

From: [Wulf, David](#)
To: (b) (6)
Subject: FW: DHS -- Missouri Secretary of State
Date: Tuesday, December 12, 2017 11:24:05 AM

From: Krebs, Christopher
Sent: Friday, September 22, 2017 4:00 PM
To: Kolasky, Robert (b) (6) >
Cc: Wulf, David (b) (6)
Subject: FW: DHS -- Missouri Secretary of State

FYI

Christopher C. Krebs
Department of Homeland Security
(b) (6)

From: (b) (6)
Sent: Friday, September 22, 2017 3:49:37 PM
To: Krebs, Christopher; (b) (6)
Cc: (b) (6)
Subject: FW: DHS -- Missouri Secretary of State

(b) (5), (b) (6), (b) (7)(A), (b) (7)(E)

Thanks.

(b) (6)
U.S. Department of Homeland Security
Office: (b) (6)
Mobile: (b) (6)
(b) (6) @hq.dhs.gov


Sent from phone. Please excuse typos.

From: (b) (6)
Sent: Friday, September 22, 2017 8:43:36 PM
To: (b) (6)
Cc: (b) (6)
Subject: DHS -- Missouri Secretary of State

(b) (6)

(b) (5), (b) (6), (b) (7)(A), (b) (7)(E)

(b) (5), (b) (6), (b) (7)(A), (b) (7)(E)




Much appreciated.

(b) (6)




Missouri Secretary of State

Cell (b) (6)



Sent from my iPhone

From: (b) (6)
To: [Kolasky, Robert](#)
Cc: (b) (6) [Wulf, David](#) (b) (6)
Subject: Article: Congressional Task Force on Election Security--Preliminary Findings and Recommendations
Date: Thursday, November 16, 2017 11:00:00 AM
Attachments: [cs11152017_CTFES_Findings.pdf](#)

Bob-

Per your request (b) (5), (b) (7)(E)

Link to article is below.

<https://www.politico.com/newsletters/morning-cybersecurity/2017/11/15/house-dems-nearing-release-of-major-election-security-legislation-223370>

Thanks,

(b)

(b) (6)

DHS, Office of Infrastructure Protection

(b) (6)

CONGRESSIONAL TASK FORCE ON ELECTION SECURITY

PRELIMINARY FINDINGS AND RECOMMENDATIONS

One year ago, 139 million Americans cast their vote in the wake of a massive Russian cyber-enabled influence operation designed to “undermine public faith in the U.S. democratic process, denigrate Secretary [Hillary] Clinton, and harm her electability and potential presidency.” Using a vast network of social media trolls, fake “bot” accounts, and state-owned news outlets, the Kremlin spread disinformation to the American electorate through more than 1,000 YouTube videos, 130,000 tweets, and 80,000 Facebook posts viewed by as many as 150 million people on Facebook platforms alone. They hacked into U.S. political organizations, selectively exposing sensitive personal information about DNC staffers using third-party intermediaries like WikiLeaks. Finally, according to U.S. intelligence reports, Russia targeted voter registration databases in at least 21 states and sought to infiltrate the networks of voting equipment vendors, political parties, and at least one local election board.

Although this election cycle was unlike any before, the U.S. Intelligence Community warns that it may be the “New Normal.” Recent reports show that the vast majority of U.S. states are still relying on outdated, insecure voting equipment and other election technologies that lack even basic cybersecurity standards. Meanwhile, Republicans in Congress have shown little interest in fighting Russian interference, and have instead chosen to act on measures that would eliminate rather than bolster funding for the Election Assistance Commission (EAC), the Federal agency responsible for helping states secure these vulnerable systems.

With just over a year until the 2018 midterm elections, it is important that we reflect on lessons learned in the last year and focus the spotlight on election security to push for reforms that protect the integrity of the ballot box.

The Congressional Task Force on Election Security has spent the past five months working together to understand the threats to election infrastructure and how to address them. The Task Force found:

- ***Election security is national security, and our election infrastructure is critical infrastructure.*** Federal law defines critical infrastructure as systems and assets for which “incapacity or destruction . . . would have a debilitating impact on security, national economic security, national public health or safety,” or any combination thereof. Such infrastructure is given priority access to threat intelligence, incident response, technical assistance, and other products and services to help owners and operators harden their defenses. It is hard to imagine a system failure that would inflict more damage than a foreign adversary infiltrating our voting systems to hijack our democratic process. Nonetheless, Trump’s Homeland Security Department (DHS) has wavered on its commitment to honor the Obama Administration’s decision to designate election systems as a critical infrastructure subsector. Whether the next Secretary of Homeland Security will take a firm stand and maintain the designation remains to be seen.
- ***Our election infrastructure is vulnerable.*** Many elections across our country are being run on equipment that is either obsolete or near the end of its useful life. In over 40 states, elections are carried out using voting machines and voter registration databases created more than a decade ago. These technologies are more likely to suffer from known vulnerabilities that cannot be patched easily, if at all. As we saw at this year’s DEFCON Voting Village, even hackers with limited prior knowledge, tools, and resources are able to breach voting machines in a matter of minutes.
- ***These vulnerable systems are being targeted by one of the world’s most sophisticated cyber actors.*** According to the U.S. Intelligence Community, Russian interference in the 2016 election “demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations,” and warned that “Moscow will apply lessons learned from...the US presidential election to future influence efforts worldwide, including against US allies and their election processes.” We cannot reasonably assume that state voting systems are secure enough to withstand a state-sponsored cyber-attack, and we have no reason to believe these attacks will subside.

- **Fortunately, many of the security solutions and best practices are already known.** We can mitigate many vulnerabilities with existing, time-tested cybersecurity fixes found in the NIST Cybersecurity Framework and the CIS “Top 20” Critical Security Controls. By adopting even the Top 5 security controls, organizations can thwart 85% of common cyberattacks. Security experts also tend to agree on the types of voting systems most susceptible to compromise, and are urging election officials to phase out paperless Direct Recording Electronic (DRE) machines, replace these machines with voter-marked paper ballots, and carry out risk-limiting audits to verify election results.
- **Federal agencies like DHS and EAC are important partners in this effort, but they need resources and consistent support from Congress.** We have a rare window of opportunity to promote the widespread adoption of common-sense security measures that protect the integrity of the ballot box. This is not the time to diminish Federal efforts or shut down important lines of dialogue between DHS and election administrators.

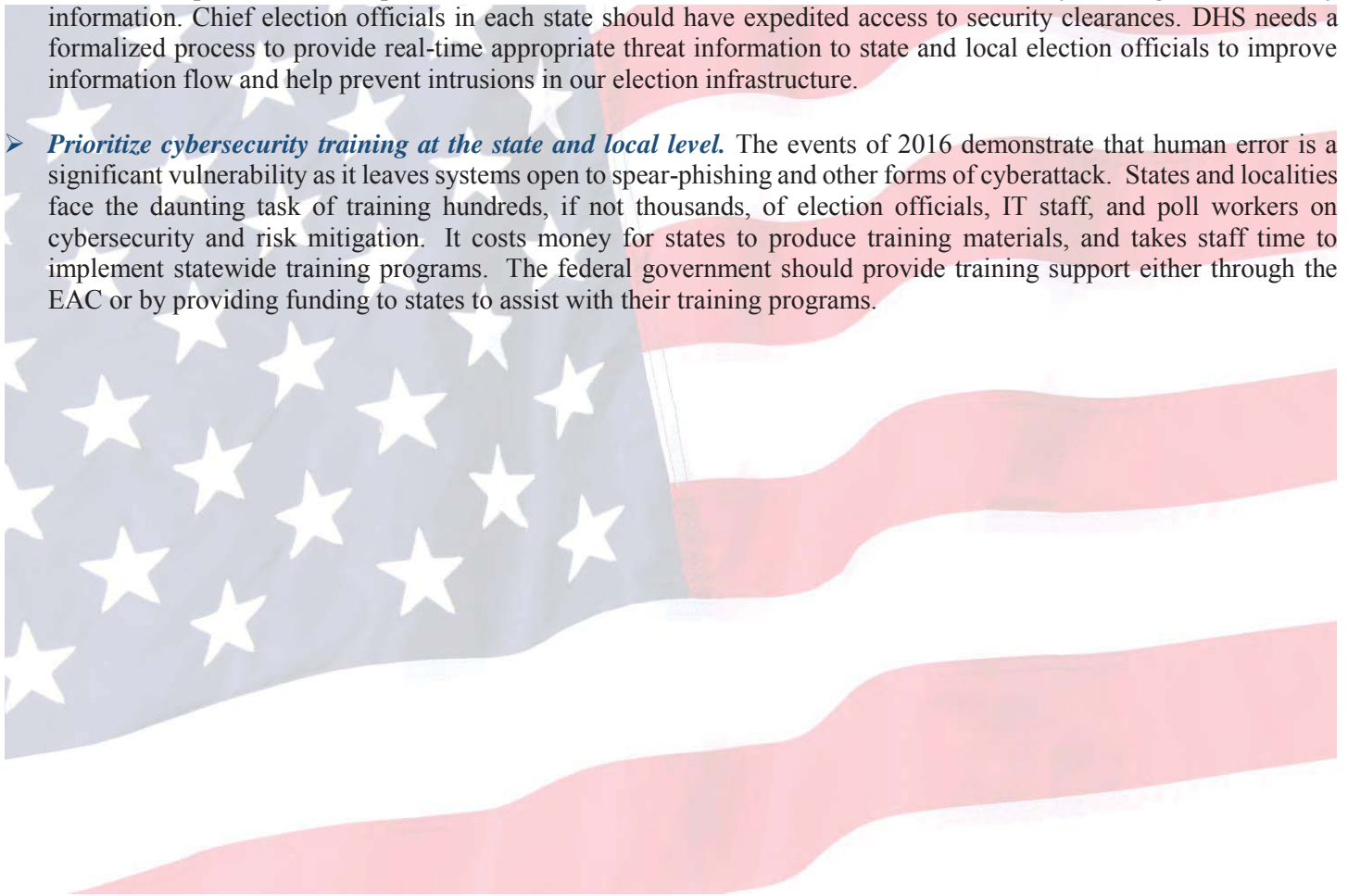
DHS is able to provide participating state and local governments with cyber threat intelligence, vulnerability assessments, penetration testing, scanning of databases and operating systems, and other cybersecurity services at no cost. Despite some initial confusion about the critical infrastructure designation, DHS has worked to build relationships with election officials, clarify the voluntary nature of DHS services, resolve disparities in information sharing and victim notification, and assist the subsector in formally establishing a Coordinating Council, which had its first meeting this fall. Where DHS has rendered assistance, officials report that cyber hygiene scans and other services are valuable. However, there is currently a 9-month wait list for Risk and Vulnerability Assessments, and questions remain about how to ensure threat information reaches election officials, many of whom lack security clearances.

The EAC has been a valuable partner to state and county election officials. The agency has played a crucial role in election security by serving as a clearinghouse of information for state and local election officials, facilitating communications between these officials and DHS, providing easy-to-use cybersecurity guidance, and testing and certifying voting machines. Numerous state and local officials have expressed support and appreciation for the agency’s work. Unfortunately, in recent years Republicans have made several attempts to terminate the agency. Instead, Congress should support the EAC and provide it with the resources it needs to help states secure their election systems. In addition, the President should nominate and the Senate should confirm a fourth commissioner to the EAC so that the agency can operate with its full slate of commissioners.

In light of its preliminary findings, the Task Force makes the following recommendations:

- **Maintain the designation of election infrastructure as a critical infrastructure subsector.** This designation ensures that state and local election officials receive prioritized access to DHS’ cybersecurity services. Defining election systems as critical infrastructure means these systems will, on a more formal and enduring basis, be a priority for DHS cybersecurity assistance. These services are an important force multiplier, especially at the state and local level, where resources are scarce.
- **Help states fund and maintain secure election systems.** We cannot ask our state and local election officials to take on a state actor like Russia alone. Although states and counties are largely responsible for elections, Congress has a role to play in helping states fund the purchase of newer, more secure election systems, and requiring such systems adhere to baseline cybersecurity standards. Election officials need money to replace aging voting systems, many of which do not provide an auditable paper trail. It is important to note, however, that cyber threats evolve at a rapid pace, and a one-time lump sum investment is not enough. States also need resources for maintenance and periodic upgrades, and cybersecurity training for poll workers and other election officials.
- **States should conduct post-election risk-limiting audits.** A risk-limiting audit involves hand counting a certain number of ballots to determine whether the reported election outcome was correct. Risk-limiting audits used advanced statistical methods to enable states to determine that the original vote count was accurate with a high degree of confidence. These audits are useful in detecting any incorrect election outcomes, whether they are caused by a cyberattack or something more mundane like a programming error. Moreover, conducting these audits as a matter of course increases public confidence in the election system.

- ***Empower Federal agencies to be effective partners in pushing out nationwide security reforms.*** With midterm elections in a year, election officials cannot afford to wait 9 months for valuable cybersecurity services like Risk and Vulnerability Assessments. At the same time, we cannot ask DHS to deliver election assistance at the expense of its other critical infrastructure customers. We should give DHS the resources it needs to provide election officials with timely assessments and other cybersecurity services, without detracting from its overall critical infrastructure mission. Similarly, Congress should fund EAC at a level commensurate with its expanded role in election cybersecurity and confirm a fourth commissioner so the agency is able to continue to serve as a resource on election administration.
- ***Establish clear and effective channels for sharing threat and intelligence information with election officials.*** Effective information sharing is critical to address the decentralized threat that our nation faces in terms of securing our elections. Prior to the 2016 elections, we have seen how information sharing failures can cause catastrophic events. The 9/11 terrorist attacks exposed serious gaps in information sharing within the Federal government and state and local law enforcement partners. It is imperative that election officials have access to the most timely and high-level security information. Chief election officials in each state should have expedited access to security clearances. DHS needs a formalized process to provide real-time appropriate threat information to state and local election officials to improve information flow and help prevent intrusions in our election infrastructure.
- ***Prioritize cybersecurity training at the state and local level.*** The events of 2016 demonstrate that human error is a significant vulnerability as it leaves systems open to spear-phishing and other forms of cyberattack. States and localities face the daunting task of training hundreds, if not thousands, of election officials, IT staff, and poll workers on cybersecurity and risk mitigation. It costs money for states to produce training materials, and takes staff time to implement statewide training programs. The federal government should provide training support either through the EAC or by providing funding to states to assist with their training programs.



From: (b) (6)
To: (b) (6)
Subject: FW: 20171003.36 [FOR ADJUDICATION] Gov. McAuliffe writes regarding upcoming Virginia election and requests DHS work directly with state officials (WF1151061)
Date: Friday, November 3, 2017 4:36:01 PM
Attachments: (b) (5), (b) (7)(E)

Any chance you can look at this?

From: (b) (6)
Sent: Friday, November 03, 2017 3:51:00 PM
To: (b) (6)
Cc: IPExecSec
Subject: 20171003.36 [FOR ADJUDICATION] Gov. McAuliffe writes regarding upcoming Virginia election and requests DHS work directly with state officials (b) (7)(E)

(b) (6)

Just assigned this to the COS bucket.

Please review the attached adjudicated response to Gov McAuliffe.
It came back from NPPD with some edits from OGC, PLCY, MGMT and OPE. SOPD adjudicated these edits.

Due today by 5pm.

R/
(b) (6)
Correspondence Analyst
DHS, Office of Infrastructure Protection
(b) (6)

From: (b) (6)
To: (b) (6)
Subject: FW: Coverage of Yesterday's Hearing
Date: Thursday, November 30, 2017 10:27:26 AM

(b) (6)
Assistant Director (Acting), External Affairs, Infrastructure Protection
NPPD/Department of Homeland Security
O: (b) (6)
@hq.dhs.gov

From: (b) (6)
Sent: Thursday, November 30, 2017 1:26:51 PM
To: (b) (6)
Subject: Coverage of Yesterday's Hearing

Good morning,

Below are news clips from the cybersecurity of voting machines hearing yesterday.

[Vote-Hacking Fears Help State Officials Get Security Clearances \(11/29\) – Bloomberg](#)

Three months before some U.S. states host primary elections, the Department of Homeland Security has begun offering security clearances to state officials to more easily share classified information as the threat of cyberattacks looms over next year's polls.

[States Need Federal Help to Protect Voting Machines from Russian Hackers \(11/29\) – USA Today](#)

Congress needs to boost funding to states to help them buy secure voting machines to prevent Russia and other hostile nations from hacking U.S. elections. Experts also recommended that states stop using touchscreen voting machines and replace them with paper-based systems such as optical scanners that tabulate paper ballots and provide tangible evidence of election results.

[Cybersecurity of Voting Machines \(11/29\) – C-SPAN](#)

Two House Oversight and Government Reform subcommittees examined the cybersecurity of U.S. voting machines and what the federal government and states can do to prepare for the 2018 midterm election. Chris Krebs, Senior Official Performing the Duties of the Under Secretary, testified at this hearing.

[DHS official says 'trust' with states prevents sharing cyber threats to election with Congress \(11/30\) – Inside Cybersecurity](#)

The Department of Homeland Security's Christopher Krebs told House lawmakers that a "trust" relationship with state officials has prevented the department from sharing specific details about cyber threats to the 2016 presidential election with Congress. Krebs said "we

From: (b) (6)
To: (b) (6)
Cc: [IP Executive Secretariat](#) (b) (6)
Subject: RE: ASSIGNMENT [DRAFT FOR IP COS APPROVAL] Sen. Durbin writes on Russia's interference with the election process (b) (7)(E)
Date: Monday, July 24, 2017 4:54:36 PM
Attachments: (b) (5)

(b) (6)

Edits attached. Reviewed by (b) (6)

V/R,

(b) (6)

From: (b) (6)
Sent: Thursday, July 20, 2017 6:25 PM
To: (b) (6)
Cc: IP Executive Secretariat (b) (6)
Subject: RE: ASSIGNMENT [DRAFT FOR IP COS APPROVAL] Sen. Durbin writes on Russia's interference with the election (b) (7)(E)

(b) (6) sending this via email for ease of review. Please let us know if you have any issue with CS&C's draft response to Sen Durbin's letter.

Will send via ESTT as well.

(b) (6)
Executive Secretary for Infrastructure Protection
U.S. Department of Homeland Security
National Protection and Programs Directorate
(b) (6)
Arlington, VA 22201
Desk: (b) (6)
Cell: (b) (6)

[How are we doing?](#)

From: IP_4 (b) (6)
Sent: Thursday, July 20, 2017 10:39 AM
To: (b) (6)
Subject: ASSIGNMENT [DRAFT FOR IP COS APPROVAL] Sen. Durbin writes on Russia's interference

with the election process (b) (7)(E)

Assignment Notification for IP_4

The following task has been assigned to your organization from NPPD_ExecSec4

Task ID: (b) (7)(E)

Task Title: [DRAFT FOR IP COS APPROVAL] Sen. Durbin writes on Russia's interference with the election process (b) (7)(E)

Due date: 7/21/2017 5:00:00 PM

Task Requirement:

Date of Tasking	Thursday, July 20, 2017
Subject	Sen. Durbin writes on Russia's interference with the election process
Requested Action	COS level review of draft and enclosure.
Requested Products	N/A
Lead Office	CS&C
Required Coordinators	OGC (b) (6) IP, EA (OLA)
Special Instructions	Please see incoming and CS&C's draft response and enclosure for review.
Notes	Per previous discussions between NPPD Exec Sec, CS&C, and IP, all election interference related actions should be coordinated with IP.
Date Due to NPPD ExecSec	July 21 at COB
Control Numbers	DHS (b) (7)(E) ESTT: (b) (7)(E)
NPPD ExecSec POC	(b) (6) @hq.dhs.gov

Task Note:

Tasked by (b) (6)

To view details of this task, please check the IP_4 Dashboard and click on (b) (7)(E) [DRAFT FOR IP COS APPROVAL] Sen. Durbin writes on Russia's interference with the election process (b) (7)(E)

(b) (7)(E)

Operational questions contact your ExecSec POC

Technical Questions contact: (b) (7)(E)

From: (b) (6)
To: (b) (6)
Cc: (b) (6)
Subject: RE: COMMENT/CLEARANCE DUE BY 3:00PM TODAY - FW: election security related legislation for review - 1) RESILIENCE Act; 2) Securing America's Elections Act of 2017; 3) SAVE Act
Date: Tuesday, December 5, 2017 3:27:29 PM
Attachments: (b) (5)
Importance: High

ALCON,

Following up to see if there are any concerns/ comments to the attached legislation for inclusion prior to clearing without comment?

(b) (6)

From: (b) (6)
To: (b) (6)
Subject: RE: Interesting Article
Date: Sunday, September 3, 2017 3:59:00 PM

(b) (6)

(b) (5), (b) (6)

v/r,
Greg

(b) (6)
U.S. Department of Homeland Security
Office of Infrastructure Protection
(b) (6)
q.dhs.gov

From: (b) (6)
Sent: Friday, August 25, 2017 10:37 PM
To: (b) (6)
Subject: Interesting Article

<http://www.msn.com/en-us/news/politics/us-state-election-officials-still-in-the-dark-on-russian-hacking/ar-AAqGmUf>

From: (b) (6)
Subject: FW: JOINT DHS, ODNI, FBI STATEMENT ON RUSSIAN MALICIOUS CYBER ACTIVITY
Date: Thursday, December 29, 2016 2:22:14 PM
Attachments: (b) (5), (b) (7)(E)

FYI team! Pls let me know if you come across this in your analysis as well! Thanks!

V/r,
(b) (6)

Sent from iPhone

From: DHS.IGA
Sent: Thursday, December 29, 2016 3:09:58 PM
To: DHS.IGA
Subject: 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.

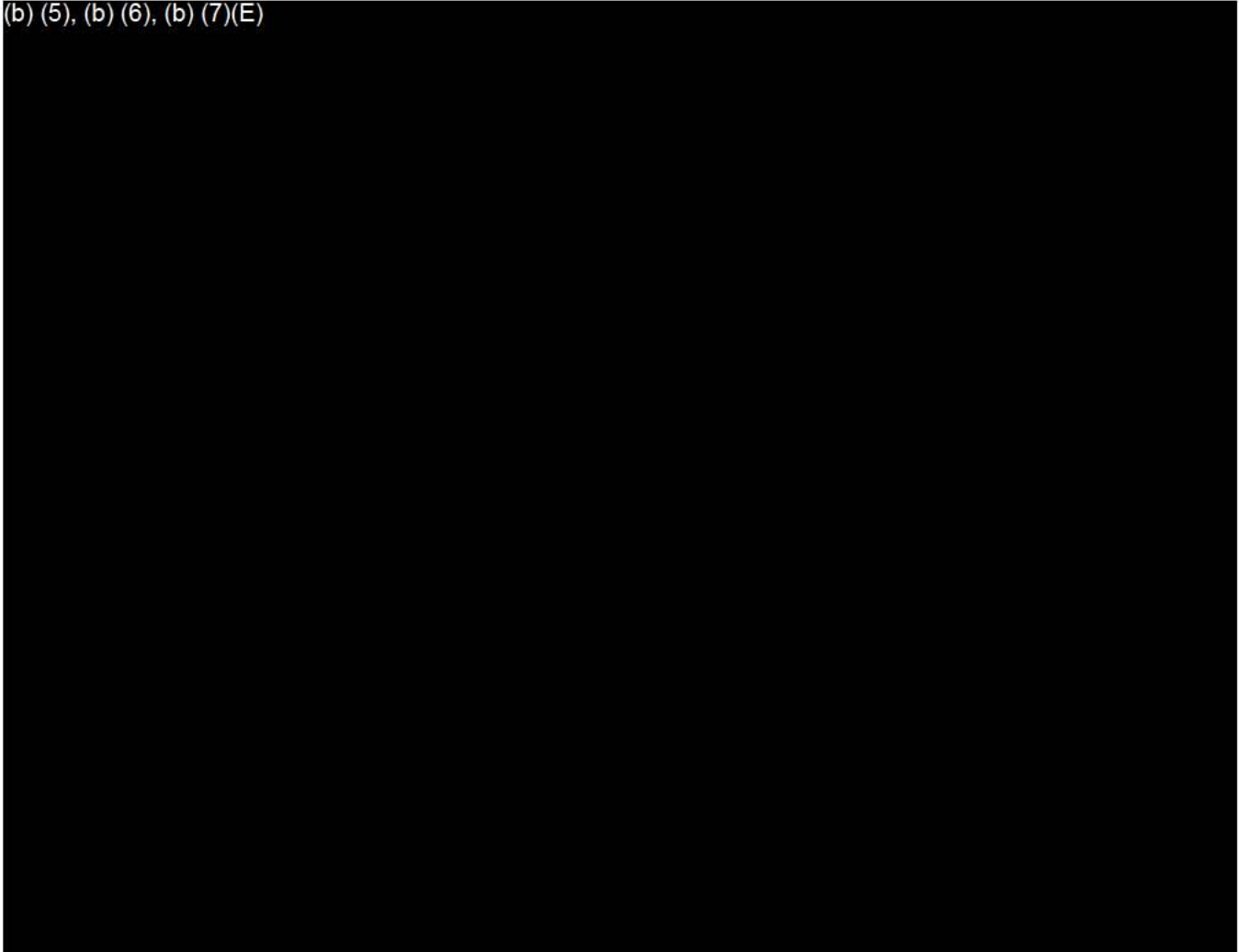
We encourage security companies and private sector owners and operators to look back within their network traffic for signs of the malicious activity described in the Joint Analysis Report. We also encourage such entities to utilize these indicators in their proactive defense efforts to block malicious 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).

###

From: (b) (6)
To: (b) (6)
Cc: (b) (6)
Subject: FW: U.S. state election officials still in the dark on Russian hacking
Date: Tuesday, September 5, 2017 2:08:08 PM
Attachments: [image003.png](#)
Importance: High

(b) (5), (b) (6), (b) (7)(E)



U.S. state election officials still in the dark on Russian hacking

By Dustin Volz

[Reuters](#) August 25, 2017

[https://www.yahoo.com/news/u-state-election-officials-still-dark-russian-hacking-](https://www.yahoo.com/news/u-state-election-officials-still-dark-russian-hacking-100227732.html)

[100227732.html](https://www.yahoo.com/news/u-state-election-officials-still-dark-russian-hacking-100227732.html)

ANAHEIM, Calif. (Reuters) - The federal government has not notified U.S. state election officials if their voting systems were targeted by suspected Russian hackers during the 2016 presidential campaign, and the information will likely never be made public, a top state election chief told Reuters.

"You're absolutely never going to learn it, because we don't even know it," Judd Choate, state

election director for Colorado and president of the National Association of State Election Directors, said in an interview on Thursday during the group's summer conference.

Nearly 10 months after Republican Donald Trump's upset presidential victory over Democrat Hillary Clinton, Choate said he had not spoken to a single state election director who had been told by the U.S. Department of Homeland Security if their state was among those attacked.

The lack of information-sharing on the election breaches reflects the difficulty state and federal officials have had in working together to protect U.S. voting from cyber threats. All U.S. elections are run by state and local governments, which have varying degrees of technical competence.

DHS told Congress in June that 21 states were targeted during the 2016 presidential race, and that while a small number were breached, there was no evidence any votes were manipulated.

Other reports have said 39 states were targeted. Choate said he had heard both numbers mentioned.

Several lawmakers, including Senator Mark Warner, the top Democrat on the U.S. Senate Intelligence Committee, have expressed frustration at DHS' refusal to identify which states had been targeted. Arizona and Illinois confirmed last year that hackers had targeted their voter registration systems.

In a statement, the DHS did not refute that states had not been notified if they were targeted, adding the agency informed the owners or operators of systems potentially victimized "who may not necessarily" be state election officials.

DHS was working with senior state election officials "to determine how best to share this information while protecting the integrity of investigations and the confidentiality of system owners," the agency said.

U.S. intelligence agencies have concluded that the Kremlin orchestrated an operation that included hacking and online propaganda intended to tilt the November election in Trump's favor.

Several congressional committees are investigating and Special Counsel Robert Mueller is leading a separate probe into the Russia matter, including whether Moscow colluded with the Trump campaign. Russia has denied election meddling and Trump has denied any collusion.

'LEARN FROM THE MISSTEPS'

The four-day conference of election directors was originally supposed to be about issues like voter registration, but took a sharp turn following the election hacking.

"After the 2000 election, we all had to be lawyers," Choate said. "And now after the 2016 election, we all have to be cyber security experts."

DHS representatives at the event fended off questions about whether the federal government would be prepared to mobilize sufficient support for the states in the event of a catastrophic cyber attack near or during the 2018 elections.

"We want to make sure we learn from the missteps that may have happened in 2016 and we

want to make sure we continue building on the things we did that were right," Robert Gatlin, a DHS cyber official, said during a panel discussion.

Gatlin said the agency was working with U.S. intelligence agencies to "downgrade" more classified information so it could be shared with the states. Information about cyber attacks is typically guarded by a high classification because it may involve nation-state involvement or contain sensitive sources and methods, he said.

Legislation recently approved by the Senate Intelligence Committee would require the director of national intelligence to sponsor top-secret security clearance for eligible election officials in each state, something the National Association of Secretaries of State has advocated.

The bill would also require DHS to submit a report to Congress detailing cyber attacks and attempted cyber attacks by foreign governments on U.S. election infrastructure during the 2016 election.

Choate said communication about cyber threats had improved with federal agencies since the election and the decision by the outgoing Obama administration in January to elevate voting systems to a "critical infrastructure designation."

Prior to the election, some state officials worried that closer oversight of election systems represented a dangerous federal intrusion into local affairs.

(Reporting by Dustin Volz; Editing by Jonathan Weber and Peter Cooney)

(b) (6)
[Redacted text block]



This communication is covered by federal and state law governing electronic communications and may contain confidential, legally privileged information. If you are not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message or any attachments is prohibited. If you received this message in error, please reply immediately to the sender and delete this message.

The subsequent 6 pages, (NPPD 002079 through NPPD 002084) are being withheld in their entirety pursuant to 5 U.S.C. § 552 (b)(5), (b)(7)(A), (b)(7)(E) and (b)(7)(F).

NPPD 002079 – NPPD 002084