDs and Segments:

22-26844-F

22-26842-F

22-26841-F

22-26840-F 3

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

Deed of Gift Restrictions

A. Closed by Executive Order 13526 governing access to national security information.
B. Closed by statute or by the agency which originated the document.
C. Closed in accordance with restrictions contained in donor's deed of gift.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Records Not Subject to FOIA

Court Sealed - The document is withheld under a court seal and is not subject to the Freedom of Information Act.

Withdrawal Marker
Obama Presidential Library

FORM	SUBJECT/TITLE	PAGES	DATE	RESTRICTION(S)
Email	From Avril D. Haines to Lisa O. Monaco et al., re: Per the Q/A discussed	1	12/29/2016	P5;

This marker identifies the original location of the withdrawn item listed above. For a complete list of items withdrawn from this folder, see the Withdrawal/Redaction Sheet at the front of the folder.

COLLECTION:
National Security Council - Homeland Security and Counter-Terrorism Directorate

SERIES:
Monaco, Lisa - Subject Files

FOLDER TITLE:
Russia Response Rollout

FRC ID:
70724

OA Num.:
W1100

NARA Num.:

FOIA IDs and Segments:

22-26844-F

22-26842-F

22-26841-F

22-26840-F 3

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

Deed of Gift Restrictions

A. Closed by Executive Order 13526 governing access to national security information.
B. Closed by statute or by the agency which originated the document.
C. Closed in accordance with restrictions contained in donor's deed of gift.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Records Not Subject to FOIA

Court Sealed - The document is withheld under a court seal and is not subject to the Freedom of Information Act.

Withdrawal Marker
Obama Presidential Library

FORM	SUBJECT/TITLE	PAGES	DATE	RESTRICTION(S)
Draft	Cyber: Response to Russian Malicious Cyber Activity and Harassment	14	N.D.	P5;

This marker identifies the original location of the withdrawn item listed above. For a complete list of items withdrawn from this folder, see the Withdrawal/Redaction Sheet at the front of the folder.

COLLECTION:
National Security Council - Homeland Security and Counter-Terrorism Directorate

SERIES:
Monaco, Lisa - Subject Files

FOLDER TITLE:
Russia Response Rollout

FRC ID:
70724

OA Num.:
W1100

NARA Num.:

FOIA IDs and Segments:

22-26844-F

22-26842-F

22-26841-F

22-26840-F 3

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

Deed of Gift Restrictions

A. Closed by Executive Order 13526 governing access to national security information.
B. Closed by statute or by the agency which originated the document.
C. Closed in accordance with restrictions contained in donor's deed of gift.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Records Not Subject to FOIA

Court Sealed - The document is withheld under a court seal and is not subject to the Freedom of Information Act.

DNI/DHS/FBI

0110

Withdrawal Marker
Obama Presidential Library

FORM	SUBJECT/TITLE	PAGES	DATE	RESTRICTION(S)
Draft	Draft Joint DHS/DNI/FBI Press Statement	2	12/27/2016	P1/b1;

This marker identifies the original location of the withdrawn item listed above. For a complete list of items withdrawn from this folder, see the Withdrawal/Redaction Sheet at the front of the folder.

COLLECTION:
National Security Council - Homeland Security and Counter-Terrorism Directorate

SERIES:
Monaco, Lisa - Subject Files

FOLDER TITLE:
Russia Response Rollout

FRC ID:
70724

OA Num.:
W1100

NARA Num.:

FOIA IDs and Segments:

22-26844-F

22-26842-F

22-26841-F

22-26840-F 3

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

Deed of Gift Restrictions

A. Closed by Executive Order 13526 governing access to national security information.
B. Closed by statute or by the agency which originated the document.
C. Closed in accordance with restrictions contained in donor's deed of gift.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Records Not Subject to FOIA

Court Sealed - The document is withheld under a court seal and is not subject to the Freedom of Information Act.

JAR/Exec. Summary

Withdrawal Marker
Obama Presidential Library

FORM	SUBJECT/TITLE	PAGES	DATE	RESTRICTION(S)
Draft	Joint Analysis Report, re: Operation Grizzly Steppe - Russian Malicious Cyber Activity	12	12/29/2016	P5;

This marker identifies the original location of the withdrawn item listed above. For a complete list of items withdrawn from this folder, see the Withdrawal/Redaction Sheet at the front of the folder.

COLLECTION:
National Security Council - Homeland Security and Counter-Terrorism Directorate

SERIES:
Monaco, Lisa - Subject Files

FOLDER TITLE:
Russia Response Rollout

FRC ID:
70724

OA Num.:
W1100

NARA Num.:

FOIA IDs and Segments:

22-26844-F

22-26842-F

22-26841-F

22-26840-F 3

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

Deed of Gift Restrictions

A. Closed by Executive Order 13526 governing access to national security information.
B. Closed by statute or by the agency which originated the document.
C. Closed in accordance with restrictions contained in donor's deed of gift.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Records Not Subject to FOIA

Court Sealed - The document is withheld under a court seal and is not subject to the Freedom of Information Act.

Withdrawal Marker
Obama Presidential Library

FORM	SUBJECT/TITLE	PAGES	DATE	RESTRICTION(S)
Draft	Operation Grizzly Steppe	6	12/27/2016	P1/b1; P5;

This marker identifies the original location of the withdrawn item listed above. For a complete list of items withdrawn from this folder, see the Withdrawal/Redaction Sheet at the front of the folder.

COLLECTION:
National Security Council - Homeland Security and Counter-Terrorism Directorate

SERIES:
Monaco, Lisa - Subject Files

FOLDER TITLE:
Russia Response Rollout

FRC ID:
70724

OA Num.:
W1100

NARA Num.:

FOIA IDs and Segments:

22-26844-F

22-26842-F

22-26841-F

22-26840-F 3

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

Deed of Gift Restrictions

A. Closed by Executive Order 13526 governing access to national security information.
B. Closed by statute or by the agency which originated the document.
C. Closed in accordance with restrictions contained in donor's deed of gift.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Records Not Subject to FOIA

Court Sealed - The document is withheld under a court seal and is not subject to the Freedom of Information Act.

PRIOR STATEMENTS

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
Public Affairs Office
LEADING INTELLIGENCE INTEGRATION

Remarks as delivered by
The Honorable James R. Clapper
Director of National Intelligence

Senate Select Committee on Intelligence – IC's Worldwide Threat Assessment
Opening Statement

Tuesday Feb 9, 2016
2:30 p.m.

Hart Senate Office Building – Washington DC

Chairman Burr and Vice Chairman Feinstein, members of the committee. First, Chairman Burr, thanks very much for the acknowledgment particularly of the great men and women of the US intelligence community whom we represent here today. And it's very appropriate that you do that for the great work that they do. And, Madam Vice Chairman, thank you very much for acknowledging my long service. That's very gracious of you.

We're here today to update you on some, but certainly not all, of the pressing intelligence and national security issues facing our nation, many of which you both alluded to, and so there will be a certain amount of echo here I guess. In the interest of time, and to get to your questions, we'll just cover some of the wave tops, and mine will be the only opening statements, so we can go to your questions.

I apologize in advance to the crossover members who were present this morning at the Senate Armed Services Committee, but in the highest traditions of "that's our story and we're sticking to it," it'll be the same statement.

As I said last year, unpredictable instability has become the "new normal," and this trend will continue for the foreseeable future. Violent extremists are operationally active in about 40 countries. Seven countries are experiencing a collapse of central government authority, and 14 others face regime-threatening, or violent, instability or both. Another 59 countries face a significant risk of instability through 2016.

The record level of migrants, more than one million arriving in Europe, is likely to grow further this year. Migration and displacement will strain countries in Europe, Asia, Africa and the Americas. There are now some 60 million people who are considered displaced globally.

Extreme weather, climate change, environmental degradation, rising demand for food and water, poor policy decisions and inadequate infrastructure will magnify this instability. Infectious diseases and vulnerabilities in the global supply chain for medical countermeasures will continue to pose threats. For example, the Zika virus, first detected in the Western Hemisphere in 2014, has reached the US and is projected to cause up to four million cases in this hemisphere.

With that preface, I want to briefly comment on both technology and cyber specifically. Technological innovation during the next few years will have an even more significant impact on our way of life. This innovation is central to our economic prosperity, but it will bring new security vulnerabilities. The Internet of Things will connect tens of billions of new physical devices that could be exploited. Artificial intelligence will enable computers to make autonomous decisions about data and physical systems, and potentially disrupt labor markets.

Russia and China continue to have the most sophisticated cyber programs. China continues cyber espionage against the United States. Whether China's commitment of last September moderates its economic espionage, remains to be seen. Iran and North Korea continue to conduct cyber espionage as they enhance their attack capabilities.

Non-state actors also pose cyber threats. ISIL has used cyber to its great advantage, not only for recruitment and propaganda, but also to hack and release sensitive information about US military personnel. As a non-state actor, ISIL displays unprecedented online proficiency. Cybercriminals remain the most pervasive cyber threat to the US financial sector. They use cyber to conduct theft, extortion and other criminal activities.

Turning to terrorism, there are now more Sunni violent extremist groups, members and safe havens than at any time in history. The rate of foreign fighters traveling to the conflict zones in Syria and Iraq in the past few years is without precedent. At least 38,200 foreign fighters—including at least 6,900 from Western countries—have traveled to Syria from at least 120 countries since the beginning of the conflict in 2012.

As we saw in the November Paris attacks, returning foreign fighters with firsthand battlefield experience pose a dangerous operational threat. ISIL has demonstrated sophisticated attack tactics and tradecraft.

ISIL, including its eight established and several more emerging branches, has become the preeminent global terrorist threat. ISIL has attempted or conducted scores of attacks outside of Syria and Iraq in the past 15 months. And ISIL's estimated strength globally exceeds that of al-Qa'ida. ISIL's leaders are determined seek to strike the US homeland—beyond inspiring homegrown violent extremist attacks. Although the US is a harder target than Europe, ISIL external operations remains a critical factor in our threat assessments in 2016.

Al-Qa'ida's affiliates also have proven resilient. Despite counterterrorism pressure that has largely decimated the "core" leadership in Afghanistan and Pakistan, al-Qa'ida affiliates are positioned to make gains in 2016. Al-Qa'ida in the Arabian Peninsula (AQAP) and the al-Nusrah Front – the al-Qa'ida chapter in Syria, are the two most capable al-Qai'da branches.

The increased use by violent extremists of encrypted and secure Internet and mobile-based technologies enables terrorist actors to "go dark" and serves to undercut intelligence and law enforcement efforts.

Iran continues to be the foremost state sponsor of terrorism and exert its influence in regional crises in the mid-East through the Islamic Revolutionary Guard Corps—Qods Force, its terrorist

partner Lebanese Hezbollah, and proxy groups. Iran and Hezbollah remain a continuing terrorist threat to US interests and partners worldwide.

We saw firsthand the threat posed in the United States by homegrown violent extremists in the July attack in Chattanooga and the attack in San Bernardino.

In 2014, the FBI arrested nine ISIL supporters. And in 2015, that number increased over fivefold.

Turning to weapons of mass destruction, North Korea continues to conduct test activities with concern to United States. On Saturday evening, Pyongyang conducted a satellite launch and subsequently claimed that the satellite was successfully placed in orbit. In addition, last month, North Korea carried out its fourth nuclear test claiming it was a "hydrogen bomb." But the yield was too low for it to have been a successful test of a staged thermonuclear device. Pyongyang continues to produce fissile material and develop a submarine-launched ballistic missile. It is also committed to developing a long-range, nuclear-armed missile that is capable of posing a direct threat to the United States, although the system has not been flight-tested.

Despite its economic challenges, Russia continues its aggressive military modernization program. It has the largest, and most capable, foreign nuclear-armed ballistic missile force. It has developed a cruise missile that violates the Intermediate-Range Nuclear Forces or INF Treaty.

China continues to modernize its nuclear missile force and is striving for a secure, second-strike capability. It continues to profess a “no first use” doctrine.

The Joint Comprehensive Plan of Action, or JCPOA, provides us much greater transparency into Iran’s fissile material production. It increases the time the Iranians would need to produce enough highly enriched uranium for a nuclear weapon, from a few months to about a year. Iran probably views the JCPOA as a means to remove sanctions while preserving nuclear capabilities. Iran’s perception of how the JCPOA helps it achieve its overall strategic goals will dictate the level of its adherence to the agreement over time.

Chemical weapons continue to pose a threat in Syria and Iraq. Damascus has used chemicals against the opposition on multiple occasions since Syria joined the Chemical Weapons Convention. ISIL has also used toxic chemicals in Iraq and Syria, including the blister agent sulfur mustard—the first time an extremist group has produced and used a chemical warfare agent in an attack since Aum Shinrikyo used sarin in Japan in 1995.

Turning to space and counter-space, there are about 80 countries are now engaged in the space domain. Russia and China understand how our military fights and how heavily we rely on space. They are each pursuing destructive and disruptive anti-satellite systems. China continues to make progress on its anti-satellite missile program.

Moving to counterintelligence, the threat from foreign intelligence entities, both state and non-state, is persistent, complex, and evolving. Targeting and collection of US political, military, economic, and technical information by foreign intelligence services continues unabated. Russia

and China pose the greatest threat, followed by Iran and Cuba on a lesser scale. As well, the threat from insiders taking advantage of their access to collect and remove sensitive national security information will remain a persistent challenge for us.

With respect to transnational organized crime, I want to touch on one issue, specifically drug trafficking. Southwest border seizures of heroin in the United States have doubled since 2010. Over 10,000 people died of heroin overdoses in 2014—much of it laced with fentanyl, which is 30 to 50 times more potent than heroin. In that same year, more than 28,000 died from opioid overdoses. Cocaine production in Colombia, from which most US supplies originate, has increased significantly.

Now, let me quickly move through a few regional issues.

In East Asia, China's leaders are pursuing an active foreign policy while dealing with much slower economic growth. Chinese leaders have also embarked on the most ambitious military reforms in China's history. Regional tension will continue as China pursues construction at its outposts in the South China Sea.

Russia has demonstrated its military capabilities to project itself as a global power, command respect from the West, maintain domestic support for the regime, and advance Russian interests globally. Moscow's objectives in Ukraine will probably remain unchanged, including maintaining long-term influence over Kiev and frustrating its attempts to integrate into Western institutions. Putin is the first leader since Stalin to expand Russia's territory.

Moscow's military venture into Syria marks its first use since its foray into Afghanistan of significant expeditionary combat power outside the post-Soviet space. Its interventions demonstrate the improvements in Russian military capabilities and the Kremlin's confidence in using them.

Moscow faces the reality, however, of economic recession, driven in large part by falling oil prices, as well as sanctions. Russia's nearly 4 percent GDP contraction last year will probably extend into 2016.

In the Middle East and South Asia, there are more cross-border military operations underway in the mid-East region than at any time since the 1973 Arab-Israeli War. Anti-ISIL forces in Iraq will probably make incremental gains through this spring, similar to those made in Bayji and Ramadi in the past few months. ISIL is now somewhat on the defensive, and its territory and manpower are shrinking, but it remains a formidable threat.

In Syria, pro-regime forces have the initiative, having made some strategic gains near Aleppo and Latakia in the north, as well as in southern Syria. Manpower shortages will continue to undermine the Syrian regime's ability to accomplish strategic battlefield objectives. The opposition has less equipment and firepower, and its groups lack unity. They sometimes have competing battlefield interests and fight among themselves. Meanwhile, some 250,000 people have been killed as this war has dragged on.

The humanitarian situation in Syria continues to deteriorate. As of last month, there are approximately 4.4 million Syrian refugees and another 6.5 million internally displaced persons, which together represent about half of Syria's preconflict population.

In Libya, despite the December agreement to form a new "Government of National Accord," establishing authority and security across the country will be difficult at best, with hundreds of militia groups operating throughout the country. ISIL has established one of its most developed branch outside of Syria and Iraq in Libya and maintains a presence in Surt, Benghazi, Tripoli, and other areas of the country.

In Yemen, the conflict will probably remain stalemated through at least mid-2016. Meanwhile, AQAP and ISIL's affiliates in Yemen have exploited the conflict and the collapse of government authority to recruit and expand territorial control. The country's economic and humanitarian situation also continues to deteriorate.

Iran deepened its involvement in the Syrian, Iraq, and Yemeni conflicts in 2015. It also increased military cooperation with Russia, highlighted by its battlefield alliance in Syria in support of the regime. Iran's Supreme Leader continues to view the United States as a major threat. We assess that his views will not change despite the implementation of the JCPOA deal, the exchange of detainees, and the release of the 10 U.S. Sailors.

In South Asia, Afghanistan is at serious risk of a political breakdown during 2016, occasioned by mounting political, economic, and security challenges. Waning political cohesion, increasingly assertive local powerbrokers, financial shortfalls, and sustained countrywide Taliban attacks are eroding stability.

Needless to say, there are many more threats to US interests worldwide that we can address, most of which are covered in our Statement for the Record. But I'll stop this litany of doom and open to your questions.

Needless to say, there are many more threats to US interests worldwide that we can address, most of which are covered in our Statement for the Record. But I'll stop this litany of doom and open to your questions.

Before I do that, I do want to answer one question that Madam Vice Chairman asked about the state of the community now versus five years ago. I would like to think that we are better as a community, just from the simple proposition of the sum being greater than the parts, because we operate as an integrated enterprise. And others may have a comment on that and none of them are unwilling to disagree with me, but that's my view. So, I'll stop there and open to your questions.

###

THE ASPEN INSTITUTE

ASPEN SECURITY FORUM 2016

THE VIEW FROM THE WEST WING

Aspen Meadows Campus
Greenwald Pavilion
Aspen, Colorado

Saturday, July 30, 2016

LIST OF PARTICIPANTS

CLARK ERVIN
Executive Director, Homeland Security Program
The Aspen Institute

WALTER ISAACSON
President and CEO
The Aspen Institute

LISA MONACO
Assistant to the President for Homeland Security and Counterterrorism

* * * * *

THE VIEW FROM THE WEST WING

(2:15 p.m.)

MR. ERVIN: All right everyone. We will get started, if you could make your way to your seats, please. Well, as I think you all know by now, I am Clark Ervin, the Executive Director of the Homeland Security Program here at the Aspen Institute and the organizer of the Aspen Security Forum. I want to thank all of you for being with us for these past three days.

Every year, it seems as if world events conspire to underscore just how important the Aspen Security Forum is. And I want you all, please, to join me in thanking our sponsors and thanking our speakers and moderators for three absolutely riveting days of conversation.

(Applause)

MR. ERVIN: It's very appropriate that our final conversation is moderated by our President and CEO, Walter Isaacson. So Walter, take it away.

MR. ISAACSON: Thank you very much.

(Applause)

MR. ISAACSON: And it's not only a great honor to have Lisa Monaco here, but it's a great personal pleasure. Most of the people I've met working in government, great servants, really diligent, but nobody is like Lisa who combines being both nice, level-headed, smart but also very diligent, so diligent that I said, "What did you do today?" She said, "I spent three hours on a secure conference call," so while the rest of us were hiking, so.

MS. MONACO: It's okay.

(Laughter)

MR. ISAACSON: So thank you and welcome.

MS. MONACO: Thanks very much. It's great to be here. It's a credit to you and to Clark and to the whole team for putting on yet another great event. It's also a rare privilege for me to get outside of what is commonly referred to my cave or bunker in the White House which has no windows, let alone a beautiful tent. So it's great to be here. Thank you.

MR. ISAACSON: It's great. If we could start with Syria, we've heard today --

(Laughter)

MR. ISAACSON: -- or the threat of bears, we could do that. But we've heard at this conference that we really are making headway against ISIL in Syria. Do you worry about a resurgence of Al-Qaeda if that happens?

MS. MONACO: I do. I do, and I should say, you know, we've talked rightly a lot about the threat from ISIL and I am sure we'll get into more of that here and the hybrid threat that it presents. But I think any discussion of the terrorism threat that we face today has got to also underscore the threat, the continued threat we face from Al-Qaeda. Now John Brennan talked about this yesterday that Al-Qaeda core while greatly decimated, Al-Qaeda remains a lethal organization with its affiliates like AQAP and others.

But what I think we really need to underscore is the fact that Al-Nusra, which is in fact Al-Qaeda in Syria, is a threat to us. It has established a growing safe haven in Syria and they have taken advantage of the chaos in Syria. People will remember that in 2014, when we began our military operations in Syria and Iraq, we did so against ISIL. But we also simultaneously undertook actions and strikes against a group of Al-Qaeda veterans who had moved quite deliberately from the Afghanistan-Pakistan region to Syria for the expressed purpose of taking advantage of that ungoverned space.

MR. ISAACSON: How closely are they aligned or they're competitors, ISIL and Al-Qaeda, in Syria?

MS. MONACO: So they're competitors at this stage. And you got into this a little bit with Dina did with John yesterday. And I think we have to constantly be watching that relationship, but we should not be take our -- we should not take our eye off the ball and let any success against ISIL, which we are having substantial success and we've got momentum against ISIL in both Iraq and Syria. But we should not, and we should be very careful that that success does not also create a vacuum for Al-Qaeda in Syria.

MR. ISAACSON: How are the threats between -- from ISIL versus Al-Nusra, how are they different?

MS. MONACO: So I think -- and this has been also been talked about to some degree, but I think it's important to remember ISIL presents what I call a hybrid threat. It is at once a terrorist group most -- most assuredly, engaging in directed and complex attacks like we saw in Brussels and Paris and other places. It is an insurgent army undertaking military tactics and operations and taking swaths of territory, although less now than before, but it is also a social phenomenon. And it's this last piece that I think is -- makes it a distinguishing -- is the distinguishing factor in the threat that it poses. Its ability to utilize the online space and frankly to digitize the threat that we face is -- makes me believe that we have -- we have now confronted and are in a new phase of the threat that we face. We're in a moment that's different from one that I've seen.

Now ISIL at once is trying to do directed attacks and complex attacks as we've seen, but they're also extolling their followers and their adherence to undertake attacks wherever they are, and to do so without needing to travel, to train, to become vetted or undergo any type of discipline, but rather to undertake terrorist attacks wherever they are using the tools of our everyday life. We saw Mohammad Adnani extol followers to undertake attacks where they are, to use a gun if they have a gun, to use a knife if they have a knife, to use a truck if they have a truck.

MR. ISAACSON: Which is what they did in Nice.

MS. MONACO: Exactly.

MR. ISAACSON: So we then have to fight them in a different way, meaning a bigger threat from ISIL comes from the homegrown self-radicalized at times terrorists who may be like the guy in Orlando, just totally confused about many things, but then decides to say, "I was an adherent and I'm doing this for ISIL." Does that mean that we have to have closer relationships with our domestic Muslim communities? And if so, I think General Clapper said earlier at this conference, that it's very dangerous, the rhetoric that you hear in many places about demonizing Muslims.

MS. MONACO: Look, I think we have to have greater relationships and greater connectivity with the Muslim-American community, with communities of all stripes around the country because the distinction, I think, in the moment we are in now is that we are confronting this threat, as you've noted, that is more diffuse, it's more unpredictable and it is, I think, maybe less sophisticated attacks that occur, but they are certainly deadly and they bespeak a level of unease for people that I think is quite reasonable. So I think what we're doing and what we have to continue to do is constantly recalibrate the tools that we are using.

So, for instance, after 9/11 we set up, I think, across the last administration and this one, an architecture that was focused on building up our intelligence capabilities, breaking down barriers, breaking down walls between law enforcement and the intelligence community, taking what we call on all-tools approach to disrupt threats, whether it's military intelligence, law enforcement, diplomacy. And that architecture has been created and has been, I would argue, quite effective at discerning, detecting, disrupting complex attacks that are based on a networked structure, that are based on a hierarchical model such as the one that Al-Qaeda and core has employed.

But the threat we're facing now is both -- assuredly that and so we have to continue to use those

tools and continue to foster the partnerships we have with our international partners between law enforcement, intelligence agencies. But the Orlando example or the individual who is self-radicalized online, our net is not designed and is, frankly, not capable of detecting that. How do you detect when something goes wrong in somebody's mind and something resonates within them to commit a violent act? That means we're going to have to rely a great deal more on our communities, on giving them the tools to intervene, to identify and work with individuals who are on a path to radicalization.

It means we're going to have to work in greater numbers and with greater urgency with the private sector, with those who have developed the platforms that are frankly being misused to peddle this venom and really brutal messaging from ISIL. I think we've got a lot of those tools that we're developing. I think we're going to have to continue to recalibrate and because some tools that we used for the post 9/11 era aren't always going to be applicable for the threats we are facing going forward.

MR. ISAACSON: Well, let's drill down on the two things you said, work more closely with the Muslim community, work more closely with the private sector tech community. Starting with the Muslim community, how harmful is it really when people are demonizing the Muslim community?

MS. MONACO: So look, I think now this -- this debate about what do you call radical Islam, et cetera, violent extremism, this has taken on a political resonance and has gotten into the -- a very heated political debate, and I'm not going to get into that. From a purely counterterrorism professional perspective, the enemies we are fighting, the groups like ISIL and Al-Qaeda that are trying to recruit, radicalize and mobilize individuals to violence are doing so on a message that we, the American people, the United States, are at war with Islam, that we are trying to promote a clash with civilization. So why would we do anything to further that?

Now, there is no denying that a tremendous amount of violence from these groups, all of the violence

from these groups, has been undertaken and perpetrated based on a perversion of Islam, there's no denying that. But we need to focus on the goal, which is why are and how do we stop radical jihadists or violent extremists of all stripes from trying to kill us.

MR. ISAACSON: But Secretary Jeh Johnson, Homeland Security Secretary, sort of your counterpart since you're the President's Chief Advisor on Homeland Security, says he's actually now been going into Muslim communities and finding it harder. And the first things I say to him is, "Why is everybody in America demonizing?"

MS. MONACO: Yeah, it's -- that it does not help our ability to reach out to maintain relationships with the Muslim community. I hear a lot, I sit down with representatives from across the diaspora, from across the civil society, and what I hear is a concern not only about rhetoric and labels, but about a sense that the U.S. government should not securitize the relationship with the Muslim community, which makes complete sense.

MR. ISAACSON: Explain what you mean by securitize.

MS. MONACO: So that all interactions between the Muslim community and the government should not be done through the law enforcement lens, which of course is right. We've got to broaden that and our strategy for countering violent extremism recognizes that, right? So this is a strategy that is based on enabling communities from the ground up, whether you're teachers, whether you're medical professionals, whether you're community organizers, whether you're state and local government, or whether you're local law enforcement, to be able to come together and build your own recipes, your own strategies for whatever is going to work in your community for helping individuals, usually young, lost and troubled souls, from not becoming, frankly, soulless killers.

MR. ISAACSON: We should give credit because the George W. Bush administration started that process.

MS. MONACO: Absolutely. Absolutely.

MR. ISAACSON: Now you talked about the tech community. As the President's Chief Homeland Security Advisor, you helped lead a delegation not too long ago out to Silicon Valley, I'll call it, although you were all around California, I think. If you had to just request right now and say, "Here is three things the tech community could best do for us," what would they be?

MS. MONACO: So, some of it is already being done, which is broadening the conversation beyond the encryption conversation, which I think is a very important one for all the reasons that John Brennan talked about yesterday. But we have the best innovative minds in this country, I'm clearly biased, but not to say there isn't great entrepreneurs and -- and inventors and engineers elsewhere in the world, but I think we've got the best innovative minds in the United States. And they have built the platforms that have become the tool of choice for terrorists to both peddle their propaganda, but also to use for operations.

So it starts in the open lane, it starts on Twitter, it starts in the open source community, but then goes to the darker side of the web. What we need to do is enlist the private sector's help in having those tools that they invented not to be used for this purpose. I firmly believe that the innovators in this country don't want their -- they're patriots, they don't want their platforms used for this purpose.

And how do we help them enforce their own terms of service? Every tech platform I've ever talked to has got their own terms of service about what's permissible on their platform, but they -- what they have said is they want information to be a two-way street, what are we seeing from government -- from the government perspective about how terrorists are using their platforms that might help them enforce their own terms of service. So that's one thing.

The second thing is they are sitting on a lot of knowhow in terms of marketing and branding and getting messages out that frankly the USG is not particularly

expert in. You know, anything that has a U.S. government stamp on it that is trying to counter ISIL's message, I would submit, is probably not going to be the most resonant with the target audience. So what we have done is alter our counter-messaging approach, and we've done this at the State Department with something called the Global Engagement Center, and we've gone -- shifted from the approach that says the U.S. government should be tweeting at terrorists and undertaking our own U.S. government stamp to counter-messaging and rather bringing in experts who can advise us on why is ISIL's messaging getting so much resonance.

And Brett McGurk talked about this yesterday, they're not drawing people in with beheading videos, they're drawing individuals in, and mostly young people in, with messages that have themes, and this we had some experts explain this to me and it was really interesting, with themes of strength and warmth and belonging. And how you counter that is a different proposition than trying to get into a religious debate with ISIL, which we in the U.S. government should not be doing.

MR. ISAACSON: You know, you kind of shunted aside the encryption question, but CIA Director Brennan yesterday on this stage just went at it really strong and said we should not be celebrating technology companies that are purposely building devices and systems to be out of the reach of the law and valid court's subpoena power. Do you believe that?

MS. MONACO: So I come at this as somebody who spent, before I came to the White House, 15 years in the Justice Department as a federal prosecutor, as a career prosecutor, as the Chief of Staff at the FBI and then as the leader of the national security prosecutions in the department. So I believe strongly that we are a system of laws and the system that we have built that has served us so well for many years and has dealt with technological innovation and our courts and our rule of law system has enabled us to balance that. So I believe we ought to be using that same approach here and that should serve us well.

Now, the fact of the matter is nobody has a stronger interest in strong encryption than the people operating classified systems, the people looking at the nuclear codes, the people who have a responsibility to make sure the air traffic control system is -- stays upright. So there is no scenario, as the President has said, that we in the U.S. government don't want really strong encryption. That said, what has been frustrating, I think, in this debate is there has been a series of discussions where there's a perception that both sides have an absolutist position. We got to get away from that. And I think that's what John Brennan was saying, I think, quite well and quite eloquently yesterday that we've got to move off the absolutist positions, and maybe we've got to break up this problem and make it a little bit smaller.

There are some issues that confront state and local and federal law enforcement when it comes to getting evidence to put the terrorists to the -- to put the pedophile, to put others in jail and make a case. There's a separate problem when it comes to data that's in motion. So how do we address both of those issues, they're separate, they present different challenges. But I'll tell you something, we, in the U.S. government, aren't going to be able to do it alone and there's no one-size-fit-all solution. We're going to need the innovative minds that have built these platforms to help us.

MR. ISAACSON: And what does your conversation say with Tim Cook or others been like recently on that?

MS. MONACO: So, you know, you talked about the delegation that I was a part of out to Silicon Valley earlier this year. You know, there is, I think, a real sense amongst -- and I think these are firmly held and legitimately held views -- that the greater good maybe in having strong encryption that is not accessible in any way to law enforcement and there are some people who have that view. I think that from the standpoint of somebody like myself and others with a responsibility with the public who expect us to stop terrorist plots, to enforce the law, hose come in real tension and --

MR. ISAACSON: So you still have that tension at the moment?

MS. MONACO: I think it's fundamental and it's not based on, I think, anybody not wanting to do the right thing. But people have, you know, people on this issue unlike any other, I think, I've confronted in my recent history in government, this is a really, really tough issue.

MR. ISAACSON: When the hack on the Office of Personnel Management happened last year probably by the Chinese, the Director of National Intelligence, General Clapper was on this stage and he kind of shrugged in a way and said, "You know, score one for them, this is the way spying works, and we're upset, but it's the way -- the way things happen." The hack on the Democratic National Committee, is that different, fundamentally different?

MS. MONACO: So I don't think we know enough yet. And obviously, as has been said I think from this stage and others many times over the course of the last three days, it'll surprise none of you particularly those of you in the press that I'm not going to comment on that specific investigation.

(Laughter)

MS. MONACO: But look, I think the debate at Hellespont is a worthwhile one. The debate about what does it take and when do we attribute and how do we attribute an intrusion, what is that all about and we can talk about that. And then once you discern that, what do you say about it and what do you do.

Now the process by which we've -- and we've evolved in this in the cyber security realm and there are some examples of it recently; the Sony hack the North Korean attack on Sony Pictures. That I think allowed us to utilize a series of best practices that we've built up and it kind of came together in the Sony situation. And what we did there was rely on the investigative agency. The FBI was on the ground working with Sony Pictures to investigate the incident, pool their knowledge with the

rest of the intelligence community, work very rapidly I think both to -- and this is important, share very quickly I think within 24 hours of them being on the ground in that investigation they were able to and we as a government were able to share information back out about the malware that had been used.

And so that is a very important cycle that we have to get into as a government because so much of the infrastructure is in private networks, right? So if the government isn't protecting every individual computer we've got to enable when we see threats to it get that information out just like we do in the terrorism context. So the FBI was able to do that very quickly.

MR. ISAACSON: Oh, boy, that's the only time I can think of that you named names. Meaning the Chinese -- I mean, you won't -- may not say, but Chinese everybody has said did OPM, Russians got into the White House and State Department a year ago and yet the administration has been reluctant to point fingers.

MS. MONACO: So I think I would challenge the premise of that question, although it was more a statement and less a question. So we did it in Sony. And we did so based on as I said, bringing the intelligence community together, looking at this, reaching a level of confidence, which is an important thing. You have to have a certain degree of confidence and ability to prove it, right? Because you're putting that out there and it's still drew some fire from some quarters.

And importantly though, to marry that attribution about the who did it, with what they did, right? And here in the Sony case, we discerned that this was activity that was unacceptable. It had crossed a threshold. It was both destructive, it fried the computers of Sony Pictures, took them offline and it was coercive. And those two things along with the -- our confidence in the attribution and our ability to talk about it in a way that would not disclose sources and methods and hinder our ability to make such attribution in the future, all combined to say you know we're going to call this out.

We called out the Chinese military members who hacked into a number of industries and I know because I started that investigation. When I was the Head of the National Security Division I started that investigation with great prosecutors up in Pittsburg and prosecutors from the National Security Division. And I remember going over and briefing my predecessor, John Brennan and sitting down in the now my windowless office and laying it out and saying this is what they're doing, these are the individuals we've identified, this is what we think is happening.

MR. ISAACSON: That was the National Security Division of the U.S. Justice Department?

MS. MONACO: That's correct.

MR. ISAACSON: Has the DNC hack been referred to the National Security Division of the U.S. Justice Department?

MS. MONACO: I'm not going to talk about that investigation.

MR. ISAACSON: Okay.

MS. MONACO: But my point being that this -- that in that case, we started the investigation when I was the Head of the National Security Division. It developed and what you saw a couple of years ago was indictments against five members -- military members of the PLA for cyber-enabled economic espionage against our companies. So what did we have there? We had strong intelligence, great investigative work rooted in a very high confidence level that these individuals were the ones who did it, that they did it at the behest of the state that we could prove that. We could disclose that without hurting our intelligence tools and their conduct was violative of both criminal statute and a norm that says you're not going to steal from our companies for the enrichment of yours and for your state.

MR. ISAACSON: So you started by saying you

first need the high degree of confidence?

MS. MONACO: Sure.

MR. ISAACSON: -- that you have it right. Approximately how long would it take on any hack like recent ones, I mean we don't have to go into any specifics, but if like -- if something happened in the sheer does it take weeks, months or a year to figure out -- I mean why does it take so long to?

MS. MONACO: Yeah, so the cyber security experts in the room will not be surprised to hear me say it's really a case by case situation. And it's really -- you know look, these actors some of them are more sophisticated than others. I would note that Russia apropos of nothing in particular is a particularly sophisticated actor. And they use very sophisticated tools. Different actors use different tools, whether it's state, sub-state actors. So there's no timeframe you can put on it.

But I think the point I'm trying to make is the framework we look at this through is first and foremost, an investigation that brings the government together, brings the intelligence community together rapidly. What do we know? How do we know it? What's our confidence level? And what have they done? So what I would say here is that the debate around this if this is an attribution that separate -- we need to separate the questions around this issue which is attribution and who did it is one question, what did they do and for what purpose is another.

And what I would say is, if there -- if this is an intrusion for the purpose of stealing information not to inform intelligence or inform their own governmental decisions but in order to coerce and take coercive action and undertake information operations and influence operations that is a different type of activity.

MR. ISAACSON: Okay, then let's stipulate, we're not talking about any one --

MS. MONACO: I hear you.

MR. ISAACSON: -- particular hack or whatever, but you just said something very interesting.

MS. MONACO: I hope so.

(Laughter)

MR. ISAACSON: -- which is what is the purpose and that there is a difference in purpose between trying to take that information for commercial reason --

MS. MONACO: Sure.

MR. ISAACSON: -- for spying reason, and take that information to coerce or influence a political system. Something else that John Brennan said, that this is a -- it would be theoretically a different order of magnitude if it were leaked simply to influence our election.

MS. MONACO: Without a question of doubt, that there are -- there are different reasons that we see intrusions. You may see an intrusion for the purpose of an intrusion, for the purpose of exploring, for the purpose of stealing information, for the purpose of simply understanding what that system looks like to be used for some purpose later.

You could see an intrusion for purposes of destruction as we saw in Sony or in the Saudi Aramco case or see an intrusion for purposes of stealing commercial secrets for the purpose of commercial gain in another country. These are all different approaches which I distinguish from traditional espionage.

MR. ISAACSON: And walk us down through what would happen -- what happens when you sort of have attribution? You're 95, 99, 99.9% sure of attribution, you're the person who has to coordinate then to get into a room with the President and say, do we or do we not name who did this. Walk us through that process, please.

MS. MONACO: So again it's going to be a case by case basis. It's going to be a question of the confidence level. It's going to be a question of what are the tools that are in place. And then what is the follow on, right? So naming and shaming is one thing, the responses that we have at our disposal maybe another. And I think something that this administration has been extremely clear about that all tools are going to be on the table, whether it's the terrorism approach to identify, detect and disrupt threats to the United States.

Similarly we've taken that approach in the cyber realm. So you've seen us employ sanctions as in the case of North Korea. You've seen us employ law enforcement tools as in the case of the China PLA case and frankly the Iranian indictments that the Justice Department did against Iranian actors for attacking and committing DDoS attacks against our financial sector as well as an intrusion into the Bowman Dam in New York.

So there is a range of tools, some of them maybe stated, some of them maybe visible, some of them may not be, some of them maybe diplomacy. All of those things are on the table when that discussion happens.

MR. ISAACSON: David Sanger, who is here, has a piece he just posted, which I know you've read. There's David, in the New York Times this afternoon online, which talks about this very issue of when do you name, what do you do sanctions, whether it's economics do you have, secret things you sometimes do maybe but also public things. In a case that involves a critical infrastructure which is our American political system; not talking about -- this could happen many times whether it's -- so I'm not just talking about DNC, I'm just talking about for politics, do you owe more to the American people to come forth?

MS. MONACO: You know, I think it is a -- I think John Brennan was right, it is a serious, serious issue, a serious thing if there is deliberate intrusion for the purpose of coercing and influencing the political process. I think one of the things this discussion is -- has important implications for both the scale of this if

this is a new technique, right, having using cyber means in yet another new way. And this is we've seen this across the board, right?

MR. ISAACSON: I'm sorry, what do you mean in a new way?

MS. MONACO: Meaning using cyber theft for the purposes of coercion or influence, right?

MR. ISAACSON: Got you.

MS. MONACO: So that is -- that could be we could be in a new world in terms of that as a new tool. Seeing yet again the cyber realm and the digital domain being a place where new tools are used for kind of old types of operations, whether it's stealing, espionage, influence campaigns. And the implications are I think very important. The scale, right, so the barrier to entry for something like this is really quite low. The ability to get in unseen doesn't -- may not take a tremendous amount of overhead costs.

Then the other thing is I think it makes us consider what is critical infrastructure. Everyone knows the power grid is and you know the air traffic control system et cetera, but how should we be thinking about critical infrastructure in a broader way.

MR. ISAACSON: So in other words, the electoral process maybe a critical infrastructure. Would that even mean you're trying to protect voting machines and stuff like that?

MS. MONACO: Sure. I mean there was a good piece recently I saw about what is the level of vulnerability to those types of industries that and also may only get used periodically. But it's all the more reason why I think the President has been very clear from his first days in office, the cyber threat is one that poses not only a national security, but an economic security challenge for us.

And we have seen a tremendous evolution in the

tools that are being used, the tactics, the vectors, the actors from nation states to sub-state actors to criminals or hactivists to of course terrorists. And the attack surface which cyber security experts talk about is so vast and getting bigger with the Internet of Things that it is really has to be a shared responsibility.

I am fond of using the terrorism model to apply to the cyber threat and I think there's a lot we can learn from applying a lot we can learn from how we changed our organization as a government to combat cyber threats -- I'm sorry to combat terrorism threats.

MR. ISAACSON: Right.

MS. MONACO: I think we can learn a lot and apply that to the cyber challenge, there's a difference though. 80, 90% of the networks in this country are in the control of the private sector or state and local actors. It is not the federal government. So we need to rely on that information exchanged with all levels of government and between the public and private sector if we're going to be able to defend ourselves.

MR. ISAACSON: Well, I hope you can protect us against the digital Chad's crisis for this coming election when it happens. One of the things that Aspen Security Group is almost modeled on the Aspen Strategy Group, if Clark won't take offence of that. And the Aspen Strategy Group began with Brent Scowcroft and others to do deterrents but deterrents when it came to strategic deterrents meaning nuclear weapons and that sort of thing. And one of the ideas and thoughts they came up with over the 40 years of this thing is that in order to have strategic deterrents, you have to be a little bit open and talk about your offensive capability. You have to say, here's intermediate range nuclear forces based here that will do this. Will there come a time when you think it's worthy -- worthwhile to talk about our offensive cyber capabilities?

MS. MONACO: I think -- I think there's some truth to that and I think there is a -- there is a framework that we are building that draws on exactly this

concept of deterrents and what are the signal-- what's the signaling that we have to send. Because in the cyber realm, as you say, what's acceptable, what's not acceptable, we haven't developed a set of norms around that. So the danger of escalation, misinterpretation is such that I think you know we have to be responsible about; but we should be very clear as we have been very clear that we will respond to those actions whether it's cyber or otherwise that threaten our interests.

Now the other thing we have discussions about with is that cyber effects don't always necessitate cyber responses. They should be on the table, but you don't always have to respond --

MR. ISAACSON: But are we developing a doctrine? I mean, we would know what to do precisely if a North Korean missile had hit the Sony lot, but we don't quite have the doctrines yet, how do we develop the doctrines and then work with the Chinese and Russians do, what would be the counterpart of assault talks in the '60s and '70s?

MS. MONACO: You know I think we do have a doctrine. I think it's the same doctrine in many respects that we apply in the physical world, right? Respect for sovereignty or taking into account sovereignty, we recognize an international law applies in the cyber realm. We have been working very hard over the last several years to bring the international community along to a set of peacetime cyber norms. Countries, nation states should not impair another country's critical infrastructure.

MR. ISAACSON: So in other words, they -- that norm which I've obviously read about and you gave a talk about means that in peacetime, it's generally now agreed upon amongst nations that you don't take somebody's electricity grid down or it's an act of war?

MS. MONACO: And or it's also a way to isolate those nations that do.

MR. ISAACSON: Right.

MS. MONACO: I mean, this is what --

MR. ISAACSON: But so you've created that one, do you think interfering in a political process should be at that level?

MS. MONACO: I think it's a serious question. I think it's something that if there is coercion, if there is destruction, the other thing I think we need to talk about is manipulation of data, right?

MR. ISAACSON: Right.

MS. MONACO: Which is --

MR. ISAACSON: In other words, stealing data, manipulating it, faking it and then releasing it to somebody?

MS. MONACO: Or intruding in a particular data system and manipulating that data and undermining the integrity of that data such that the owner of that may not know and may not be able to rely on the integrity of that data. I think that is a near to mid-term concern that we should be very, very focused on.

MR. ISAACSON: But we have offensive capabilities, do you think we should be -- I mean can you talk it all about hinting at what are -- what we could retaliate with offensively?

MS. MONACO: Well, we've been very clear about the use of cyber operations on the battlefield in the campaign against ISIL, right? Now I think we should be clear that we're willing to use that that we are using it, but I also don't think we should be telegraphing our punches. So I think there is a -- there's a reasonable distance between articulating norms, trying to bring the international community along, isolating those actors just as we do in the physical realm and in the physical space; isolating actors who violate international norms with a whole range of tools, whether it's sanctions, whether it's diplomacy, whether it's law enforcement, whether it's militarily. We should be building up those norms and we should be quite clear as we have been for instance in the

counter-ISIL campaign that cyber operations are part of the suite of tools that the commander has at his or her disposal and they will be used. But I'm not going to telegraph where we should be dropping the cyber-bomb anymore than I would be directing the F-16.

MR. ISAACSON: You will be happy to know, I am going to end with two friendlier questions about things that seem to be going right. We hear a lot about the border and how we can keep the border safe and people pouring in, and yet I have some the presentations that in the past year that's really gotten under control. Tell us how you got the border with Mexico situation under control, you and Jeh Johnson.

MS. MONACO: More importantly, the wonderful people in the Department of Homeland Security and the Border Patrol working with partners. Look, it's true that border apprehensions are kind of the leading indicator of those trying to cross the border or down. It's also true as we have seen over the last couple of years that the flow of unaccompanied children and families has increased over time. That is a function of a number of things including tremendously difficult and dangerous situations in Central America.

So what we've done is because under our laws if a child comes across the board, we've got a responsibility to provide care, provide an understanding as to whether or not that individual has an asylum claim et cetera. We've increased our capacity to address that flow of unaccompanied children and families. But importantly, we work with the Mexican government to help them control their southern border because it's their southern borders which impacts their northern border, our southern border, so we've worked very hard with the Mexican government to help them including giving them tools with experts from the Department of Homeland Security and Customs and Border Patrol to help the Mexican's control their southern border.

But importantly, to work with Central American nations to address really what is the root cause of some of these kids and these families making an incredibly

dangerous journey and working with them and working across the law enforcement and intelligence community to crackdown on the smuggling network. So you saw just recently, Costa Rica has agreed to provide a place where Central American refugees can go and not make that dangerous journey, but see if their asylum claim has merit even before they make the dangerous journey. And so we are doing more of that. So, all of that has combined I think to try and be first and foremost not sacrifice our safety, but to do so smartly.

MR. ISAACSON: And the other headline we read at the beginning of this summer was that it was going to be an absolute TSA nightmare that lines in airports were going to be, you know, what -- that didn't really happen, what are you doing technologically and in other ways, I know Peter Neffenger is here, that's Peter, they had a -- I shouldn't say that people will be coming up to you --

(Laughter)

MR. ISAACSON: -- trying to get TSA pre-clear. But Peter Neffenger gave us a really good briefing about three days ago on some of the things that have been upgraded, the technologies, everything from Atlanta to New York to Chicago airport and prevented and even bringing people back to work and TSA full time instead of part time to prevent this. How did that work in the White House and TSA?

MS. MONACO: Well, let me just say I am very glad you recognized Peter Neffenger, who is the administrator of TSA who -- this is the guy who runs into a problem, right, and does not shy from the problem. And when you've got all eyes on you and you know the world and the TV screaming that the world is falling, Pete and his team have maintained incredibly cool heads and really attack the problem. And you have mentioned a lot of things. I think Pete has applied his skills and his leadership as the former commander of the Coast Guard that he was, to bring a level of innovation, management reform and partnership with the private sector, with airports, with airlines and importantly, the state and local governments who by the way are responsible for those

airports.

So, all the things you said, innovating, creating a management structure and an incident command post at headquarters in -- at TSA to say what's happening in the system, how do we surge resources and address problems before they become acute. So all of the reforms that you talked about I think have combined to a point where I think 99% of the traveling public this summer has waited less than 30 minutes. So, focusing particularly on these top seven airports that really create some of the backlogs, it's been a tremendous credit to Pete.

MR. ISAACSON: I am going to go to the audience for questions. Why don't you bring a mic? Pete, did you want to say something on that? No, okay. I really wanted to give you some -- some little credit.

MS. MONACO: He is worried everyone wants to get their pre-check application approved.

MR. ISAACSON: Right here, yes and then -- okay. They will come running.

MS. HOWARD: Ma'am, thank you for being here. Well, the DHS has a --

MR. ISAACSON: Do you want to say your name?

MS. HOWARD: Oh I am sorry, I am just so excited. Andrea Howard, I am at King's College London right now. DHS has identified 16 critical infrastructure sectors, what do you personally see as most specific catastrophic target for a cyber attack either in the United States or elsewhere?

MS. MONACO: So, as you have shutters going through the crowd, look, I think what we have to understand is we've identified those 16 critical infrastructure sectors as a way to organize our efforts and our work with them. So, whether it's the financial institutions, the telecom networks, the power grid, the energy sector, I think what we need to recognize is because we are so intertwined, the attack in the power

grid may have a cascading effect or more importantly, the attack on one financial sector element may have a cascading effect. So, I am not going to sit here and give the terrorist actors a roadmap to where they should most effectively point their efforts. But what you've seen us do is try and organize our efforts and prioritize them.

MR. ISAACSON: Yes ma'am, right there and I will get to the back in a minute and then, yes.

MS. BRIGGS: Rachel Briggs from Hostage U.S. Thank you for your comments and for your leadership in this area. I wanted to ask you about the support available for the victims of terrorism. We have heard over the last few days that we are facing the very real prospect of more attacks here in the homeland in the way that we have unfortunately seen in Europe. Do you think at the moment that the U.S. government currently has the right level of provision for those victims who face really complex health and mental health problems over a very prolonged period of time?

MS. MONACO: It's a great question. And I think we should recognize Rachel Briggs who has done great innovative work at Hostage U.S. taking what is a very effective framework from Hostage U.K. and bringing it here to help families of hostages who have been killed or taken abroad, so just tremendous work by Rachel and her team. You know, I think the victim services, for lack of a better word, are what we are doing now from a federal perspective is really only one small piece of the puzzle, right? It has got to come at the local level, but we need to make sure that we have made available as much in the way of federal resources as we can.

So what happens in real life and I will tell you having spent time about three hours with the President when he was in Orlando meeting with the families of that devastating attack is what we try and do is have the victim services in that case from the FBI, really provide kind of a backstop and provide a network of resources that they can plug into the local communities. That's where I think we are best not coming in and big footing a local communities approach, but rather giving them tools, giving

them additional resources, but letting them say what's going to be the most effective thing for the communities that are devastated.

MR. ISAACSON: Yes, I think that was in the back, yes. Whoever it is, yes.

MR. WALDT: Very quickly before I have to catch my plane, I am sorry. I am [Eric Waldt], D.C. Metropolitan Police Department. As you've probably read or know Ted Koppel had a book out earlier this year called *Lights Out* that talks about the dangerous nexus between the cyber attacks and the vulnerabilities in our electric grid and he points some criticism at DHS and FEMA in particularly for lack of plans to handle a long sustained electric grid failure. Perhaps you could comment on what you see his criticisms, whether you believe them to be valid and what plans you see either in place or coming?

MS. MONACO: So, I have to confess, I haven't read Ted Koppel's book, although it was given to me as a gift for the speech I just gave at a cyber security conference. But --

MR. ISAACSON: So, you will read it or try it.

(Laughter)

MS. MONACO: In my copious free time.

MR. ISAACSON: Yeah.

MS. MONACO: Look, one of the things we are doing is working with what we call the sector specific agencies, right? So, the Department of Energy has undertaken I think a very focused and very good effort under the leadership of Erne Moniz and Liz Sherwood-Randall to bring the leaders of the power sector, the leaders of the electric grid all around the table to make sure that there is a place to intersect in terms of information sharing where we get information about cyber vulnerabilities, about malware that we are pushing it out both through DHS, but also through this -- through the sector specific agencies.

One of the things we've done to try and buck up that effort is create something called the Cyber Threat Intelligence Integration Center, CTIIC. Again building on the terrorism model, we have NCTC that is -- brings all of the elements of the intelligence community together to be aware of all the terrorist threats that we are facing and then make sure that the policymakers and operators have that information.

We've now done the same thing with CTIIC. Before last year, there was not one single place in the government even though we face such a big cyber threat, there wasn't any single place in the government responsible for integrating all that information. So, now CTIIC is doing that. And importantly part of its mission is to downgrade or declassify information that can then be shared by DHS out with industry including the electric sector.

MR. ISAACSON: And the electric sector is one among many that's partly private, sometimes public-private companies, you have both CTIIC and you've -- one of the few laws that got passed this year was to enable information sharing and even reduce the amount of risk you would have from antitrust --

MS. MONACO: That's exactly right.

MR. ISAACSON: -- that you have shared with other people.

MS. MONACO: Yeah, we've --

MR. ISAACSON: But how do we get people to share more because we kept hearing his week that still industry isn't sharing quite enough?

MS. MONACO: So, look, I think this is going to be a bit of a cultural evolution. One of the things about the cyber threat is it's not all technology, there is a lot of human behavior involved, right. The seatbelt analogy I think is instructive. There was a time when we didn't all get in our cars and reflexively put on our

seatbelts. But we have to over time change our behavior around common cyber security practices. So one of the things that we did in passing bipartisan, yes, bipartisan cyber security information sharing legislation last year was to put in place a framework that said, if you share information about the breach that has occurred in your company, you do so through the Department of Homeland Security after you take appropriate privacy protection measures on that information, you, company X, will have liability protection for sharing that information.

I think companies were both very fearful of sharing information with the government for fear that their customers or shareholders would sue them for that and they were I think fearful of sharing with each other on the theory that there will be some allegation of collusion. So two things that we did was make very clear what the antitrust rules of the road were and that a company would receive liability protection for sharing information with the government.

MR. ISAACSON: But they say this taking for example Centers for Disease Control, if somebody gets Penicillin anywhere, gets bit anywhere by a mosquito, it all goes into a big database and they have huge amounts of data and they analyze it. We get hacked at the Aspen Institute two or three times a month, we don't have a database we can just send it to. Why isn't there a big national database like the Centers for Disease Control has where you can have experts and even the public looking in and trying to figure out the pattern?

MS. MONACO: Well, so I would argue, that's in large part what DHS has done and Suzanne Spaulding is here somewhere, she and her team at DHS under and I am going to throw yet another acronym at you, bear with me, it's called the NCCIC, the National Cyber Communications Integration Center and what that does is, this information whether you're a company, whether you're a state and local government, whether you're from a particular industry, share that information into NCCIC which has all of the government alphabet soup present in it, but it also importantly has industry present. So, it has representatives from industry sectors sitting side-by-side

understanding what that information is. So that really is the type of --

MR. ISAACSON: Yes, but let me push back.

MS. MONACO: Sure.

MR. ISAACSON: In the minute it took us to discuss this, let's take Citicorp, probably got twice hacked and attacked and they caught, they didn't send that information to you, did they? They are not doing it yet.

MS. MONACO: Well, I hope -- I hope that they are going to avail themselves of what this legislation put in place, which is it said, DHS needs to have a automated indicator sharing system, so to make it a lot easier for companies and frankly for government agencies who also have been victims to share that information.

MR. ISAACSON: Yes sir. Okay. I can't see because of lights.

MR. BLUM: John Blum is my name. Isaacson has been pushing you all evening to try to get you to talk a little bit more about our aggressive side. And when I hear public officials talk about our morality and how moral we are, it scares me. We are not dealing with moral people, we are dealing with people in Russia and especially in the Middle East that don't have the same kind of moral structure we do. So, can you give us some kind of sense of what aggressive positive things we are doing, can we hear what's going on, the top officials in the Kremlin, can we hear what's going on in the Middle East when two guys talk together who are officials and important, or don't you want to comment on that at all?

MS. MONACO: If you're asking me to disclose what our intelligence methods are and where they are, I will decline your kind invitation.

MR. ISAACSON: Well, you assures that we're at least being aggressive.

MS. MONACO: In the cyber realm, in the military

realm, in the law enforcement realm, absolutely and I don't think that there is or there should be a whole lot of debate about that. When you look at the number of terrorists that we have taken off the battlefield, with the amount of territory that ISIL no longer controls, with the 14,000 strikes that have occurred in the campaign against ISIL in Iraq and Syria over the course of this --

MR. ISAACSON: Okay, let me -- hold it right there, you just said 14,000 drone strike or strikes, whatever, some drones, some not, again why don't you say what cyber attacks we have done, if can say what drones and other strikes were done?

MS. MONACO: Well, because I think it's a lot more difficult to say, look we can lay out the list and we have laid out the list of the leadership of ISIL and Al-Qaeda that we've killed with drone strikes, with Special Forces operations and the intelligence that has yielded that, which has led to yet more operations. That is something that you can see and you can describe. But the cyber methods that we are using, I personally don't think it makes a whole lot of sense to describe that for our adversary who can anymore than it would make sense for me to say, tomorrow we are going to strike the oil infrastructure at these coordinates next to Damascus, that doesn't make a whole lot of sense to me.

So I am not sure why we would transmit what cyber effects we would have in that realm either. That said, we should be very clear about the norms that we are applying. So, for instance, in the kinetic world, when we are dropping bombs, we do so under a set of laws and norms, the law of armed conflict which you and the rest I hope of the citizenry can have confidence that we are doing so adhering to the laws, adhering to proportional collateral damage as has been talked about and that we are doing so consistent with our values. I don't think anybody should shrink from that, I don't think it's something we should apologize for, that's what makes this country great.

We should I think have the same confidence and you should be able to have the same confidence that we are

applying that framework in a way that is effective and protects our interests and aggressively under the same framework in the cyber realm.

MR. ISAACSON: Yes, back there and then I will catch you next. Sorry.

MR. BLATZ: Hi, [Bob Blatz], Cincinnati. Could you comment on a recent article in the Wall Street Journal where they were reporting or German intelligence was reporting that Iran was acquiring nuclear materials?

MS. MONACO: I can't comment on that, although I would refer you to, I don't know if you here for John Brennan's --

MR. BLATZ: I was.

MS. MONACO: -- comments yesterday about the monitoring of the joint comprehensive plan of action and his description of Iran's compliance thus far there.

MR. ISAACSON: And so basically not to get in the specifics, we should feel assured that there has been in general compliance with the joint plan of action.

MS. MONACO: Thus far, and again I would say, I think John's comments about that hit the mark.

MR. ISAACSON: Yes ma'am, in the white. Yes.

MS. LEMMON: Thank you so much. Gayle Lemmon from Council on Foreign Relations. And I just had a quick question. I was speaking with military folks recently who are doing counter-ISIL messaging and they talked about the frustration and the challenge of doing that when you're up against people who are really nimble, really flexible, don't have a 12-step process of approvals to go through before they get their messaging out. And I wonder if you could talk about the challenge and the mismatch there.

MR. ISAACSON: Good question.

MS. MONACO: Yes, I've heard and we have talked about this in terms of DoD's operations on this score. I think the counter messaging that we are talking about here and I that was referencing earlier really is about enabling, amplifying other voices, right? So, the individuals or the voices, the credible voices in the Gulf and across the Arab world where 90% of ISIL's messaging is done, that needs to come not from us, frankly not from DoD, not from state, not from anybody else again with the U.S. seal, but from voices that are going to be credible and targeted at frankly the target audience. And what we've been trying to do is build up those voices, working with for instance the Sawab Center in the Emirates, doing the same thing that we are going to be doing in Malaysia. So, that's really where we are trying to target our counter messaging.

MR. ISAACSON: Yes. Kimberly, yes.

MS. DOZIER: Kim Dozier at the Daily Beast and CNN. Lisa, do Americans need to get used to the concept of terrorism like they got used to the concept mass shootings. We've heard this week that in the near-term there might be a military defeat of ISIS on the battlefield, but that the generational fight to come will be against ISIS, Nusra, Al-Qaeda in smaller forms.

MS. MONACO: So, it's a good question. Look, I think the spate of attacks particularly that we've seen over the last say six to eight weeks when you're talking everything from Istanbul to Orlando, to Dhaka in Bangladesh, Saudi Arabia, you name it, I think people rightly have a sense of unease and I think it's because it is so unpredictable. So, I often get the question, are we in the new normal and I think that's really the point of your question. And I hesitate to agree with that premise because I don't think the type of carnage and depravity that we've seen for instance in something like Nice, that should never be, we should never consider that normal.

If we've gotten to that point, I think we've lost our way. But I do think that and this gets back to the start of the question that Walter asked me, we are in a different moment and we are facing a threat that is much

more unpredictable. And what I think Americans need to recognize is that they got to be part of the apparatus that enables us to prevent these, right? So it has got to come from the communities, law enforcement and intelligence as we talked about earlier is not going to necessarily be able to identify the person who radicalizes very quickly, has no contact with Al-Qaeda, Nusra, ISIL, Boko Haram, you name it, has no outward direction and we are going to have to engage more with communities to divert that individual, keep them from going down that path, but divert them if they get on that path, that very dark path to violence and but at the end of the day, we are going to have to rely and I'm heartened when I think about this because I think this is something that we have readily in our toolkit, which is the resilience of the American people.

We've seen it time and time again from Boston to San Bernardino to Orlando, we are going to have to remember and continue to draw upon the resilience in our communities because we will continue to face violence from deranged, radicalized extremists of all stripes and we are going to have to continue to summon the resilience to address it.

MR. ISAACSON: Yes, now we have gone a bit long and I appreciate it Lisa, your willingness to stay. Well, there are a couple more questions, way back there, I have been discriminating against the way back.

MR. MARTIN: Thank you. Todd Martin from Aspen. I am not sure this is a question directly in your current responsibility, but I am sure you are close enough to answer it, which is how is strategy determined at the very top level in the zone of ISIL and the Middle East because there is political issues, there is military issues, there is history, there is cyber. How is strategy determined so that President Obama or any other president would have the smartest way forward through that mirage of difficult factors?

MS. MONACO: You mean U.S. strategy, you are talking about, yes. It starts from the top, from the president based on discussions with his National Security

Team and I'm at that table. So actually your question is more on point than maybe you think. And it starts with his direction and what you see reflected is evident in the counter-ISIL campaign, which is that strategy is not solely a military strategy, it is not solely a humanitarian effort, it is not solely a diplomatic strategy, it is a comprehensive approach first and foremost to squeeze ISIL where it is in its twin capitals of Mosul in Iraq and Iraq and Syria and as Brett has very capably talked about and has been leading this effort to go after its networks, whether they're financial, whether they are foreign fighters, manpower, whether they are network of messaging and then to go after the branches that they have been able to have take root in and now eight different provinces.

So the strategy comes from the president's leadership that this has to be a comprehensive approach that relies on and is done in concert with a stable of partners across the globe. We now have 67 partners in this coalition and that comes from the president's leadership that our strategies got to be one that's done with partners, that is comprehensive, that cuts across and is built on the notion that we are not going to ultimately have a solution to the problems in Syria and Iraq solely militarily, but it has to be one that's built on a political foundation.

MR. ISAACSON: Lisa, you are about to end your term in a few months. Let me let you end by reflecting on what it's like to be sort of right in the center every morning at 5:00 a.m. to be hit with things that you are going to have to brief on in a couple of hours. Tell us a little bit about how you feel just a career prosecutor who suddenly ended up in a situation room.

MS. MONACO: You know, it's unbelievable I think sometimes when I reflect about how incredibly fortunate I have been to be able to have a series of roles where I hopefully have been able to contribute, whether it's being a career prosecutor which as an assistant U.S. attorney, it's the best job in the world to get to stand up and say Lisa Monaco for the United States, to helping FBI Director Mueller transform that agency from a law enforcement,

solely law enforcement organization to a national security organization, to leading a group of incredibly professional prosecutors at the Justice Department to now sitting in the Oval Office every morning with the President talking to him about the challenges we face, I think I'll ultimately get over the fact that he basically refers to me as Dr. Doom because nothing I bring to him is ever positive.

MR. ISAACSON: Whenever he sees your name on phone ID, he knows something bad has happened.

MS. MONACO: Yes, it's usually not good news. But that's an incredible privilege. It is absolutely unrelenting, but it's an incredible privilege to contribute and to have as your job to help the National Security Team, basically the job description is to help keep the country safe. It doesn't get any better than that.

MR. ISAACSON: Yeah, that's what we've heard all week, whether it's Jeh Johnson, Peter Neffenger. We thank you for your service and thank you for being here.

(Applause)

* * * * *

Readout of Secretary Johnson's Call with State Election Officials on Cybersecurity

Release Date: August 15, 2016

For Immediate Release
DHS Press Office
Contact: 202-282-8010

Today, Secretary of Homeland Security Jeh Johnson hosted a phone call with members of the National Association of Secretaries of State (NASS) and other Chief Election Officials to discuss the cybersecurity of the election infrastructure. It is critically important to continue to work to ensure the security and resilience of our electoral infrastructure, particularly as the risk environment evolves. Representatives from the U.S. Election Assistance Commission, the Department of Commerce's National Institute for Standards and Technology (NIST), and the Department of Justice (DOJ) also participated in the call.

During today's call, Secretary Johnson offered assistance in helping state officials manage risks to voting systems in each state's jurisdiction. While DHS is not aware of any specific or credible cybersecurity threats relating to the upcoming general election systems, Secretary Johnson reiterated that

DHS, the Election Assistance Commission, NIST, and DOJ are available to offer support and assistance in protecting against cyber attacks. He also recognized the important work already being done in the states to ensure the integrity and security of the nation's elections. Secretary Johnson further emphasized that DHS is exploring all ways to deliver more support to the sector in a collaborative and non-prescriptive manner, and would be examining whether designating certain electoral systems as critical infrastructure would be an effective way to offer this support.

As part of the ongoing effort, the Secretary also announced that DHS is convening a Voting Infrastructure Cybersecurity Action Campaign with experts from all levels of government and the private sector to raise awareness of cybersecurity risks potentially affecting voting infrastructure and promote the security and resilience of the electoral process. Representatives of the National Association of Secretaries of State were invited to join this group to provide their expertise and input.

Secretary Johnson encouraged state officials to focus on implementing existing recommendations from NIST and the EAC on securing election infrastructure, such as ensuring that electronic voting machines are not connected to the internet while voting is taking place.

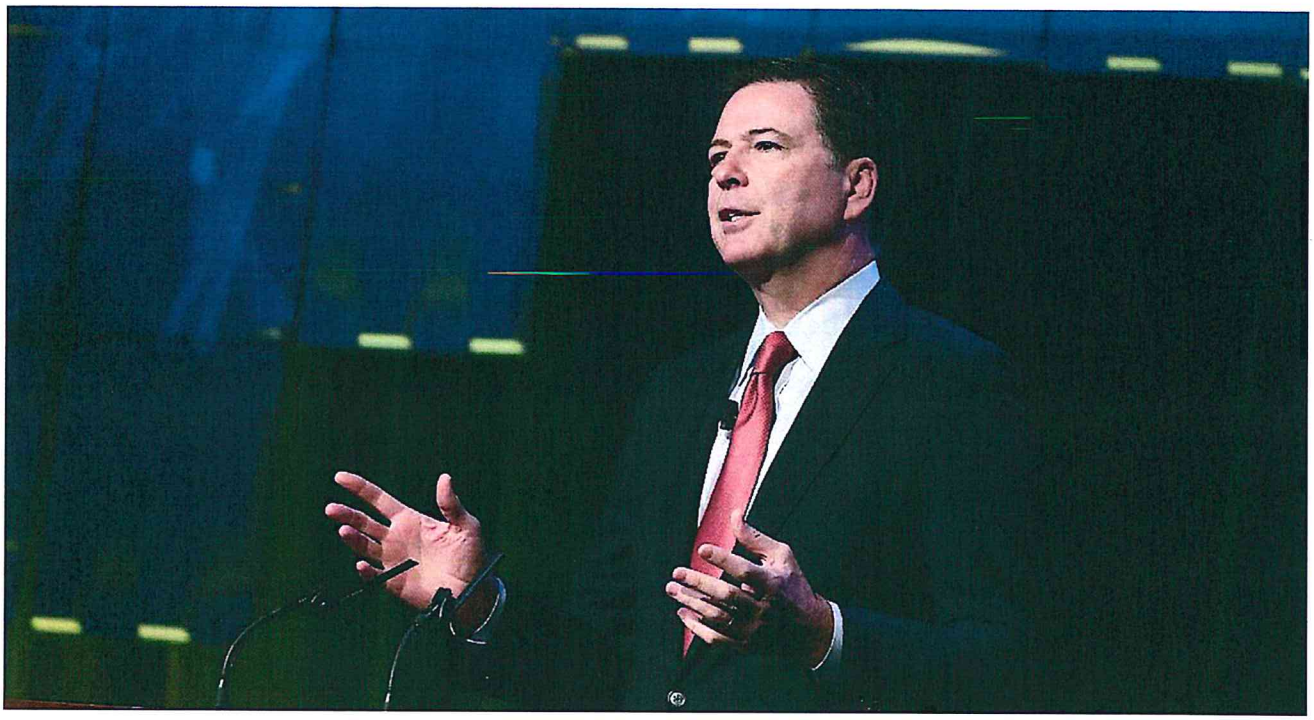
Secretary Johnson offered the assistance of the Department's National Cybersecurity and Communications Integration Center (NCCIC) to conduct vulnerability scans, provide actionable information, and access to other tools and resources for improving cybersecurity.

###

Topics: Cybersecurity (/topics/cyber-security)

Last Published Date: August 16, 2016

POLITICO



FBI Director James Comey speaks Tuesday during a government symposium on cyber security in Washington, D.C. | Getty

Comey: FBI takes election tampering 'very seriously'

By **TIM STARKS** | 08/30/16 10:44 AM EDT

One day after reports the FBI had warned states of potential hacks on their election systems, Director James Comey declined to address the bureau's investigation, simply insisting he takes the matter "very seriously."

The FBI alert — sent Aug. 18 and revealed publicly on Monday — sparked fears that recent cyberattacks on voter databases in Illinois and Arizona were harbingers of a nationwide hacking assault on state voting systems, possibly linked to Russia.

"It won't surprise you that I'm not going to give an answer that touches on any particular matter we're looking at," Comey said Tuesday at a conference hosted by digital security firm

Symantec.

Multiple security researchers and former FBI officials said the bureau's alert showed signs that investigators may suspect a government-backed hack. Many worried that meant the intrusions were part of a suspected Russian attempt to meddle in the U.S. election.

Moscow-backed hackers have already been blamed for leaking embarrassing documents and emails stolen from the Democratic National Committee and the Democratic Congressional Campaign Committee.

Supporters of Democratic nominee Hillary Clinton have alleged the efforts are part of a Kremlin plot to install GOP rival Donald Trump in the White House.

"Maybe I can say this," Comey said. "We take very seriously any effort by any actor, including nation-states, and maybe especially nation-states, that moves beyond the collection of information about our country and that offers the prospect of an effort to influence the conduct of affairs in our country."

Election security specialists say hackers with access to voter rolls could alter vote totals by removing people from the registration list.

"Whether that's an election or something else," those kinds of hackers are "something we take very, very seriously, and we very work very hard to understand so that we can equip the rest of our government for options on how to deal with it," Comey added.

Joint DHS and ODNI Election Security Statement

Friday, October 07, 2016

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

October 07, 2016

Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security

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.

Newsroom Categories

- Recent News
- Reports & Publications
- Press Releases
- Speeches & Interviews
- Congressional Testimonies
- Featured Articles
- IC in the News

Archive

- 2017
- 2016
- 2015
- 2014
- 2013
- 2012
- 2011
- 2010
- 2009
- 2008
- 2007
- 2006
- 2005

Sign Up For ODNI Email Updates

About This Site
Contact the IC IG
No Fear Act
Privacy Policy
Customer Service
FOIA
Contact Us

About
Mission, Vision, Goals
History
ODNI Seal
Organization
Leadership
ODNI FAQ

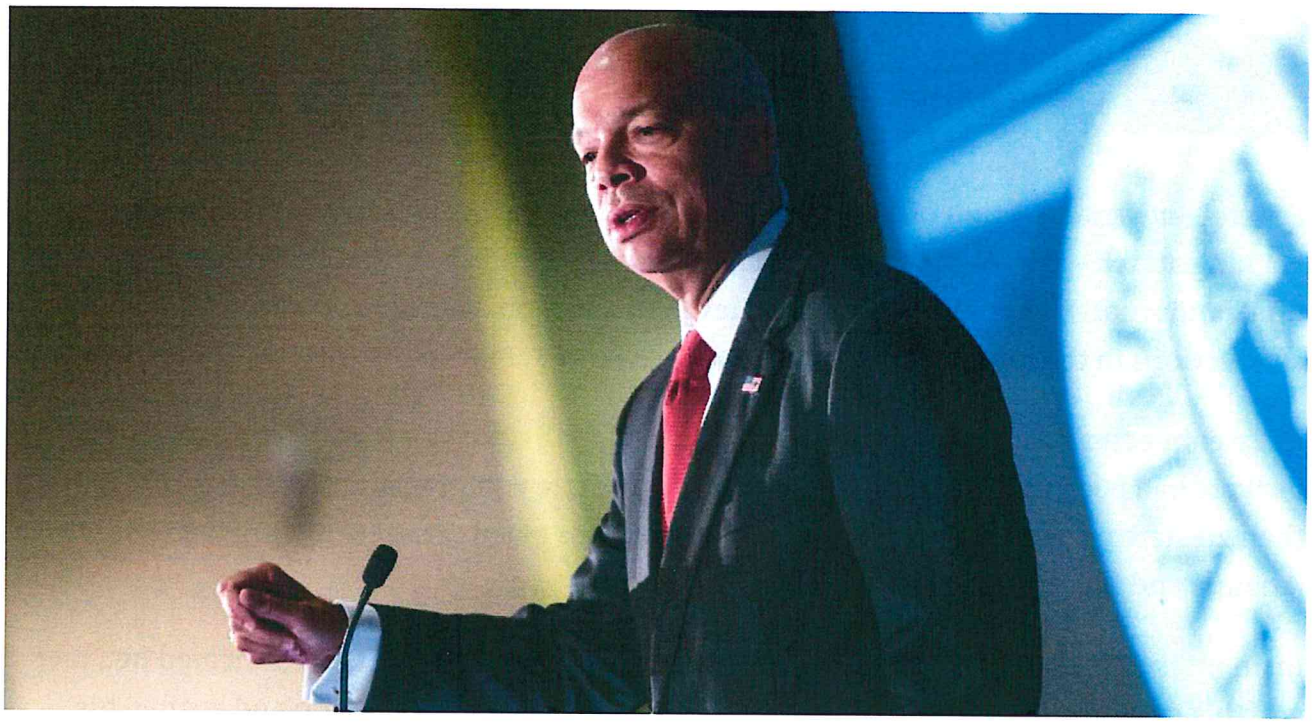
Intelligence Community
Professional Ethics
Transparency
Members of the IC
IC Seal
IC Policies & Reports
Review Group

Newsroom
Recent News
Reports & Publications
Press Releases
Speeches & Interviews
Testimonies
Featured Articles
IC in the News

Careers
Careers at ODNI
Careers in the IC
For Students
Veterans

Resources
For Kids
Ready.gov
Open.gov
Flu.gov
Plain Language Act
Plugins
Furlough Resources
Operating Status

POLITICO



"We hope to see more," DHS Secretary Jeh Johnson said of states seeking to thwart election hackers. | Getty

DHS official: Half of U.S. states have sought help to thwart election hackers

By **DARREN SAMUELSOHN** | 10/05/16 07:25 PM EDT

Hacking threats have prompted 25 states so far to seek out the Obama administration's help in assessing vulnerabilities and fending off attacks to their voting systems headed into Election Day, a Department of Homeland Security official told POLITICO on Wednesday.

DHS won't name the specific states that have reached out for federal aid — that's up to each individual state to confirm, the agency said. But DHS has been providing a running total on the overall number of states. Last Friday, a department official said that 21 states had expressed an interest in its vulnerability scanning services.

"We hope to see more," DHS Secretary Jeh Johnson said in a statement on Saturday.

Concerns about a cyberattack on the nation's election system have grown in recent months, following a series of suspected Russian hacks targeting Democratic political offices, the Hillary Clinton campaign and state election networks. GOP nominee Donald Trump has also prompted concerns about the integrity of the election by repeatedly stating the outcome will be "rigged" and by calling for his supporters to volunteer in "certain areas" as poll watchers.

A new Snowden? NSA contractor charged with stealing classified info

By **JOSH GERSTEIN** and **CORY BENNETT**

Federal and state election officials insist the country's balloting is secure from a widespread hacking attack — they note the diverse nature of 50 different state jurisdictions, plus thousands more at the county and local level. In addition, voting itself doesn't involve any connections to the internet, officials insist.

But weaknesses do exist across the system, too. A DHS official last week confirmed that hackers had been detected seriously probing into state voter registration systems in more than 20 states, and they actually had varying degrees of success getting into the rolls in Arizona and Illinois.

In an interview last week, Colorado Secretary of State Wayne Williams confirmed he's met with officials from DHS, the FBI and the U.S. attorney office in Colorado and availed his state of the federal government's resources. "We do participate in that process," he said.

Georgia Secretary of State Brian Kemp also told POLITICO it was "great" that states had the opportunity to tap federal officials for help prepping for the election. But the Republican said he also wasn't bowled over by what the federal government was providing in the way of detection services.

"They're not offering anything we're not already doing in Georgia in regards to running penetration tests on our system," Kemp said.

Press Call TPs

028

Withdrawal Marker
Obama Presidential Library

FORM	SUBJECT/TITLE	PAGES	DATE	RESTRICTION(S)
Draft	Talking Points for Cyber Validator Calls	3	N.D.	P5;

This marker identifies the original location of the withdrawn item listed above. For a complete list of items withdrawn from this folder, see the Withdrawal/Redaction Sheet at the front of the folder.

COLLECTION:
National Security Council - Homeland Security and Counter-Terrorism Directorate

SERIES:
Monaco, Lisa - Subject Files

FOLDER TITLE:
Russia Response Rollout

FRC ID:
70724

OA Num.:
W1100

NARA Num.:

FOIA IDs and Segments:

22-26844-F

22-26842-F

22-26841-F

22-26840-F 3

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

Deed of Gift Restrictions

A. Closed by Executive Order 13526 governing access to national security information.
B. Closed by statute or by the agency which originated the document.
C. Closed in accordance with restrictions contained in donor's deed of gift.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Records Not Subject to FOIA

Court Sealed - The document is withheld under a court seal and is not subject to the Freedom of Information Act.

E.O.

030

EXECUTIVE ORDER

- - - - - - -

TAKING ADDITIONAL STEPS TO ADDRESS THE NATIONAL EMERGENCY WITH RESPECT TO SIGNIFICANT MALICIOUS CYBER-ENABLED ACTIVITIES

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 *et seq.*) (NEA), and section 301 of title 3, United States Code,

I, BARACK OBAMA, President of the United States of America, in order to take additional steps to deal with the national emergency with respect to significant malicious cyber-enabled activities declared in Executive Order 13694 of April 1, 2015, and in view of the increasing use of such activities to undermine democratic processes or institutions, hereby order:

Section 1. Section 1(a) of Executive Order 13694 is hereby amended to read as follows:

"Section 1. (a) All property and interests in property that are in the United States, that hereafter come within the United States, or that are or hereafter come within the possession or control of any United States person of the following persons are blocked and may not be transferred, paid, exported, withdrawn, or otherwise dealt in:

(i) the persons listed in the Annex to this order;

(ii) any person determined by the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to be responsible for or complicit in, or to have engaged in, directly or indirectly, cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that have the purpose or effect of:

(A) harming, or otherwise significantly compromising the provision of services by, a computer or network of computers that support one or more entities in a critical infrastructure sector;

(B) significantly compromising the provision of services by one or more entities in a critical infrastructure sector;

(C) causing a significant disruption to the availability of a computer or network of computers;

(D) causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain; or

(E) tampering with, altering, or causing a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions; and

(iii) any person determined by the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State:

(A) to be responsible for or complicit in, or to have engaged in, the receipt or use for commercial or competitive advantage or private financial gain, or by a commercial entity, outside the United States of trade secrets misappropriated through cyber-enabled means, knowing they have been misappropriated, where the misappropriation of such trade secrets is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economy of the United States;

(B) to have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, any activity described in subsections (a)(ii) or (a)(iii)(A) of this section or any person whose property and interests in property are blocked pursuant to this order;

(C) to be owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, any person whose property and interests in property are blocked pursuant to this order; or

(D) to have attempted to engage in any of the activities described in subsections (a)(ii) and (a)(iii)(A)-(C) of this section."

Sec. 2. Executive Order 13694 is further amended by adding as an Annex to Executive Order 13694 the Annex to this order.

Sec. 3. Executive Order 13694 is further amended by redesignating section 10 as section 11 and adding a new section 10 to read as follows:

"Sec. 10. The Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, is hereby authorized to determine that circumstances no longer warrant the blocking of the property and interests in property of a person listed in the Annex to this order, and to take necessary action to give effect to that determination."

Sec. 4. This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

Sec. 5. This order is effective at 12:01 a.m. eastern standard time on December 29, 2016.

THE WHITE HOUSE,

December 28, 2016.

Annex

Entities

1. Main Intelligence Directorate (a.k.a. Glavnoe Razvedyvatel'noe Upravlenie) (a.k.a. GRU); Moscow, Russia
2. Federal Security Service (a.k.a. Federalnaya Sluzhba Bezopasnosti) (a.k.a FSB); Moscow, Russia
3. Special Technology Center (a.k.a. STLC, Ltd. Special Technology Center St. Petersburg); St. Petersburg, Russia
4. Zorsecurity (a.k.a. Esage Lab); Moscow, Russia
5. Autonomous Noncommercial Organization "Professional Association of Designers of Data Processing Systems" (a.k.a. ANO PO KSI); Moscow, Russia

Individuals

1. Igor Valentinovich Korobov; DOB Aug 3, 1956; nationality, Russian
2. Sergey Aleksandrovich Gizunov; DOB Oct 18, 1956; nationality, Russian
3. Igor Olegovich Kostyukov; DOB Feb 21, 1961; nationality, Russian
4. Vladimir Stepanovich Alexseyev; DOB Apr 24, 1961; nationality, Russian

Annex

Entities

1. Main Intelligence Directorate (a.k.a. Glavnoe Razvedyvatel'noe Upravlenie) (a.k.a. GRU); Moscow, Russia
2. Federal Security Service (a.k.a. Federalnaya Sluzhba Bezopasnosti) (a.k.a FSB); Moscow, Russia
3. Special Technology Center (a.k.a. STLC, Ltd. Special Technology Center St. Petersburg); St. Petersburg, Russia
4. Zorsecurity (a.k.a. Esage Lab); Moscow, Russia
5. Autonomous Noncommercial Organization "Professional Association of Designers of Data Processing Systems" (a.k.a. ANO PO KSI); Moscow, Russia

Individuals

1. Igor Valentinovich Korobov; DOB Aug 3, 1956; nationality, Russian
2. Sergey Aleksandrovich Gizunov; DOB Oct 18, 1956; nationality, Russian
3. Igor Olegovich Kostyukov; DOB Feb 21, 1961; nationality, Russian
4. Vladimir Stepanovich Alexseyev; DOB Apr 24, 1961; nationality, Russian

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release December 29, 2016

TEXT OF A LETTER FROM THE PRESIDENT
TO THE SPEAKER OF THE HOUSE OF REPRESENTATIVES
AND THE PRESIDENT OF THE SENATE

December 28, 2016

Dear Mr. Speaker: (Dear Mr. President:)

Pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*) (IEEPA), I hereby report that I have issued an Executive Order (the "order") that takes additional steps to address the increasing use of significant malicious cyber-enabled activities to undermine democratic processes or institutions. These steps have been taken with respect to the national emergency declared in Executive Order 13694 of April 1, 2015.

The order amends section 1(a) of Executive Order 13694 by providing authority for blocking the property and interests in property of any person determined by the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to be responsible for or complicit in, or to have engaged in, directly or indirectly, cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that have the purpose or effect of tampering with, altering, or causing a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions. The order also blocks the property and interests in property of the persons listed in the Annex to the order.

I have delegated to the Secretary of the Treasury the authority, in consultation with the Attorney General and Secretary of State, to take such actions, including the promulgation of rules and regulations, and to employ all powers granted to the President by IEEPA as may be necessary to carry out the purposes of the order. All agencies of the United States Government are directed to take all appropriate measures within their authority to carry out the provisions of the order.

I am enclosing a copy of the Executive Order I have issued.

Sincerely,

BARACK OBAMA

# # #

Withdrawal Marker
Obama Presidential Library

FORM	SUBJECT/TITLE	PAGES	DATE	RESTRICTION(S)
Email	From Ned C. Price to #SUITE et al., re: [Readouts]	3	12/29/2016	P5;

This marker identifies the original location of the withdrawn item listed above. For a complete list of items withdrawn from this folder, see the Withdrawal/Redaction Sheet at the front of the folder.

COLLECTION:
National Security Council - Homeland Security and Counter-Terrorism Directorate

SERIES:
Monaco, Lisa - Subject Files

FOLDER TITLE:
Russia Response Rollout

FRC ID:
70724

OA Num.:
W1100

NARA Num.:

FOIA IDs and Segments:

22-26844-F

22-26842-F

22-26841-F

22-26840-F 3

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

Deed of Gift Restrictions

A. Closed by Executive Order 13526 governing access to national security information.
B. Closed by statute or by the agency which originated the document.
C. Closed in accordance with restrictions contained in donor's deed of gift.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Records Not Subject to FOIA

Court Sealed - The document is withheld under a court seal and is not subject to the Freedom of Information Act.

Withdrawal Marker
Obama Presidential Library

FORM	SUBJECT/TITLE	PAGES	DATE	RESTRICTION(S)
Email	From Ned C. Price to #SUITE et al., re: [Readout]	2	12/29/2016	P5;

This marker identifies the original location of the withdrawn item listed above. For a complete list of items withdrawn from this folder, see the Withdrawal/Redaction Sheet at the front of the folder.

COLLECTION:
National Security Council - Homeland Security and Counter-Terrorism Directorate

SERIES:
Monaco, Lisa - Subject Files

FOLDER TITLE:
Russia Response Rollout

FRC ID:
70724

OA Num.:
W1100

NARA Num.:

FOIA IDs and Segments:

22-26844-F

22-26842-F

22-26841-F

22-26840-F 3

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

Deed of Gift Restrictions

A. Closed by Executive Order 13526 governing access to national security information.
B. Closed by statute or by the agency which originated the document.
C. Closed in accordance with restrictions contained in donor's deed of gift.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Records Not Subject to FOIA

Court Sealed - The document is withheld under a court seal and is not subject to the Freedom of Information Act.

Withdrawal Marker
Obama Presidential Library

FORM	SUBJECT/TITLE	PAGES	DATE	RESTRICTION(S)
Email	From Graham H. Brookie to Lisa O. Monaco et al., re: Confirmed Participants - White House Call - (12/29) at 1:30 pm ET	2	12/29/2016	P5;

This marker identifies the original location of the withdrawn item listed above. For a complete list of items withdrawn from this folder, see the Withdrawal/Redaction Sheet at the front of the folder.

COLLECTION:
National Security Council - Homeland Security and Counter-Terrorism Directorate

SERIES:
Monaco, Lisa - Subject Files

FOLDER TITLE:
Russia Response Rollout

FRC ID:
70724

OA Num.:
W1100

NARA Num.:

FOIA IDs and Segments:

22-26844-F

22-26842-F

22-26841-F

22-26840-F 3

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

Deed of Gift Restrictions

A. Closed by Executive Order 13526 governing access to national security information.
B. Closed by statute or by the agency which originated the document.
C. Closed in accordance with restrictions contained in donor's deed of gift.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Records Not Subject to FOIA

Court Sealed - The document is withheld under a court seal and is not subject to the Freedom of Information Act.

1. Tick Toc
2. POTUS statement
3. Q/A
4. Fact sheet
5. JAR
6. DNI/DHS statement - (Oct 7)
7. EO

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
LEADING INTELLIGENCE INTEGRATION

Joint DHS and ODNI Election Security Statement

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

October 07, 2016

Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security

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

Joint DHS and ODNI Election Security Statement

to state and local officials.

Withdrawal Marker
Obama Presidential Library

FORM	SUBJECT/TITLE	PAGES	DATE	RESTRICTION(S)
Email	From Joe "Michael" Daniel to Lisa O. Monaco et al.	1	12/28/2016	P1/b1;

This marker identifies the original location of the withdrawn item listed above. For a complete list of items withdrawn from this folder, see the Withdrawal/Redaction Sheet at the front of the folder.

COLLECTION:
National Secuirty Council - Homeland Security and Counter-Terrorism Directorate

SERIES:
Monaco, Lisa - Subject Files

FOLDER TITLE:
Russia Response Rollout

FRC ID:
70724

OA Num.:
W1100

NARA Num.:

FOIA IDs and Segments:

22-26844-F 3

22-26842-F 3

22-26841-F 3

22-26840-F 3

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

Deed of Gift Restrictions

A. Closed by Executive Order 13526 governing access to national security information.
B. Closed by statute or by the agency which originated the document.
C. Closed in accordance with restrictions contained in donor's deed of gift.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Records Not Subject to FOIA

Court Sealed - The document is withheld under a court seal and is not subject to the Freedom of Information Act.