AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 115–347

OPEN HEARING: ELECTION SECURITY

HEARING

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE

OF THE

UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

WEDNESDAY, MARCH 21, 2018

Printed for the use of the Select Committee on Intelligence

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
29–480 PDF WASHINGTON : 2018

SELECT COMMITTEE ON INTELLIGENCE

[Established by S. Res. 400, 94th Cong., 2d Sess.]

RICHARD BURR, North Carolina, *Chairman*
MARK R. WARNER, Virginia, *Vice Chairman*

JAMES E. RISCH, Idaho
MARCO RUBIO, Florida
SUSAN COLLINS, Maine
ROY BLUNT, Missouri
JAMES LANKFORD, Oklahoma
TOM COTTON, Arkansas
JOHN CORNYN, Texas

DIANNE FEINSTEIN, California
RON WYDEN, Oregon
MARTIN HEINRICH, New Mexico
ANGUS KING, Maine
JOE MANCHIN, West Virginia
KAMALA HARRIS, California

MITCH MCCONNELL, Kentucky, *Ex Officio*
CHUCK SCHUMER, New York, *Ex Officio*
JOHN MCCAIN, Arizona, *Ex Officio*
JACK REED, Rhode Island, *Ex Officio*

CHRIS JOYNER, *Staff Director*
MICHAEL CASEY, *Minority Staff Director*
KELSEY STROUD BAILEY, *Chief Clerk*

CONTENTS

MARCH 21, 2018

OPENING STATEMENTS

Burr, Hon. Richard, Chairman, a U.S. Senator from North Carolina 1
Warner, Mark R., Vice Chairman, a U.S. Senator from Virginia 2

WITNESSES

Panel 1

Nielsen, Kirstjen, Secretary, Department of Homeland Security 4
Prepared statement 7
Johnson, Jeh Charles, former Secretary, Department of Homeland Security 14
Prepared statement 15

Panel 2

Manfra, Jeanette, Assistant Secretary, National Protection and Programs Directorate, Office of Cyber Security and Communications, Department of Homeland Security 48
Condos, Jim, Secretary of State, State of Vermont 50
Prepared statement 52
Cohen, Amy, Executive Director, National Association of State Election Directors 57
Prepared statement 61
Rosenbach, Eric, Co-Director, Belfer Center for Science and International Affairs, Harvard Kennedy School 66
Prepared statement 69

SUPPLEMENTAL MATERIAL

Prepared Statement of Thomas Hicks, Chairman, U.S. Election Assistance Commission 98

OPEN HEARING: ELECTION SECURITY

WEDNESDAY, MARCH 21, 2018

U.S. SENATE,
SELECT COMMITTEE ON INTELLIGENCE,
Washington, DC.

The Committee met, pursuant to notice, at 9:34 a.m. in Room SH–216, Hart Senate Office Building, Hon. Richard Burr (Chairman of the Committee) presiding.

Present: Burr, Warner, Risch, Rubio, Collins, Blunt, Lankford, Cotton, Cornyn, Feinstein, Wyden, Heinrich, King, Manchin, Harris, and Reed.

OPENING STATEMENT OF HON. RICHARD BURR, CHAIRMAN, A U.S. SENATOR FROM NORTH CAROLINA

Chairman BURR. I'd like to call this hearing to order, and at the beginning of this hearing I would like to thank all the members, the witnesses, the press, and those visitors that we have today, with the inclement weather that was predicted and some has fallen. We thought it was important to continue this hearing, so I'm grateful to each of our witnesses. And to those that couldn't make it because of flights today, we have tried to adjust so we've got the appropriate witnesses for the second panel as well.

Today the committee convenes the first open hearing to reflect the progress and preliminary recommendations and findings of our investigation into Russia's attempt to interfere in the 2016 U.S. elections. I'd like to welcome our two distinguished witnesses: Secretary of Homeland Security Kirstjen Nielsen; and former Secretary of Homeland Security Jeh Johnson. Jeh, I am grateful for the service that you provided to your country in a number of places. And, Secretary Nielsen, I have enjoyed very much the time that you have been there and look forward to what we can accomplish between this committee and the Department of Homeland Security in the future.

I want to thank both of you for being here—for being here together, which I think is unprecedented, and I am grateful to the Administration for agreeing. It speaks to the importance of the issue and sends a message that transcends partisanship.

The Vice Chairman and I asked the two of you to appear together to tell the story of what happened in 2016, how the Department reacted then and how it has evolved and what it is doing today. I think your collective remarks will show the remarkable evolution of an agency that is playing an increasingly important role to support the states.

When this cyber threat surfaced in 2016, many struggled to understand the attack, the intentions behind it, and how to respond. By the beginning of 2018, however, DHS has made great strides towards better understanding elections, better understanding the states, and providing assistance that makes a difference to the security of our elections.

But there's more to do. There's a long wait time for DHS premier services. States are still not getting all the information they feel they need to secure their systems. The Department's ability to collect all the information needed to fully understand the problem is an open question, and attributing cyber attacks quickly and authoritatively is a continuing challenge.

Secretary Nielsen, as you appropriately note in your statement, the administration of elections is the responsibility of the State and local officials. And the support your agency provides is on a voluntary basis. What we've learned is that states will only engage with the Department if they feel there's value. And I'm confident that the customer service, if you can call it that, and the value you're providing to your State partners is improving every single day.

Securing our elections requires immediate action and the urgency is reflected in the committee's recommendations released yesterday. We've convened today's hearing, in the midst of a snowstorm of sorts, to speak to the American people publicly about the threat posed by Russia and the efforts by our Federal, State, and local governments to protect against it.

This issue is urgent. If we start to fix these problems tomorrow, we still might not be in time to save the system for 2016 and 2020.

I understand, Secretary Nielsen, you have a hard stop, something about a Cabinet meeting, and we respect those Cabinet meetings when the President calls it. So in the interest of time, I will end there and I will turn to the Vice Chairman for any remarks he might have.

OPENING STATEMENT OF HON. MARK R. WARNER, VICE CHAIRMAN, A U.S. SENATOR FROM VIRGINIA

Vice Chairman WARNER. Thank you, Mr. Chairman. I'd like to welcome the witnesses as well.

Today's hearing comes at a critical time. The committee remains in the midst of our bipartisan investigation into the Russian attacks during the 2016 election, and we still have more work to do. However, we as a committee felt it was important to move out our initial findings and recommendations on securing our election infrastructure, given the upcoming elections in November.

Our main question today is, how do we protect 2018 elections? And the threat is real and growing. During the 2016 campaign, we saw unprecedented targeting of election infrastructure by Russian actors. Russian hackers were able to penetrate Illinois' voter registration database and access 90,000 voter registration records. They also attempted to target the election systems of at least 20 other states. The intelligence community's assessment last January concluded that Russia secured and maintained access to multiple elements of U.S. State and local election boards.

The truth is clear that 2016 will not be the last of their attempts. Just weeks ago, we heard from all our top intelligence officials testifying before this committee that the Russians will continue to attack our elections. Unfortunately, there are signs that the Kremlin is becoming more brazen. As we saw recently, the Putin regime was behind an assassination attempt on European soil with a prohibited military-grade nerve agent. This is obviously not the action of a regime that will be easily deterred.

So how are we prepared to come against this threat that we know is coming again? Elections at all levels are central to our democracy, to our institutions, and to our government's legitimacy, and I remain concerned that we're still not fully prepared.

Candidly—and I've shared this with both of you—I was disappointed on how the Department of Homeland Security, the primary U.S. government agency responsible for election security, approached this issue early on. During the 2016 election, officials at both the Federal and State level were caught flat-footed, and the follow-up from the new Administration was not much better.

Last June we heard from DHS, FBI, and State election officials about the threat to our election systems, which, based upon Secretary Johnson's earlier actions, DHS considers part of our Nation's critical infrastructure. Despite evidence of interference, the Federal Government and the states had barely communicated about strengthening our defenses. It was not until the fall of 2017 that DHS even fully notified the states that they had been potential targets. And unfortunately, that was an issue that members of this committee, bipartisan, stressed in our hearing last June. Candidly, we have to improve those communications.

But clearly, more must be done, from hardening our election registration and voting systems, to ensuring that voting machines have backup paper ballots, to instituting audits and providing additional Federal assistance to those states that request it. One area I know that we're not going to talk about today, but I think does need additional investigation, is how we make sure that the ultimate startups, campaigns, have to practice basic cyber security.

The threat is real and the need to act is urgent. We need the Administration to accelerate its efforts. Perhaps most of all, we need a President who will acknowledge the gravity of this threat and lead a whole-of-society effort to harden our defenses and inoculate our society against Russia's malicious interference. The fact that the President did not even bring up the topic of our election security when he called Vladimir Putin to congratulate him on his victory in a precooked election I believe is extremely troubling.

The good news is this problem is not a Democratic or Republican one, and I personally want to thank all the members of the committee on both sides of the aisle for the good work that they've done. We're going to hear from some of them who've been working on a set of recommendations, and Senator Rubio has also been working on a set of recommendations. We all have to get this done and we have to act quickly.

Again, I am pleased to have both of the secretaries here. I know it's a little bit unprecedented. I thank them both for being here and thank them for getting through the storm.

With that, Mr. Chairman, I look forward to our hearing.

Chairman BURR. I thank the Vice Chairman.

This morning we'll hear from Secretary Nielsen and Secretary Johnson. Their testimony will be followed up by questions of up to five minutes from members, recognizing first Senator Collins, followed by Heinrich, Lankford, Harris, the Chair, the Vice Chair, and then members based upon seniority after that.

Having covered that, Secretary Nielsen, the floor is yours.

STATEMENT OF KIRSTJEN NIELSEN, SECRETARY, DEPARTMENT OF HOMELAND SECURITY

Secretary NIELSEN. Well, good morning. Thank you for having me here. I want to thank Chairman Burr, Vice Chairman Warner, and all the members of the committee for not only the opportunity to testify, but I really do want to thank you for your leadership. Your bipartisan efforts here to assess what we did, what we didn't do, what we can do better, what we can do better in partnership, really can't be overstated in terms of its importance, so I thank you for that.

Before we begin, I just wanted to extend my thanks to the first responders who've been working around the clock in Texas on the package bombing case. At DHS we've been in close contact with those on the ground and, although the situation appears to be over, we urge the public to remain alert and report any suspicious activity or packages or devices.

Over the course of nearly three weeks, at least seven explosive devices were encountered in and around the Austin area, with five of them unfortunately detonating. Our thoughts go out to the victims and their families, and our gratitude is extended to the frontline defenders who helped locate the alleged perpetrator.

The suspect is now deceased, but the case is yet another stark reminder of the importance of both public vigilance and also how important it is for close Federal, State, and local coordination. That coordination is also relevant, clearly, to the issue we have before us today.

In a democracy, citizens must have faith that their vote counts and is counted correctly. Recently, in the United States and around the globe, we have seen malicious foreign actors attempt to subvert democracy by taking action to influence voters and by exploiting vulnerabilities in cyber space to attack election systems.

In 2016, we know that Russian actors targeted State election systems. We have no evidence that votes were changed as a result of their efforts. However, the threat of interference remains and we recognize that the 2018 midterm and future elections are clearly potential targets for Russian hacking attempts.

Today we have a whole-of-government effort to improve the resilience and security of those systems, which is led by DHS with assistance from the Departments of Justice, the FBI, and the Office of the Director of National Intelligence. We are working with the vendor community and, most importantly, we are working in voluntary partnership with our State and local election partners.

There is also a separate initiative to address efforts by foreign nationals to influence our elections through messaging, propaganda, and manipulation. I think this is also a very important

topic. That effort is being led by the Department of Justice, the FBI, and the Department of State.

While DHS will, of course, support this effort, I will let my colleagues discuss their work in that area, and instead today I look forward to discussing the work that the Department is doing to assist State and local officials to harden our election systems.

Under our Constitution and laws, as has been mentioned by the Chairman and the Vice, the administration of elections is the responsibility of State and local officials. The Department's mission is to provide assistance and support to those officials in the form of advice, intelligence, technical support, incident response planning, with the ultimate goal of building a more resilient, redundant, and secure election enterprise.

Our services are voluntary and not all election officials accept our offer of support. We continue to offer it; we continue to demonstrate its value. But in many cases, State and local officials have their own resources and simply don't require the assistance that we're offering.

DHS typically offers a range of technical services. We'll go into some detail today about those. More than half of the states have signed up for our cyber hygiene scanning service, which is an automated remote scan that gives State and local officials a report identifying vulnerabilities and offering recommendations to mitigate them.

We also provide, as I believe you all have noted, on-risk site—excuse me—on-site risk and vulnerability assessments. The assessments are more thorough. We do pen testing. It's a full report of vulnerability and recommendations, and over the past year we've increased the availability of these assessments and prioritized them.

Information sharing is also critical. We share information directly with election officials through trusted third parties such as the Multi-State Information Sharing and Analysis Center, or MS–ISAC, and we look forward to the creation of the Election ISAC. The National Cybersecurity and Communications Integration Center, or the NCCIC, is the Department's hub for information-sharing activity.

Actionable and timely information empowers election officials to make more risk-informed decisions. We must rapidly share information about potential compromises with the broader community so that everyone can defend their systems. This collective defense approach makes all election systems more secure.

We're also working with State election officials to share classified information on specific threats, including sponsoring up to three officials per State with security clearances and providing one-day read-ins as needed when needed, as we did in mid-February for the secretaries of state and election directors. We are also working with the intelligence community to rapidly declassify information to share with our stakeholders.

To be clear, there has been a learning curve on the sharing of information. The election systems in states are often owned and operated by different systems: the secretary of state, the State CIO, in some cases the State CSO, the governor's office, or even counties. While appropriate technical information and notifications were

shared with system owners, we have taken steps to share information much more broadly and rapidly.

Beyond sharing information, we also share best practices for risk management, such as paper ballot backups and risk-limiting audits. The ultimate goal, of course, is enhancing network protection, but we must be prepared for any eventuality, including unauthorized access to systems.

The NCCIC is, again, the center of these efforts. Every day our protective security advisors and cyber security advisors located nationwide are working with election officials on incident response planning and crisis communications. Just yesterday, we had both our head of NPPD as well as our cyber security advisor in Cook County, real-time helping in case there was any issue with the election.

DHS is committed to working collaboratively with those administrating our elections. We have formalized and better coordinated these efforts through the establishment of government and sector coordinating councils. And today I can say with confidence that we know whom to contact in every State to share threat information. That capability did not exist in 2016.

DHS is leading Federal efforts to support and enhance the security of election systems across the country. Yet, we do face a technology deficit that exists not just in election infrastructure, but across State and local government systems. It will require a significant investment over time and will require a whole-of-government solution to ensure continued confidence in our elections.

Personally, I'm looking across my existing authorities as Secretary of the Department and looking at our available grant programs for opportunities to help State and locals in this area. I look forward to working with Congress. I read with great interest the recommendations that were released yesterday from your study and certainly look forward to working with you on implementing them.

Thank you for the opportunity to appear and I look forward to your questions.

[The prepared statement of Secretary Nielsen follows:]

Statement for the Record
of
U.S. Department of Homeland Security

FOR A HEARING ON

"Election Security"

BEFORE THE
UNITED STATES SENATE
SELECT COMMITTEE ON INTELLIGENCE

Wednesdy, March 21, 2018

Washington, DC

Chairman Burr, Vice Chairman Warner, and members of the Committee, thank you for today's opportunity to testify regarding the U.S. Department of Homeland Security's (DHS) ongoing efforts to assist with reducing and mitigating risks to our election infrastructure. Almost a year ago, DHS appeared before this Committee to testify on the same topic. Today, DHS is pleased to share with you the progress we have made to establish trust-based partnerships with our Nation's election officials who administer our democratic election processes. Recognizing that the 2018 U.S. mid-term elections are a potential target for malicious cyber activity, DHS is committed to robust engagement with state and local election officials, as well as private sector entities, to assist them with defining their risk, and providing them with information and capabilities that enable them to better defend their infrastructure. Safeguarding and securing cyberspace is a core homeland security mission.

Election security and integrity covers a number of issues. Of primary importance to this committee are two. The first is election security – the physical and cyber security related to voting and the tallying of the votes. The second is efforts to counter foreign influence of voters themselves. Within the federal government, DHS has the primary responsibility for the former and that is what this testimony will cover. While countering foreign influence is a critical issue in its own right, it involves the leadership of multiple other departments and agencies.

Under our Constitution and laws, the administration of elections is the responsibility of state and local officials. The Department's mission is to provide *assistance* to election officials in the form of advice, intelligence, technical support, and incident response planning with the ultimate goal of building a more resilient and secure election enterprise.

As such, DHS and our federal partners have formalized the prioritization of ***voluntary*** cybersecurity assistance for election infrastructure similar to that which is provided to a range of other critical infrastructure entities, such as financial institutions and electric utilities.

Since 2016, DHS's National Protection and Programs Directorate (NPPD) has convened federal government and election officials regularly to share cybersecurity risk information and to determine an effective means of assistance. The Election Infrastructure Subsector (EIS) Government Coordinating Council (GCC) has worked to establish goals and objectives, to develop plans for the EIS partnership, and to lay the groundwork for developing an EIS Sector-Specific Plan (SSP). GCC representatives include DHS, the Election Assistance Commission (EAC), and 24 state and local election officials. Participation in the council is entirely voluntary and does not change the fundamental role of state and local jurisdictions in overseeing elections.

Additionally, DHS and EAC have worked with election industry representatives to launch an industry-led Sector Coordinating Council (SCC). In general the SCC is self-organized, self-run, and self-governed, with leadership designated by the sector membership. The SCC serves as industry's principal entity for coordinating with the government on critical infrastructure security activities and issues related to sector-specific strategies, and policies. The collaboration of the GCC and SCC is through an established process under DHS's authority to provide a forum in which government and private sector entities can jointly engage in a broad spectrum of activities to coordinate critical infrastructure security and resilience efforts. This structure is used in each of the critical infrastructure sectors established under Presidential Policy

Directive 21—Critical Infrastructure Security and Resilience. It provides a well-tested mechanism across critical infrastructure sectors for sharing threat information among the federal government and critical infrastructure partners, advancing risk management efforts, and prioritizing services available to sector partners in a trusted environment.

In addition to the work of the EIS-GCC and SCC, NPPD continues to directly engage state and local election officials – coordinating requests for assistance, risk mitigation, information sharing, and incident coordination, resources, and services. In order to ensure a coordinated approach from the federal government, NPPD brought together stakeholders from across the Department and other federal agencies as part of an Election Task Force (ETF). The ETF increases the Department's efficiency and effectiveness in understanding, responding to, communicating, and sharing information related to cyber threats. The ETF serves to provide actionable information and offer assistance to assist election officials with strengthening their election infrastructure by reducing and mitigating cyber risk, and increasing resilience of their processes.

Within the context of today's hearing, the Department's testimony will address the unclassified assessment of malicious cyber operations directed against U.S. election infrastructure. DHS's testimony will outline its efforts to help enhance the security of elections that are administered by state and local jurisdictions around the country, our progress to date, and our strategy moving forward.

Assessing the Threat

DHS regularly coordinates with the the intelligence community, and law enforcement partners on potential threats to the Homeland. Among non-federal partners, DHS has been engaging state and local officials, as well as relevant private sector entities, to assess the scale and scope of malicious cyber activity potentially targeting the U.S. election infrastructure. Election infrastructure includes the information and communications technology, capabilities, physical assets, and technologies that enable the registration and validation of voters; the casting, transmission, tabulation, and reporting of votes; and the certification, auditing, and verification of elections.

In addition to working directly with state and local officials, we have partnered with trusted third parties to analyze relevant cyber data, including the Multi-State Information Sharing and Analysis Center (MS-ISAC), the National Association of Secretaries of State and the National Association of State Election Directors. We also used our field personnel deployed around the country, to help further facilitate information sharing and enhance outreach. Such engagement paid off in terms of identifying suspicious and malicious cyber activity targeting election infrastructure in 2016. A body of knowledge grew throughout the summer and fall of 2016 about suspected Russian government cyber activities, indicators, and understanding that helped drive collection, investigations, and incident response activities. On October 7, 2016, DHS and the Office of the Director of National Intelligence (ODNI) released a joint statement on election security and urged state and local governments to be vigilant and seek cybersecurity assistance. Our message today remains the same.

Enhancing Security for Future Elections

NPPD is committed to ensuring a coordinated response from DHS and its federal partners to plan for, prepare for, and mitigate risk to election infrastructure. We understand that working with election infrastructure stakeholders is essential to ensuring a more secure election. Based on our assessment of activity observed in the 2016 elections, NPPD and our stakeholders are increasing awareness of potential vulnerabilities and providing capabilities to enhance the security of U.S. election infrastructure as well as that of our democratic allies.

As mentioned before, under the Constitution and our system of laws, federal elections administered by state and local election officials in thousands of jurisdictions. Security awareness for election officials did not begin in 2016, State and local election officials across the country have a long-standing history of working both individually and collectively to reduce risks and ensure the integrity of their elections. In partnering with these officials through both new and existing, ongoing engagements, NPPD is working to provide value-added – yet voluntary – services to support their efforts to secure elections.

Improving Coordination with State and local partners. Increasingly, the nation's election infrastructure leverages information technology, or IT, for efficiency and convenience. While the benefits are many, reliance on IT introduces cybersecurity risks, just like in any other enterprise environment. Just like with other sectors, NPPD helps stakeholders in federal departments and agencies, state and local governments, and the private sector to manage these cybersecurity risks. Consistent with our long-standing partnerships with state and local governments, we have been working with election officials to share information about cybersecurity risks, and to provide voluntary resources and technical assistance.

The National Cybersecurity and Communications Integration Center (NCCIC) works with the MS-ISAC to provide threat and vulnerability information to state and local officials. Created by DHS over a decade ago, the MS-ISAC is partially funded by NPPD. The MS-ISAC's membership is limited to state and local government entities, and all fifty states and U.S. territories are members. It has representatives co-located with the NCCIC to enable regular collaboration and access to information and services for state chief information officers.

Providing Technical Assistance and Sharing Information. Through engagements with state and local election officials, including working through the Sector Coordinating Council, NPPD actively promotes a range of services to include but are not limited to the following:

Cyber hygiene service for Internet-facing systems: Through this automated, remote scan, NPPD provides state and local officials with a report identifying vulnerabilities and mitigation recommendations to improve the cybersecurity of systems connected to the Internet, such as online voter registration systems, election night reporting systems, and other Internet-connected election management systems.

Risk and vulnerability assessments: We have prioritized State and local election systems upon request, and increased the availability of risk and vulnerability assessments (RVAs). RVAs are more in-depth and executed on-site by NPPD cybersecurity experts. These

evaluations include a system-wide understanding of vulnerabilities, focused on both internal and external systems. When NPPD conducts these assessments, we provide a full report of vulnerabilities and recommended mitigations following the testing.

Incident response assistance: We encourage state and local election officials to report suspected malicious cyber activity to the NCCIC. Upon request, the NCCIC can provide on-site assistance in identifying and remediating a cyber incident. Information reported to the NCCIC is also critical to the federal government's ability to broadly assess malicious attempts to infiltrate election systems. This technical information will also be shared with other state officials so they have the ability to defend their own systems from similar malicious activity.

Knowing what to do when a security incident happens – whether physical or cyber – before it happens, is critical. NPPD supports election officials with incident response planning including participating in exercises and reviewing incident response playbooks. Crisis communications is core component of these efforts, ensuring officials are able to communicate transparently and authoritatively their constituents when an incident unfolds. In some cases, we do this directly with state and local jurisdictions. In others, we partner with outside organizations. We recognize that securing our nation's systems is a shared responsibility, and we are leveraging partnerships to advance that mission.

Information sharing: NPPD shares relevant information on cyber incidents. Information is shared directly with stakeholders and also through trusted third parties. For instance, the NCCIC works with the MS-ISAC, allowing election officials to connect with the MS-ISAC or their State Chief Information Officer to rapidly receive information they can use to protect their systems. State election officials may also receive information directly from the NCCIC. Best practices, cyber threat information, and technical indicators, some of which had been previously classified, have been shared with election officials in thousands of state and local jurisdictions. In all cases, the information sharing and/or use of such cybersecurity risk indicators, or information related to cybersecurity risks and incidents complies with applicable lawful restrictions on its collection and use.

Classified information sharing: To most effectively share information with all of our partners—not just those with security clearances—DHS works with the intelligence community to rapidly declassify relevant intelligence or provide tearlines. While DHS prioritizes declassifying information to the extent possible, DHS also provides classified information to cleared stakeholders, as appropriate. DHS has been working with state chief election officials and additional election staff in each state to provide them with security clearances. By working with the Office of the Director of National Intelligence and the Federal Bureau of Investigation, in February 2018 election officials from each state received one-day read-ins for a classified threat briefing while they were in Washington, DC. This briefing demonstrated our commitment to ensuring election officials have the information they need to understand the threats they face.

Field-based cybersecurity advisors and protective security advisors: NPPD has more than 130 cybersecurity and protective security personnel available to provide actionable information and connect election officials to a range of tools and resources to improve the cybersecurity preparedness of election systems; and to secure the physical site security of voting

machine storage and polling places. These advisors are also available to assist with planning and incident management for both cyber and physical incidents.

Physical and protective security tools, training, and resources: NPPD provides guidance and tools to improve the security of polling sites and other physical election infrastructure. This guidance can be found at www.dhs.gov/hometown-security. This guidance helps to train administrative and volunteer staff on identifying and reporting suspicious activities, active shooter scenarios, and what to do if they suspect an improvised explosive device.

Election Security Efforts Moving Forward

This year our Nation is preparing for upcoming primary and special elections as well as the general election in November. Some states such as Arizona, Texas, and Illinois have already conducted primary elections. Just yesterday, NPPD teammembers observed and supported election security efforts Chicago, demonstrating our close partnership with State and local election officials. We have been working with election officials in all states to enhance the security of their elections by offering support and by establishing essential lines of communications at all levels – public and private – for reporting both suspicious cyber activity and incidents. This information sharing is critical and our goal is to enhance transparency and have visibility of aggregated elections-related cybersecurity efforts. We are also working with election officials, vendors, the EAC, and NIST to characterize risk to election systems and ensure appropriate mitigations are understood and available in the marketplace. As a part of this process, we work with these stakeholders to recommend best practices to ensure a secure and verifiable vote.

Over the course of the past eight months, DHS has made tremendous strides and has been committed to working collaboratively with those on the front lines of administering our elections—state and local election officials and the vendor community—to secure election infrastructure from risks. The establishment of government and sector coordinating councils will build the foundations for this enduring partnership not only in 2018, but for future elections as well. We will remain transparent as well as agile in combating and securing our physical and cyber infrastructure. However, we recognize that there is a signfiicant technology deficit across State and local governments, and State and local election systems, in particular. It will take signficant and continual investment to ensure that systems are upgraded and insecure or vulnerable systems are retired.

While the activities described above deal with DHS's efforts to secure election infrastructure, there is a whole of government approach under this administration to address election infrastructure security as well as countering foreign influence. Two weeks ago, the leaders of DHS, DOJ, FBI, DNI, NSA and others convened a meeting at the National Cybersecurity and Communication Integration Center to futher coordinate our efforts. Tthe White House is holding a follow up meeting on this topic later today. As a group, this Administration – this President – is committed to addressing these risks.

In closing, we recognize the fundamental link between public trust in our election infrastructure and the confidence the American public places in basic democratic functions. Ensuring the security of our electoral process is a vital national interest and one of our highest priorities at DHS. Our voting infrastructure is diverse, subject to local control, and has many checks and balances. As the threat environment evolves, DHS will continue to work with federal agencies, state and local partners, and private sector entities to enhance our understanding of the threat; and to make essential physical and cybersecurity tools and resources available to the public and private sectors to increase security and resiliency.

Thank you for the opportunity to appear before the Committee today. The Department looks forward to your questions.

Chairman BURR. Secretary Nielsen, thank you very much.

Secretary Johnson, you are recognized. The floor is yours.

STATEMENT OF JEH CHARLES JOHNSON, FORMER SECRETARY, DEPARTMENT OF HOMELAND SECURITY

Mr. JOHNSON. Chairman Burr, Vice Chairman Warner, other members of this committee: I am pleased to be here alongside the Secretary of Homeland Security as a witness and a concerned private citizen. I had the privilege of testifying before Congress 26 times in 37 months as Secretary, and if I'm not called back once in a while I begin to feel left out.

I'm also pleased that this committee has undertaken this hearing on this important topic of election cyber security. You have my prepared statement; I won't read it in detail. It sets forth the efforts we made in the Department of Homeland Security in 2016 to assist states in securing their election infrastructure prior to the election and the five written public statements I made warning the public and the states about the cyber threat to the election.

Beyond that, I'd like to say this: As each member of this committee knows, in 2016 the Russian government, at the direction of Vladimir Putin himself, orchestrated cyber attacks on our Nation for the purpose of influencing the election that year, plain and simple. The experience was a wakeup call for our Nation as it highlighted cyber vulnerabilities in our political process and in our election infrastructure itself.

Now, with the experience fresh in our minds and clear in our rearview mirror, the key question for our leaders at the national and State level is, what are we going to do about it? The matter is all the more urgent given the public testimony our Nation's intelligence chiefs gave before this very committee last month that the Russian effort to interfere in our democracy has not ended.

I have seen this committee's draft recommendations for the future and I agree with them. The reality is that, given our Electoral College and our current politics, national elections are decided in this country in a few precincts in a few key swing states. The outcome therefore may dance on the head of a pin. The writers of the TV show "House of Cards" have figured that out. So can others.

I am pleased by reports that State election officials to various degrees are now taking serious steps to fortify cyber security of their election infrastructure and that the Department of Homeland Security is currently taking serious steps to work with them in that effort. As a Nation we must resolve to strengthen our cyber security generally and the cyber security around election infrastructure specifically. Nothing less than the health and strength of our democracy depends on this.

I look forward to your questions.

[The prepared statement of Mr. Johnson follows:]

FINAL

Statement of Jeh Charles Johnson
Before the Senate Select Committee on Intelligence
March 21, 2018

Chairman Burr, Vice Chairman Warner, and other members of this Committee:

I am pleased the Committee has convened this hearing on the important topic of election cybersecurity.

In 2016 the Russian government, at the direction of Vladimir Putin himself, orchestrated cyberattacks on our Nation for the purpose of influencing the election that year – plain and simple. The experience should be a wake-up call for our Nation, as it highlighted cyber vulnerabilities in our political process, and in our election infrastructure itself. Now, with the experience fresh in our minds and clear in our rear-view mirror, the key question for our leaders at the national and state level is this: what are we doing about it? The matter is all the more urgent given the public testimony of our Nation's intelligence chiefs last month, before this very Committee, that the Russians effort continues into the ongoing 2018 midterm election season.

From December 23, 2013 to January 20, 2017 I served as Secretary of Homeland Security. During that time, I had the privilege of working with Congress to provide additional authorities to the Department of Homeland Security ("DHS") to defend the Nation's and the federal government's cybersecurity, through the Cybersecurity Act of 2015,[1] the National Cybersecurity Protection Advancement Act,[2] the Federal Information Security Modernization Act of 2014,[3] and other new laws.[4]

But, there is more to do.

Cyberattacks of all manner and from multiple sources are going to get worse before they get better. In this realm and at this moment, those on offense have the upper hand. Whether it's cyber-criminals, hacktivists, or nation-state actors, those on offense are ingenious, tenacious, agile, and getting better all the time. Those on defense struggle to keep up. As in other matters of homeland security, we must mobilize our Nation in support of stronger cyber defenses.

The views I express here are my own, based upon my personal experiences in national security and, now, as a concerned private citizen. The factual testimony I offer here is based on my best recollection of events months past, without the opportunity to review internal government documents or classified material.

---

[1] Pub. L. No. 114-113, 129 Stat. 2935 (2015).
[2] Pub. L. No. 113-282, 128 Stat. 3066 (2014).
[3] Pub. L. No. 113-283, 128 Stat. 3073 (2014).
[4] *See also* the Border Patrol Agent Pay Reform Act of 2014, Pub. L. No. 113-277, 128 Stat. 2995 (including additional authorities for cybersecurity recruitment and retention).

Sometime in 2016 I became aware of a hack into systems of the Democratic National Committee. As 2016 progressed, my concerns about the potential of a cyberattack around our national election grew. At DHS, we developed a plan to engage state election officials to offer them our cybersecurity assistance.

My staff also suggested to me that I could, under my existing authorities, declare election infrastructure to be "critical infrastructure" in this country. There are 16 infrastructure sectors – *e.g.*, financial services, dams, transportation, government facilities, the defense industrial base – that are already considered critical infrastructure. By adding election infrastructure to that list, it would principally mean two things for cybersecurity purposes: (1) election officials, upon request, would be a top priority for the receipt of DHS's services, and (2) as part of critical infrastructure, election infrastructure would receive the benefit of various domestic and international cybersecurity protections.

On August 3, 2016, in an on-the-record session with reporters, I publicly floated the idea of designating election infrastructure in this country as critical infrastructure.

Twelve days later, on August 15, I convened a conference call with secretaries of state and other chief election officials of every state in the country. I told state officials that we must ensure the security and resilience of election infrastructure, and offered DHS's assistance to the states in doing that. I also reiterated the idea of designating election infrastructure as critical infrastructure.

To my disappointment, the reaction to a critical infrastructure designation, at least from those who spoke up, ranged from neutral to negative. Those who expressed negative views stated that running elections in this country was the sovereign and exclusive responsibility of the states, and they did not want federal intrusion, a federal takeover, or federal regulation of that process. This was a profound misunderstanding of what a critical infrastructure designation would mean, which I tried to clarify for them.

But, based on what I heard on the call, my team and I decided that a critical infrastructure designation at that time, during the election season, would be counterproductive. I remained convinced it was a good idea, but we put the idea on the back burner. Instead, and more importantly in the time left before the election, we encouraged the states to seek our cybersecurity help. Prior to the election, encouraging the horses to come to the water had to be the primary objective.

At around the same time we were engaging state election officials, my staff and I began to see and hear very troubling reports of scanning and probing activities around various state voter registration databases. This was obviously a matter of great concern. In the latter half of August, the FBI issued an alert to the states about these activities, which included the IP addresses of those associated with the attempted hacks.

Both publicly and privately, my staff and I repeatedly encouraged state and local election officials to seek our cybersecurity assistance.

On September 16, I issued one of a number of public statements encouraging state election officials to strengthen their cybersecurity, and describing the range of services DHS could provide. In that statement I also said the following:

> "*In recent months we have seen suspicious cyber intrusions involving political institutions and personal communications. We have also seen some efforts at cyber intrusion of voter registration data maintained in state election systems. We have confidence in the overall integrity of our electoral systems. It is diverse, subject to local control, and has many checks and balance[s] built in. Nevertheless, we must face the reality that cyber intrusions and attacks in this country are increasingly sophisticated, from a range of increasingly capable actors that include nation-states, cyber hacktivists, and criminals. In this environment, we must be vigilant.*"[5]

In September, President Obama personally asked congressional leaders to issue a bipartisan call to state election officials to seek DHS's cybersecurity assistance. Speaker Ryan, Leader Pelosi, and Senators McConnell and Reid did so, in a joint letter dated September 28.[6]

On October 1, I issued a public statement thanking the congressional leaders for their letter, and once again encouraged the states to seek our assistance. Here again I warned of the threat we were seeing to state voter election data:

> "*In recent months, malicious cyber actors have been scanning a large number of state systems, which could be a preamble to attempted intrusions. In a few cases, we have determined that malicious actors gained access to state voting-related systems. However, we are not aware at this time of any manipulation of data. We must remain vigilant and continue to address these challenges head on.*"[7]

Meanwhile, in the August-September timeframe, our intelligence community became increasingly convinced that the Russian government was behind the hacks of the DNC and other political institutions and figures.

I and others also became personally convinced that we needed to inform the American public, prior to the election, of what we knew the Russian government was doing. In the midst of the politically-charged election season, with accusations by one of the candidates that the election was going to be "rigged," attribution was going to be a big and unprecedented step, and required careful consideration. However, we recognized

---

[5] *See* https://www.dhs.gov/news/2016/09/16/statement-secretary-johnson-concerning-cybersecurity-nation%E2%80%99s-election-systems.

[6] *See* https://www.nased.org/Four_Leaders_on_Cybersecurity_and_Elections_9-28-16.pdf.

[7] *See* https://www.dhs.gov/news/2016/10/01/statement-secretary-johnson-about-election-systems-cybersecurity.

we had an overriding responsibility to inform the public that a powerful foreign state actor had covertly intervened in our democracy.

Therefore, on October 7, Director Clapper and I issued the statement formally and publicly accusing the Russian government of directing cyber "thefts and disclosures [that] are intended to interfere with the US election process."[8] In this statement, we also warned again that "[s]ome 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" (we were not then in a position to attribute this activity to the Russian government) and once again encouraged state election officials to seek DHS's assistance.

Three days later, on October 10, I issued another public statement encouraging states and other jurisdictions to seek our assistance in the 29 days before the election.[9]

By election day on November 8, a large number of state and local election officials did in fact respond to our offers of cybersecurity assistance. More specifically, almost every state contacted DHS about its services, and 33 states and 36 cities and counties used DHS tools to scan for potential vulnerabilities and/or sought mitigation advice from us. Overall, DHS proactively provided election-related mitigation advice and cyber threat indicators/information for network defense to likely hundreds, if not thousands, of state and local officials.

On election day, DHS assembled a crisis-response team to rapidly address any reported cyber intrusions into the election process.

To my current knowledge, the Russian government did not, through any cyber intrusion, alter ballots, ballot counts or reporting of election results. I am not in a position to know whether the successful Russian government-directed hacks of the DNC and elsewhere did in fact alter public opinion and thereby alter the outcome of the presidential election.

Following the election, and at the direction of President Obama, on December 29 the U.S. government took a number of steps in response to the Russian government's efforts to interfere with our election. These included (i) sanctions against various Russian intelligence services and officers and three companies, (ii) the expulsion from our country of 35 Russian government officials, and (iii) a joint report by DHS and the FBI providing details about the tools and infrastructure used by the Russian government to compromise networks associated with the election.

On January 6, 2017, and also at the direction of President Obama, the intelligence community released an unclassified public report, "Assessing Russian Activities and

---

[8] *See* https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

[9] *See* https://www.dhs.gov/news/2016/10/10/update-secretary-johnson-dhs-election-cybersecurity-services.

Intentions in Recent US Elections," to better educate the public about what had happened.[10]

Following the election, I returned to the issue of the designation of election infrastructure as critical infrastructure. Throughout the fall, my staff had continued the dialogue with state election officials about the designation. Following the election, my staff reported to me that state officials' stated views of the designation had not changed, and continued to be neutral to negative. On January 5, I had one more conference call with state election officials to be sure I understood their reservations. Notwithstanding what I heard, I had become convinced that designating election infrastructure as critical infrastructure was something we needed to do. The next day, on January 6, I issued a public statement announcing my determination that election infrastructure in this country should be designated as a subsector of the existing "Government Facilities" critical infrastructure sector.[11]

I am pleased that in 2017 then-Secretary Kelly reaffirmed that designation.

The 2018 midterm elections are now upon us. The first primaries in the 2020 presidential election are less than two years away. I am pleased that state election officials, to various degrees, now seem to be taking serious steps to fortify the cybersecurity of their election infrastructure, and that the Department of Homeland Security is currently taking serious steps to work with state and local election officials to strengthen their cybersecurity.

As a Nation, we must resolve to strengthen our cybersecurity generally, and the cybersecurity around election infrastructure specifically. Nothing less than the health and strength of our democracy depends on this.

I am prepared to discuss further my own views on this topic, and I look forward to your questions.

---

[10] *See* https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[11] *See* https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

Chairman BURR. Thank you, Secretary Johnson.

It seems more than normal issues recently coming before this committee are not the jurisdiction of the committee. And were it not for the investigation, elections would not be the jurisdiction of this committee. But given the nature of our investigation, we have developed a committee of somewhat experts now on elections and election relationships between the Federal Government and the State. And that's why we asked Senator Collins, Senator Lankford, Senator Harris, and Senator Heinrich to take the lead as it related to election security.

At this time, I would like to recognize Senator Collins for questions, followed by Heinrich, Lankford, and Harris.

Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman and again, let me thank you and the Vice Chairman for your strong bipartisan leadership of this investigation.

Secretary Johnson, let me begin by thanking you for your extensive public service, and I very much appreciate your being here.

In the summer and fall of 2016, DHS and the FBI issued several technical warnings about possible activities against State election systems. These warnings took the form of a flash report or a similarly technical bulletin, and generally, the warnings went to the IT staff of states and not to the chief election officials. I've read one of the FBI flash bulletins. It is extremely complex and it just refers to unknown actors scanning systems.

In retrospect, do you think that it would have been better had the FBI and DHS issued a more comprehensive warning that a nation-state was attempting hostile action against State election systems?

Mr. JOHNSON. Senator, let me respectfully disagree somewhat with your premise. I, in the fall, in August, September, October, issued five written statements to the public encouraging State election officials to come in and seek our cyber security assistance, over and above the technical messages that you cited, in mid-August, mid-September, October 1, October 7, October 10.

On October 1st specifically, I said: "In recent months malicious cyber actors have been scanning a large number of State systems, which could be a preamble to attempted intrusions. In a few cases we have determined that malicious actors gained access to State voting-related systems."

That's a pretty blunt statement, in my view. We weren't then in a position in our intelligence community to attribute it to the Russian government, nor were we on October 7th. We said it was coming from a Russian business, but we weren't then in a position to say it was the Russian government. We later said that, however.

But I can tell you that, in addition to these public statements, and in addition to the work of our people, we were beating the drum pretty hard, beginning with a conference call I had with every State secretary of state on August 15th. The good news is that by Election Day 33 states actually came in and sought our cyber security assistance, and 36 cities and counties came in and sought our cyber security assistance in the time permitted.

Very definitely, Senator, as we look back on the experience two years later and we have a much clearer picture of the full extent

of what the Russian government was doing, there could have been additional efforts made. But I'm satisfied that at the time this was a front-burner item for me and I was repeatedly making public statements warning State election officials about the threat we were facing as it was evolving.

Senator COLLINS. Secretary Nielsen, at this point, we know for certain that the Russians were relentless in their efforts and also that those efforts are ongoing. And yet, when I listen to your testimony I hear no sense of urgency to really get on top of this issue.

When we held our last hearing in June, I was dismayed to learn that not a single chief State election official had received a security clearance nearly eight months after the 2016 election. We already are in an election year. We've had the by-elections in Virginia and New Jersey; we've had special elections in Pennsylvania and Alabama; our Maine primary is in June.

What specifically is DHS doing to accommodate what you said was sponsoring three officials per State for clearances? That's 150 officials. How many have actually received the clearances, and what specific actions did you take in the elections that have already occurred?

Secretary NIELSEN. Yes, ma'am. Thank you for the question. Let me just first start by saying not only is this of extreme urgency to the Department, but, as you know, we're expending not only extraordinary resources to provide any support at the request of states, but we are prioritizing election efforts and risk and vulnerability assessments for our partners in State and locals over all other critical infrastructure sectors.

With respect to the security clearances, we've done two things. We've worked out a process with the inter-agency such that if we have intel we will read in the appropriate State election officials that day, so we're not waiting for clearances. If we have something to share, we will read them in and share it that day.

With respect to the clearances, we are doing our best to speed up the process. We've prioritized them, as I said, over other clearances for other sectors. We have about 20 that have received the full clearance. We're granting interim secret clearances as quickly as we can.

Senator COLLINS. Twenty out of 150?

Secretary NIELSEN. Yes, ma'am. And so we look—I've spoken with the Chairman and the Vice Chair just before. We certainly look forward to working with this committee government-wide on how we can speed up the security clearances.

But the good news, again, is if we have something to share we will share that day. With or without a clearance, we'll read them in and share it. So it won't limit our ability to get the information to them any longer.

Chairman BURR. Senator Heinrich.

Senator HEINRICH. Thank you, Chairman.

Secretary Nielsen, Secretary Johnson said in his testimony just now that he agreed with the committee's recommendations. Do you share that view?

Secretary NIELSEN. I do, yes. And as I said in my opening remarks, I look forward to working with you on implementing them.

As you know, some of them aren't DHS, so I will be happy to advocate and support efforts throughout government.

Senator HEINRICH. Thank you.

Secretary Johnson, I know hindsight is obviously 20/20, but looking back, knowing what you know now, what might have you done different or advocated differently in the run-up to the 2016 election?

Mr. JOHNSON. Well, the thing that I advocated for most strongly and that others, obviously including the President, agreed with was prior to the election we needed to inform the American people about what we saw. Some people say we should have done so sooner, but it was not an easy decision.

With the benefit of two years' hindsight, it does seem plain, given the testimony in this room last month, that the Russian effort has not been contained; it has not been deterred. In my experience, superpowers respond to sufficient deterrence and will not engage in behavior that is cost prohibitive. Plainly, that has not occurred and more needs to be done.

With the benefit of hindsight, the sanctions we issued in late December have not worked as an effective deterrent and it's now on the current Administration to add to those and follow through on those.

Senator HEINRICH. So do you think, for example, having a very clear, articulated cyber doctrine would be an important part of sending that message of deterrence?

Mr. JOHNSON. Yes, I agree with that. Yes.

Senator HEINRICH. Secretary Nielsen, are you concerned that over a year into this Administration and despite the urging of people on both sides of the aisle on multiple committees, that we still don't have a clear administrative doctrine that draws some—that says to the Russians or others that there will be consequences if you cross this line into our elections?

Secretary NIELSEN. I agree with your comments yesterday at the press conference, sir. As you know, we have an Executive Order 13800 that requires us to develop just that. Working with the intel community, I look forward to supporting their efforts.

It does need to be whole-of-government. As the Secretary is saying, we have sanctions, but we need to continue to look at diplomats, we need to look at indictments, we need to look at what we can do under OFAC. It needs to be very clear that there are consequences when countries meddle in our affairs.

Senator HEINRICH. I don't disagree that it needs to be whole-of-government, but one of my concerns is that no one's saying, "The buck stops here." We keep hearing "whole-of-government"; we heard it in our worldwide threats hearing recently. But, someone has to take the responsibility to make this happen.

How many Cabinet meetings have been focused on the whole-of-government strategy to make sure that in 2018 this doesn't happen again?

Secretary NIELSEN. We have had a number of them. We actually have a number coming up. But I take your point. I am a very strong advocate of making it very clear who has the lead within the Federal Government for this particular issue.

Senator HEINRICH. How important is it—you know, one of my concerns is that we won't be able to get State and local officials to take the Russian cyber threat or other cyber threats seriously unless they consistently hear from the highest levels of government that this is real, that their systems are truly at risk, that they need to prepare.

Director Nielsen, do you have the support you need from the White House to persuade those officials to take this seriously?

Secretary NIELSEN. I do, yes. And I think one of the lessons we've learned is to make sure that those messages go far and wide. So I've briefed the homeland security advisors; I've briefed governors, in addition to the State election officials and secretaries of state.

But to your point, within the states, because of our decentralized system, it's very important that everyone at senior levels understands the threat and is briefed in.

Senator HEINRICH. Would it help if the President were to simply acknowledge that this happened in 2016?

Secretary NIELSEN. Yes, sir. I think he has said that it's happened. What he's—the line that he's drawing is that no votes were changed. That doesn't mean there's not a threat. It doesn't mean we need to do more to prepare.

Senator HEINRICH. Secretary Johnson, in your view, how important is it for the President to articulate and acknowledge that this happened so that people take it seriously?

Mr. JOHNSON. Very. The President of the United States is the most visible American, maybe the most visible person on the planet, and the things he says and does are watched very, very closely, so I would agree with that.

Senator HEINRICH. Thank you, Chairman.

Chairman BURR. Senator Lankford.

Senator LANKFORD. Thank you both for the work that you have done to be able to support the Nation. I appreciate you both being here and both being on this panel together. I appreciate that very much.

The decentralization of our election systems is exceptionally important, and one of the key aspects that we've tried to work through on recommendations is maintaining the states' control of elections. Both of you have affirmed that.

Both of you have also affirmed the recommendations that we have put in place. I appreciate that.

We've worked with DHS; we've worked with secretaries of state around the country, to try to be able to pull these recommendations together to be able to do it, including streamlining the communications between DHS and each of the states, updating to voting equipment that can be, and voting systems that can be, audited after the fact to just get verifiable information in that system. So, we think that's exceptionally important.

Secretary Nielsen, can you affirm to me that there is no effort from the Federal Government right now to be able to federalize our elections, and that the focus is still on working with states to be able to support them and the work that they're doing to be able to run their elections?

Secretary NIELSEN. Absolutely.

Senator LANKFORD. Talk to me a little bit about, Secretary Nielsen, about the classifications and getting classified information to individual secretaries of state. This was a struggle in previous times, during that election time period, getting information out. What would make a difference now, having clearances for individuals in the states and being able to communicate with them? What can you give to them with clearance that you couldn't give to them without?

Secretary NIELSEN. It's a good question. We've done a lot of work on three related processes over the last year. One is to work with the intel community to declassify information. As you know, some of the information does not originate within DHS, so we need to work with our partners to be able to share it.

The second one is on victim notification. We have a role there, but so does FBI and so does MS–ISAC, which in this case the Multi-State Information Sharing and Analysis Center was in some cases the first organization to identify some of the targeting. So, we have to work with whomever originates the information. We all have different roles. So we've worked to pull it all together so that we can quickly notify victims of what has occurred.

With respect to your specific question, as I mentioned to Senator Collins, what we've done is we're widely using day read-ins now, so we're not going to let security clearances hold us up. If we have information State and locals need, we will provide it.

Senator LANKFORD. So, Secretary Johnson, you had some states give you push-back when you talked about things like making states critical infrastructure in their election systems and trying to be able to get that communication. You talked about an August 15th phone call that you had with secretaries of state to be able to talk to them.

Talk me through what happened in that August 15th phone call? Is that a normally scheduled phone call? Was there consistent communication? And the things that Secretary Nielsen's dealing with now and that two-way communication that's much needed and that trust relationship, some of the things that you faced as well trying to be able to maintain trust with State election officials?

Mr. JOHNSON. Incidentally, Senator, last year, last summer, I had the occasion to drive across country and return to Oklahoma City, to the memorial there.

Senator LANKFORD. And thanks for being there, again.

Mr. JOHNSON. So August 15th I was considering designating election infrastructure critical infrastructure, which the Secretary of Homeland Security has the authority to do. But I wanted to talk to State election officials about it first. I was, frankly, surprised and disappointed that there seemed to be a lot of misapprehension about what that would mean. I said to them a number of times that what it means is that we prioritize providing assistance to you if you ask. This is voluntary. It's not a Federal takeover; it's not a binding operational directive of any sort.

And the reaction I got was largely neutral to negative; and so the priority had to be getting the states to come to us to seek our cyber security assistance. So rather than just simply make that designation, which I saw was going to be controversial at the time, we put

it aside and encouraged them to come in. And most states actually did by Election Day.

After the election, I came back to this issue. A lot of them were still opposed, but I did it anyway so that DHS would prioritize providing cyber security assistance to the states.

And when we talk about cyber doctrine, one international cyber norm is that nation-states will not attack critical infrastructure, and so by making election infrastructure part of critical infrastructure they get the protection of the international cyber norm.

Senator LANKFORD. Thank you.

Chairman BURR. Senator Harris.

Senator HARRIS. Thank you.

Secretary Nielsen, at a roundtable 42 days ago at the Homeland Security Committee meeting I asked Deputy Secretary Duke and Undersecretary Krebs whether DHS is prioritizing risk and vulnerability assessments for the states. I didn't get a clear commitment that you are.

I'd also like to know, have you received the request that we made for a timetable for those assessments? Because we've not received a response to that request.

Secretary NIELSEN. Yes, ma'am. We are prioritizing. We have 19 that are State and localities that have either been completed or are in process. We continue to offer the assistance, but we have made the commitment and prioritized the resources that any State or locality that requests that, we will have it completed before the midterm election.

Senator HARRIS. Do you have a date for completion?

Secretary NIELSEN. Well, of the 19 I can get back to you, but those are the only ones who have requested so far.

Senator HARRIS. Can you commit to completing all these assessments by June 1st, which would be five months before the election?

Secretary NIELSEN. Depending on who requests. But I'm happy to work with you on timelines as soon as we get a request.

Senator HARRIS. And of the number you mentioned you said have been completed or in the process.

Secretary NIELSEN. Yes, that's correct.

Senator HARRIS. How many have been completed?

Secretary NIELSEN. To my knowledge, 15. If that's not correct, I'll ask Jeanette Manfra to correct me when she speaks.

Senator HARRIS. Okay, because you earlier said in the process of or have been completed.

Secretary NIELSEN. That's right. So I believe 15 have been completed. But again, she'll verify if I have that number wrong.

Senator HARRIS. Okay. Well, we heard from her yesterday and she said that 14 are in the process.

Secretary NIELSEN. Okay. That's 19 total.

Senator HARRIS. Can you follow up with how many have actually been completed?

Secretary NIELSEN. Sure. Sure.

It's also a little confusing because, of course, they're states and localities. So 19 is states and localities.

Senator HARRIS. Okay. My question concerns states. Thank you.

Secretary NIELSEN. Perfect.

Senator HARRIS. Is there a protocol for following up to ensure that the reforms that you recommend have actually been completed?

Secretary NIELSEN. We do continue to work with them through hygiene scanning and others.

Senator HARRIS. Is there a protocol to do that?

Secretary NIELSEN. That is the protocol that we offer. But again, it's all voluntary, so it's not a mandatory check.

Senator HARRIS. Okay. In the intelligence community there is a concept called "duty to warn." And, Secretary Johnson, I'd like to ask you—and essentially the concept is that, if a Federal agency learns that a person is at a risk of imminent harm or an entity is at risk, that they should be informed, and obviously without giving up critical information that we have in terms of sources and methods.

Do you believe in the future that the Department should have a duty to warn states if the Department of Homeland Security is informed that there are imminent cyber security threats to their election systems?

Mr. JOHNSON. Yes, absolutely.

Senator HARRIS. Secretary Nielsen, do you agree with that?

Secretary NIELSEN. Yes.

Senator HARRIS. Will you commit, then, to this committee that you will in fact warn those states when you become aware of imminent threat to their cyber security systems for elections?

Secretary NIELSEN. With the inter-agency, yes, ma'am.

Senator HARRIS. Okay. And when you learn of these threats, will you also commit to informing immediately congressional committees, and particularly the Intelligence Committee?

Secretary NIELSEN. As you know, we—we will work with you on that. As you know, the entire process is voluntary. What we find is when we notify others of who the victims are, unfortunately it has a chilling effect and we no longer get the information from those who have been attacked. So we'll continue to work with you on how to do that.

Senator HARRIS. So my question is will you commit to specifically informing the Senate Intelligence Committee when you become aware of those threats?

Secretary NIELSEN. We'll continue to work with you on the best protocols for that, yes.

Senator HARRIS. So the answer is yes?

Secretary NIELSEN. The answer is it's very difficult if a State does not want to be identified because it's a voluntary relationship. I don't want to do anything that would limit our ability to understand who is being attacked. So we'd have to work with the victim, just like we do in any other sector, and work with you to make sure that we do it in the right way.

Senator HARRIS. Would you commit to informing your oversight committee, which is the Homeland Security Committee of the United States Senate?

Secretary NIELSEN. I understand your question, and again we'll have to work with the victims. It's a voluntary system.

Senator HARRIS. You sit on the Principals Committee of the National Security Council, is that correct?

Secretary NIELSEN. I'm a member, yes.

Senator HARRIS. Okay. And that committee is comprised of Cabinet officials and is responsible for advising the President and coordinating policy on America's most serious national security challenges. Has the Principals Committee held a meeting focused on the security of the 2018 election?

Secretary NIELSEN. I myself hosted it, yes.

Senator HARRIS. And when did that meeting take place?

Secretary NIELSEN. A few weeks ago.

Senator HARRIS. And what decisions were made regarding election security?

Secretary NIELSEN. That State and locals remain in charge; that DHS needs to continue to expand our tool kit of what we can provide in support; that we need to work on tear lines, we need to work on victim notification, we need to work on clearances, and we need to work on communications to make sure that the public is aware of the threat.

Senator HARRIS. And did you indicate timelines and due dates for what should happen before the 2018 election?

Secretary NIELSEN. Well, clearly everything should be done before that, but yes, for each one of those we have an agreement on a path forward with a timeline.

Senator HARRIS. Will you provide that to this committee?

Secretary NIELSEN. Happy to.

Senator HARRIS. Thank you.

Chairman BURR. Thank you, Senator Harris.

The Chair would recognize himself, and then the Vice Chairman, and then members based upon seniority.

Secretary Johnson, I remember very clearly when you called a Gang of Eight meeting for the notification. And if I remember my timing right, I think Senator Reid actually might have had a brief the end of July because he happened to be in town. And when everybody got back, the 1st of September, you sat down with us and sort of presented us the scenario, and at that time talked about the critical infrastructure designation. It was followed some weeks after that by an all-members brief in the Senate; I'm sure it was in the House, as well.

And I think you alluded to the fact that that was not received by the states or election officials, the critical infrastructure designation.

In hindsight, for us knowing going forward, was that a mistake to even mention that? Did that taint the pool of their trust with us, with government, and maybe what the intent was on their part?

Mr. JOHNSON. Well, we put it aside; and I was very pleased with the level of participation that we got. I thought it was important—I thought that the critical infrastructure designation, frankly, is something we should have done years before. It made so much sense.

I think that the disadvantage we had with the timing was that it was in the midst of an election year and a rather heated election year. So I did put it aside, but then I, just before leaving office, came back to it because I thought it was something important to do.

But in answer to your question, Senator, I think that we were able to build, in the time permitted, a pretty constructive relationship with a lot of states, red states and blue states, that all came to DHS to seek our assistance in the election season.

Chairman BURR. I appreciate that. Even Secretary Nielsen's reluctance to be able to say, "I would definitely do it this way"—let me just say, in our hearings we've found that states do not want a critical infrastructure designation, that there's a red line there. And I think we've learned as this has gone on. We've seen it. It's visceral.

It's something that can be overcome with trust, and I think that's why as we produce benefits to the customer, which is any official or locality that has an election, then we gain a little bit more trust, we gain a little bit more ability to play a bigger role in the partnership, but not in taking over. I want to make it clear: Our recommendations do not intend or suggest that the government take over elections. It's not the Secretary or the Department's view of that, and it wasn't from the last Administration.

But that designation did affect their willingness to come in and ask for help and suggest where problems were that they saw.

Let me ask both of you. We'll start with you, Secretary Johnson. In 2016, were there any votes that were affected by this intrusion into any system in America?

Mr. JOHNSON. Not to my knowledge, sir.

Chairman BURR. Secretary Nielsen.

Secretary NIELSEN. We have no evidence that any votes were changed.

Chairman BURR. Secretary Nielsen, looking forward ahead to 2018, what is DHS's current estimation of the threat to our elections from Russia or any other hostile actor?

Secretary NIELSEN. Thank you for the question. I think, as you've noted, many of you in the press conference yesterday, unfortunately, once these vulnerabilities have been made clear, it's not just Russia that we have to worry about. These are vulnerabilities and attack vectors that any adversary could pursue. So we think the threat remains high. We think vigilance is important, and we think there is a lot that we all need to do at all levels of government before we have the midterm elections.

I will say our decentralized nature both makes it difficult to have a nationwide effect, but also makes it perhaps a greater threat at a local level. And of course, if it's a swing State or swing area that can in turn have a national effect.

So what we're looking at is everything from registration and validation of voters, so those are the databases, through to the casting and the tabulation of votes, through to the transmission, the election night reporting, and then, of course, the certification and auditing on the back end. All of those are potential vulnerabilities. All of those require different tools and different attention by State and locals.

The last thing I would just quickly mention is we all continue to work with State and locals to also help them look at physical security. They need to make sure that the locations where the voting machines are kept, as well as the tabulation areas; they need ac-

cess control and very traditional security like we would in other critical infrastructure areas.

Chairman BURR. I thank both of you.

Let me just say for the public's education, there's a clear distinction between what we're here to talk about today, which is the election process and how an outside actor could impact or influence that, versus, say, Russia's distinct campaign at societal chaos and their use of social media platforms. That's another area of investigation by this committee.

But this particular area is focused on the elections and the process of one vote and it counts and that there's accuracy in that count.

Vice Chairman.

Vice Chairman WARNER. Thank you, Mr. Chairman.

I want to follow up on some of the line of Senator Harris' question. And I'm sympathetic to the notion that you've got to have this collaborative relationship with the states, and I think the recommendations put forward by our members don't want to take over the Federal elections.

But for both of you, because we know this is such a serious problem, because we know the Russians are and potentially others are coming at this, I think it is critical that, even if you don't want to highlight this, someone needs to highlight those states or localities that perhaps choose not to participate or not to move to a paper trail.

You know, I have empathy for Secretary Johnson's notion of calling elections critical infrastructure. I think they are, but I get the notion of the pushback.

So how do we work through that? And I believe the public does have a right to know if their State or if their community basically is ignoring this problem. Briefly, from both, if you could?

Mr. JOHNSON. Senator, there's actually a role for the United States Senate to play in this.

Vice Chairman WARNER. We're trying.

Mr. JOHNSON. During 2016, if I had resistance from a State I would call one of you and say: "Would you please call your governor? Would you please call your secretary of state and tell them that they really need to come to us for assistance?" I did have that conversation with at least one Senator, I recall very distinctly, and I thought it was effective.

Vice Chairman WARNER. Secretary Nielsen.

Secretary NIELSEN. I agree. I would say that there are 33 states right now who have their voting systems certified by EAC. I think that's important. We should seek for all states to do that. There's 35 states that require it by law, so we'll continue to work with EAC on those voluntary voting system guidelines.

But DHS is also working on our own baseline that would be a much more comprehensive look at all of the cyber security aspects within the election process. We intend to provide that to you and we intend to ask states to meet it.

We have two states who aren't working with us as much as we would like right now. We're working through that. But yes, our intent would be to go to those congressional delegations and get some help from you.

Vice Chairman WARNER. I think it's very important, because I understand you've got to have a cooperative relationship, but I do think our constituents, our voters, need to know if a State or a jurisdiction is not stepping up.

Secretary NIELSEN. I agree.

Vice Chairman WARNER. We've talked a lot about the actual voting machines, and Senator Wyden may come to this issue when his time is up, but when you look at an overall State or locality's voter file, oftentimes those voter files are maintained by an outside vendor. Many of those outside vendors then collect all the information at a single point. So you may not have to go through simply the State system, but you could actually attack the vendors.

Could you address what we're doing to try to upgrade security at the vendor level?

Secretary NIELSEN. Sure. We're working with vendors on supply chain, so we have launched a voluntary supply chain initiative within DHS across all sectors, but also to help the vendors understand the part and parcel that comprises the machines that they sell, that they offer.

We also have a system or a program called Enhanced Cyber Security Services. It's a version of our EINSTEIN program, where we take classified indicators and we offer that through the private sector to vendors and states alike. We have six states taking us up on that and multiple vendors within the vendor community.

Vice Chairman WARNER. Well, I would make a request that, again similar to the states and localities, if there are vendors who are unwilling to cooperate or upgrade their security, I think it's critically important that this committee and other committees know so that perhaps we can bring pressure, as well.

I think that is an enormous vulnerability. We've looked at the systems, but I think the vendors who service those systems. And I hope, Secretary Johnson, you would agree with that.

Let me get to one other area. Our committee's investigation has been about election systems and security and how we can protect ourselves going forward. One area that we know where the Russians penetrated in 2016 was actually the campaigns, their ability to hack into the——

Secretary NIELSEN. Right.

Vice Chairman WARNER [continuing]. The DNC and release that information on a selective basis. Campaigns in many ways are the ultimate startups. They have very little security built in. This does not fit neatly into any governmental oversight, but do you have recommendations for us? The policy recommendations so far have been around systems, but should there be basic cyber hygiene guidelines for campaigns? And I'd like to hear from both of you on that topic.

Mr. JOHNSON. Yes, Senator, and the answer is yes. Campaigns are not immune from nation-state surveillance, nation-state hacking. I was very specific in not including political campaigns in the critical infrastructure designation because I didn't think it was appropriate. But, you know, you could go on with a long list of infrastructure that needs certain basic best practices, whether it's a political campaign, a utility, an academic institution. So I would agree with that, yes.

We've seen a number of instances where political campaigns, the e-mail systems of campaigns, have been hacked and data information has been stolen, going back years, as you know.

Vice Chairman WARNER. And recognizing it's voluntary.

Secretary Nielsen.

Secretary NIELSEN. I completely agree. We are offering a variety of services there, as well: the hygiene scanning, as you mentioned, as well as just basic redundancy planning.

Again, the issue here is that the information in the voter rolls, the databases, might be changed in some way, so having some way to audit that, to have redundancy, resiliency. We're working on planning with them and helping them understand best practices for just basic continuity of operations. But yes, you're hitting on another vulnerability that should be considered.

Chairman BURR. Senator Rubio.

Senator RUBIO. Thank you both, thank you both for being here. This is an important topic that I think is misunderstood. A lot of people focus on it as far as did they change the results of the election.

So I sat down last night and I thought to myself, you know, if you were to write, what's a hypothetical that could point to people how serious a problem this can become in the future? So here's a hypothetical scenario and I want you both to kind of opine whether that's something that could happen and whether I'm right in my assumptions, all right?

So let's assume for a moment that the year is 2020 or 2024 and there's a foreign leader who's tired of being lectured about democracy in their own country and they decide they want to create chaos in the United States and create doubts about our legitimacy. So he or she orders an operation against our presidential election. And now for the last five or six years this foreign power has identified ways to penetrate election officials at the State and the county level across America. There are so many of these that there's just this target-rich environment.

One of the things they've perfected over the years, for example, in this hypothetical, is the ability to inject misinformation into the bloodstream of the internet, and they watch as this misinformation spreads like a virus until a significant number of people believe it. They've also perfected, by the way, strategic leaking of altered or factual information, which the mainstream media picks up on and it fits perfectly into the red-versus-blue dynamic that plays out on cable news, making them unwitting agents.

So the plan of this foreign power in 2020 or 2024 in this hypothetical would not be to change the election results; it would be to create doubts about the validity of the election. And then spread those doubts using social media and media driven by red-versus-blue conflict, and ultimately call into question the legitimacy of a new President and potentially even trigger a constitutional crisis.

So what they do, is they penetrate the voter database of local election officials in strategically located counties or states. And then they use analytic information they may have gotten from who knows where to identify specific voters, or maybe just party registration, maybe the stolen data of a campaign with identified supporters. And they use that information to go into the database and

they change the addresses of individuals; thereby their precincts move around. Maybe they even delete some people from the rolls.

The result is that on Election Day we start getting reports about thousands of voters in different parts of the country who can't vote because when they show up they're not registered, they're not in the system. Or they show up and they're told that their voting place is halfway across town somewhere else.

Interestingly, a significant number of these voters who start complaining about this happen to be either of the same party or at least self-identified partisans of let's just call it Candidate A, and they live in a county or in a State that miraculously happens to be controlled by government officials of the opposite party.

So these reports start getting out there and suddenly, magically, a bunch of these names on social media start spreading all these reports about what's going on on Election Day.

Here's the other thing this foreign government's been able to figure out. This is all hypothetical. They've ultimately been able to mess with the system that kind of posts the results early, not the ultimate results, but just like unofficial results. And so that evening these results start coming up and, surprisingly, Candidate A is doing better than Candidate B, and people are surprised by it. But then the official results come back and it's a total reversal.

So what happens, as you can imagine, at that point is Candidate A refuses to concede. There's this all-out fight going on in American society. In the months to come millions of people march on Washington to try to force the Electoral College not to certify. The reverse millions come out the other side.

Come January, we don't even know if we can swear in a President. The military doesn't know who the commander-in-chief is. We're in an all-out constitutional crisis, total chaos. For the first time in 200-and-something years, the American republic is under duress from the inside out.

That sounds like something from a novel or a drama, a dramatic presentation in the movies. How far-fetched is this, given the capability of foreign adversaries? Is this not the central threat that faces us when it comes to elections and the integrity of our election systems? And the reason why I ask is not because anyone on this committee doubts it, but because we also have local, State officials across the country who do not have this perspective, this broader perspective. To them it's just about whether or not they could change the tallies. You don't have to change the tallies to create all-out chaos. Is that not the central threat here?

Mr. JOHNSON. Yes, Senator. I actually believe that the first half of your hypothetical was not a hypothetical. The second half of your hypothetical, insofar as votes, was my biggest concern in the fall of 2016 when we saw the scanning and probing around voter registration data, and that's a very real threat in my judgment.

The other point I'd like to make about your hypothetical: In the fall of 2016, prior to the election, I thought long and hard about where the single points of failure are that could create that scenario. And the thing that occurred to me was Associated Press. Associated Press for years has been the entity on which we rely to report State election results to the rest of the media.

So I actually picked up the phone and called the CEO of the Associated Press to go over with him to ensure that he had enough redundancies in their system if there was a failure on election night, and I was satisfied that they did. But it's something to also focus on.

But I think your hypothetical is a very good one and I think all Americans should be concerned about it.

Secretary NIELSEN. I agree. I think what you have highlighted are all the various parts at which we need to make sure that we are securing the system, because any one of those, as you say, can create that doubt, which in and of itself is perhaps what the adversary is trying to accomplish.

So from a DHS perspective moving forward, we're looking very carefully at how we can help entities at all of the places that you described protect their databases, as we saw in the summer of 2016 with the Structured Query Language, the SQL injections and attempts to manipulate the databases. We'll be scanning for that should someone take us up on our offer.

Provisional ballots become very important for the reasons you've described. States should plan for what happens on Election Day if a variety of voters appear and suddenly they're not on the rolls but believe that they should be.

We will have people in SOCs throughout the country. We will be stood-up 24/7 on any Election Day to provide immediate instant response should anything come up.

And then, as the secretary mentioned, on election night it's very important to work with AP and others before the election results are formally certified and audited, to ensure that there's not information that's put out.

So what I would suggest is that we all look at what you would call a hypothetical, but as the secretary rightly points out, is probably closer to a very good possibility, and walk through each of those and make sure that we are providing the tools and resources we need to State and locals so that they can prevent, identify, track, and then respond to any such issues.

Chairman BURR. Senator Rubio said "hypothetical," but if I hear he's doing a book tour we're going to all claim royalty off of it.

[Laughter.]

Chairman BURR. Senator Feinstein.

Senator FEINSTEIN. Thanks, Mr. Chairman.

I think Senator Rubio hit the nail on the head, and I'll tell you what surprises me. First of all, Secretary Johnson, it's great to have you back again. I enjoyed working with you, and so welcome.

Let me ask you this first question. I don't understand. You learned about this in August. You did a number of specific things. You spoke about the dates that you did these things. And yet the American people were never told. Why?

Mr. JOHNSON. Well, Senator, the American people were told.

Senator FEINSTEIN. Not sufficiently in any way, shape, or form to know that there was a major active measure going on, perhaps by a foreign power.

Mr. JOHNSON. On October 7, 2016, the Director of National Intelligence and I issued a pretty blunt statement saying that the Russian government was interfering in our political process, directed

by the highest levels of the Russian government. That was a pretty blunt statement. Some people believe we should have done that sooner.

Frankly, it did not get the attention that I thought it should have received. It was below-the-fold news the next day because of the release of the Access Hollywood video the same day and a number of other events. I was expecting follow-up from a lot of journalists and we never got that because everyone was focused on the campaign and that video and the debate that Sunday.

Senator FEINSTEIN. As I recall, I was Ranking and, as I also recall, Senator Burr and I and a couple of others had Mr. Brennan in—not Coats—well, it was Brennan, it was the head of the—it was Comey, and it was Clapper who laid it out to us. Now, this was highly secret.

Subsequently, it became known that there were 21 states that in fact had been pierced. But that information as to what states has not been released.

So when we first heard, it was highly secret, in a SCIF. We could say nothing about it. And even now, where I see no reason that 21 states can't be released as having been even possibly pierced by an active measure of a foreign country at this time, so those states would at least know that maybe they should take a look and do something about it.

If either of you can answer that—it's not in a question form, but I think you know where I'm going, because if we're told and it's all classified we can say nothing. If this is being done by the Administration to prevent it from being released, nobody can protect themselves.

Mr. JOHNSON. Senator, two things. First, as Secretary Nielsen pointed out, very often the victims of a cyber attack are extremely sensitive to the fact of a disclosure that they were the victims of a cyber attack, and that was true in this circumstance.

I also know and recall that in 2016, when we were working with the states, every State or every State owner of a system that had been targeted, was informed either by DHS or the FBI or through the MS–ISAC, the information-sharing organization.

Senator FEINSTEIN. But it was never made public, Mr. Johnson.

Ms. Nielsen, I don't understand why the same thing persists. I mean, this "victim" sort of appellation—America's the victim and America has to know what's wrong. And if there are states that have been attacked, America should know that. So this "victim" answer with me has no credibility at all.

Secretary NIELSEN. As you know, the 21 states themselves have been notified. But I take your point.

Senator FEINSTEIN. But the people have to know. If my State is notified, I better see that they do something about it. Everybody thinks, oh, it's some other State.

Secretary NIELSEN. Right, I understand. I look forward to reading your report and finding out what you heard from the states.

I think what I was trying to explain earlier is, unfortunately what we've seen in other sectors——

Senator FEINSTEIN. There was no report.

Secretary NIELSEN. The one that you're working on, I'm sorry, the report. I just look forward to reading it to see what you've—because I know you've talked to many of the states yourselves.

But what we've seen, unfortunately, throughout the last 15 years at DHS is, when it comes to this situation the victims stop reporting. When they stop reporting, we're just not aware of the attacks. Not only can we not help them, but we can't help other victims that are likely to be victimized in the near future based on the same vulnerabilities.

So we have to balance that. I really look forward to working with you on this. I take your point. We've got to find a way to encourage reporting and encourage cooperation while also making it transparent.

Senator FEINSTEIN. But I think states have to know that it's going to be known by the public if they don't. And if it's never made public, I'll bet you you have a bunch of states: Well, we've invested in this and we're not going to do anything about it now, and we'll see what happens in the future. I'll bet that happens in some places, and you're enabling it.

Secretary NIELSEN. Well, I think what we're doing at DHS is we'll come out with this. As I mentioned before, EAC has guidelines, but we're working on a baseline that's much more comprehensive. What we will do is not only tell states that that's our best recommendation at what they need to meet, but we'll be very transparent as to the states that don't meet it. So we will do that. From a preparedness side and a prevention standpoint, we will make clear what states need to do more.

But in terms of moving forward, yes, we need to work on this issue of the notification.

Chairman BURR. Senator Feinstein and I were faced with a similar task as it related to cyber security legislation. Do you make it mandatory reporting? Do you make it voluntary? If you make it voluntary, what latitude do you have to make public disclosures of who has turned in information?

And we decided with that legislation that voluntary was the best approach for cyber reporting and it was up to the companies then whether they wanted to make public acknowledgements. I think all of us know that the banking system is riddled with intrusions, but no financial institution in America wants to go out and that to be public. So we do have a predicament.

Senator FEINSTEIN. And that may change.

Chairman BURR. That may change.

The committee is committed to work with the Department of Homeland Security to continue to make our system better.

Senator Blunt.

Senator BLUNT. Thank you, Chairman.

Well, you know, we do know that the fabric of democracy is people's belief that what happened on Election Day was what actually happened, so securing those systems, important; securing the systems of registration, important.

Secretary Johnson, you mentioned, following Senator Rubio's great hypothetical of what clearly could happen, you said it's not hypothetical. Now, you didn't mean by that that this is what happened, did you?

Mr. JOHNSON. I thought that the first half of Senator Rubio's hypothetical, as I heard it, was real——

Senator BLUNT. You think that——

Mr. JOHNSON [continuing]. Insofar as the misinformation campaign that he described.

Senator BLUNT. I thought what you were talking about was the infiltration of the registration systems.

Mr. JOHNSON. No, no. That was my—that is hypothetical, but it was my biggest concern in 2016.

Senator BLUNT. Well, it is a concern. There's no doubt about that.

At the same time, we've never had an election where—let me see if I can find your quote, Secretary Nielsen—where a number of voters didn't appear on Election Day who were not on the voting rolls but thought they were. I was a State election official; I was a local election official. There is never an election where lots of people don't show up, particularly a presidential election, and they're sure they should be on the rolls——

Secretary NIELSEN. Right.

Senator BLUNT [continuing]. But often there are reasons that they're not on the rolls.

Most states that didn't have a provisional opportunity to cast a ballot before 2000 I think added one after 2000. So that voter almost always is allowed to cast their ballot. If this needs to be judged in some way, it's done after the election. Sometimes it's easily figured out. Sometimes it turns out that the voter has already voted somewhere else, or the voter lives in another county, or the voter lives in another State. But they get a chance in most states to cast that ballot even if they have—if there's a question about whether they're on the voter rolls.

I'm much more—I'm concerned about the voter rolls, concerned about the infiltration of the voter rolls. I'm much more concerned that we secure the counting systems. We're going to have another panel to talk about that, that the counting systems themselves be secure. I think it really is critical infrastructure.

Secretary Johnson, your August outreach to election officials, did you provide much information as to what it meant to become critical infrastructure? Or did they have any reason to really understand why you were making this suggestion of a great change of responsibility 90 days before the election?

Mr. JOHNSON. I went through with them in August in detail what a critical infrastructure designation would mean. And I explained essentially three things: that it prioritizes the assistance that we provide if they ask; it means for a certain greater level of confidential communications between DHS and the states; and it means that they would have the protection of the international cyber security norm. And I stressed at the time that this is all voluntary and it prioritizes assistance if they seek it.

Senator BLUNT. You know, we're going to have a secretary of state on the next panel who I think was on that call, and I don't believe that's their view of how that conversation went. But we'll see what their view is.

The other question when you brought this up before, what would the protection of the international norm be? We've had our Federal

personnel records have been—somebody has those. We have all kinds of financial information that's been out there. What good—what is the international norm supposed to provide here that it doesn't appear to provide anywhere else in terms of real protection?

Mr. JOHNSON. The international norm is that nation-states will not attack critical infrastructure. Now, obviously it's incumbent upon the victim State to then do something about it if their critical infrastructure is attacked. But the designation makes clear that we consider election infrastructure to be critical infrastructure like government, like our defense industry, like our financial services industry.

Senator BLUNT. Well, I don't disagree that it's critical infrastructure. I'm not sure I agree that calling it "critical infrastructure" provides much of a level of security right now.

My last question for this panel. Secretary Nielsen, you mentioned the Election Assistance Commission a couple of times. Do you have concerns that we're moving into an area here where that commission and your agency will not quite know where the—how do we define this in a way that creates the lines of responsibility so that somebody knows who is responsible and what they're responsible for?

Secretary NIELSEN. Yes. As you know, DHS is working very closely with EAC. We've created a Government Coordinating Council. EAC and DHS sit on that along with a variety of State and local election officials.

EAC certifies the systems. EAC has the voluntary voting system guidelines. We're working with them and NIST to update those. They need to be updated. We hope that the final draft will come out next month. We need to continue to work with them to expedite that so that we have a guideline that reflects the current threat.

But I would say I think the role between DHS and EAC is clear right now. It's just making sure that we're doing it in lockstep so that we're together providing the assistance that the states need.

Senator BLUNT. I may have some questions for the record on that topic.

Thank you, Mr. Chairman.

Chairman BURR. Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman.

Secretary Nielsen, Secretary Johnson, good to have both of you here.

I want to start by talking about the fact, 43 percent of American voters use voting machines that researchers have found have serious security flaws, including backdoors. These companies are accountable to no one. They won't answer basic questions about their cyber security practices, and the biggest companies won't answer any questions at all.

Five states have no paper trail, and that means there is no way to prove the numbers the voting machines put out are legitimate. So much for cyber security 101.

My question to you, for Secretary Nielsen, is: Does your agency have the authority to mandate basic cyber security in the electronic voting machines used in this country?

Secretary NIELSEN. No, sir.

Senator WYDEN. Does any agency?

Secretary NIELSEN. Not to my knowledge, not at the Federal level.

Senator WYDEN. Okay.

Now, Americans don't expect states, much less county officials, to fight America's wars. The Russians have attacked our election infrastructure. Leaving our defenses to states and local entities, in my view, is not an adequate response.

Our country needs baseline mandatory Federal election security standards, and what I'm talking about here are paper ballots and post-election risk-limiting audits. You and I have talked about this before, and I'd like to get your views for the record of whether you believe the continued use of paperless voting machines in this country threatens our national security and the Department is now prepared to recommend paper ballots.

Secretary NIELSEN. So yes, sir. If there is no way to audit the election, that is absolutely a national security concern.

So we're working with states. There's a variety of ways to do that. As you know, one is paper ballots. One is having a system itself that has a voter-verified paper audit. So in other words, you vote electronically, but the machine spits out almost like a ticker tape, what you voted and you have that for your record, and then we can also have it for a record. So it's a different way of doing it from paper ballots.

But yes, sir, we absolutely have to have a way to audit and be able to verify the integrity of the information of the votes.

Senator WYDEN. I think that sounds like a step in the right direction, because I was just stunned at the brazenness of these voting machine companies. I mean, the biggest one won't answer anything at all. And you've now told us that the status quo is a national security threat.

I just want to, before we wrap up, see if we can drill a little bit further into the question of whether you all are prepared to recommend that our country have paper ballots. I think you're almost there.

Secretary NIELSEN. We have said it's a best practice. We do recommend it. What we say is you must have a way to audit. You can do it through paper ballots or you can do it through this voter verification, but you must have a way to audit and verify the election results.

Senator WYDEN. Are you aware of the way we do it in Oregon and we've done it now for decades? We vote by mail. Everybody gets a paper ballot. There is an audit trail. We've done it for decades. It's been supported by Democrats and Republicans.

I'd like in 2020 every American to get a ballot in the mail. I think it is a national scandal, the security issues you've talked about and the idea that so many of our people wait in these lines only to be told they ought to go somewhere else.

What do you think of the Oregon system?

Secretary NIELSEN. So I'm not as familiar with it. I look forward to learning more about it. Some of the issues that, aside from this particular conversation, that have been raised with mail is just making sure that the person who's voting is who we think they are. So we do have to have a way to verify identity.

Senator WYDEN. We'll show you how to do it because we've done it——

Secretary NIELSEN. Happy to learn.

Senator WYDEN [continuing]. We've done it for two decades, and we basically say right on the envelope: "If you aren't the person that you say you are, you are in one heck of a bad way. You are going to face serious, serious penalties." And that's why it has worked and is supported on both sides of the aisle.

Thank you, Mr. Chairman.

Chairman BURR. Senator Cornyn.

Senator CORNYN. Thank you both for being here. I think it sends a very good message to see both of you sitting side by side and appearing to answer the committee's questions, and appreciate your service to the country.

I want to start, Secretary Nielsen, by thanking you for your comments about the bombings in Austin. When I talked to Chief Manley at the Austin Police Department the day before yesterday, he told me there were roughly 500 Federal authorities on the ground doing everything they could to identify the bomber.

And as we've learned today, he will not be doing that anymore. But it's important to remain vigilant, I think you also said, lest there be some other unexploded bombs out there that he might have planted.

I'd like to ask both of you to comment on this. My understanding of our adversaries, whether they be Russia or China, is they view the internet and cyber space far differently than we do. In other words, they view it as a domain for information warfare. They do not allow their citizens to use the internet for the purposes that we use it for, for commerce or for communication between friends and family, to share social media, pictures of grandkids, things like that. They use it as a weapon, and we don't.

It seems like we are just constantly playing defense. And while I know today the topic of the hearing has to do with our election systems, and there couldn't be anything more important in terms of securing those election systems, it does raise the question about what is America's national security cyber strategy?

I know we learned from the Department of Defense that they are late responding to a mandate in the Defense Authorization Act to respond in terms of their role. But clearly the Department of Homeland Security plays a very important role too, but you're not alone. There are other government agencies that are involved in this question.

So what do you think it's going to take, and what do you recommend for the United States government that we do to create an all-of-government strategy to deal with the cyber threat?

Maybe start with you, Secretary Johnson.

Mr. JOHNSON. Senator, I think that's a very good question and I think you have to look at several aspects of the problem. One, I think that when you're talking about a nation-state actor we have to create an environment of sufficient deterrence to that nation-state. All nation-states will not engage or will refrain from behavior if it's cost-prohibitive behavior, if they know it's cost-prohibitive.

The Department of Homeland Security has a role on defense in working with the public to harden our cyber security. I do think

that—and I think your question touches on this—our open society, our strength as an open society, is also our vulnerability, and we have to be somewhat careful in going down the road of having U.S. government agencies trying to regulate speech, trying to regulate political speech, political debate. As you know, they do that in other countries. We don't do that here.

So the information marketplace and its easy access is definitely a problem for our democracy, but I would hesitate for the U.S. government to go down the road of trying to regulate it in some way. There are matters of Federal election law, to be sure, things that violate Title 18, but I happen to believe that a lot of this has to depend upon self-regulation by internet service providers and social media providers.

Senator CORNYN. Secretary Nielsen, do you think we have a national security strategy?

Secretary NIELSEN. We do.

Senator CORNYN. When it comes to cyber?

Secretary NIELSEN. We do. But, having said that, the White House is working on an update to the national cyber security strategy. An update to DHS's strategy will nest within that.

But I also want to just take the opportunity to reaffirm what you said. I think there's two parts to this at least. There's the part we're talking about today, but then closely related to that is the malign foreign influence in general.

I agree with Secretary Johnson, we have to be very careful in that conversation about substance, but I think the real issue is who is providing that substance. The example that I've used before is: If I read something on the internet or social media, et cetera, and I believe that it's from 50 of my closest friends and neighbors, I might feel very differently if, in turn, I'm told that's from 50 machines in Russia.

So it's not so much the substance as it is perhaps Americans need more understanding of who is messaging and the intent behind the messaging. So that is something that the DOJ, FBI, and State Department are leading on, but I do think is a very important part of this conversation.

Senator CORNYN. If the Chairman will permit me just one last comment, I think what I also think about is some of the social media companies basically throttling or censoring the news. Since they've become a primary vehicle for people to learn what's happening in the world, if they then take that role of censors, what the implications of that might be. Something for us to think about and talk about maybe in the future.

Secretary NIELSEN. Yes, we need to be very, very careful.

Chairman BURR. Thank you, Senator Cornyn.

Secretary Nielsen, your staff has accommodated a slight change in your schedule, if it's okay with you, that we would go for—we've got two members that are here, maybe a third one that might come back for questions. We will finish by 11:15 if you're in agreement.

Secretary NIELSEN. Okay, yes, sir.

Chairman BURR. Thank you.

Senator.

Senator KING. Thank, Senator—or Mr. Chairman.

I spent about an hour yesterday afternoon reading the classified draft report of our committee on this subject. All along we've been talking about the Russians penetrating our systems and messing around with our elections. That's not sufficient. What I learned yesterday was horrifying. What we saw wasn't messing around or penetrating. It was a sophisticated, thorough, comprehensive, malign, and malicious attack on our electoral system.

What worries me is that, although the intelligence is uniform that no votes were changed, they weren't doing it for fun in 2016. What it looks like is a test, and it was incredibly, as I say, thorough and comprehensive.

I want to follow up on Senator Cornyn's question. We can patch software systems till the end of time and we're not going to defeat these people. The history of warfare is the history of the invention of new offensive weapons, and then eventually defensive weapons catch up.

We saw the advent of a serious offensive weapon in 2016 being used against us. All of the patches aren't going to work if we don't have a strategy of deterrence. And that's the point of the question that Senator Cornyn asked and Senator Heinrich asked, and we don't have that strategy. In 2016 we passed the National Defense Act. It had an amendment requiring the Secretary of Defense by last June to give us the elements of a national cyber strategy. It hasn't happened yet.

180 days from that report was supposed to be a report from the President. Of course, that hasn't happened yet because the first report hasn't happened.

This problem is not being treated with the urgency that it deserves, and a deterrent strategy—because the problem now is the Russians send in this whole operation into our election system, into our states, 21 states that we know of, and paid no price. And we've had testimony from admirals and generals and people in CYBERCOM, and they've said: "Yes, Senator, there's no price that will change their calculation."

And so, Secretary, I hope when you go back—and by the way, this was a failure of the prior Administration in my view, because we've known this for four or five years, that this was coming. So this isn't a partisan observation. But I hope you'll go back and join with DNI Coats and with Secretary Mattis and the President and make this the highest priority that we have.

This is, I believe, with the possible exception of North Korea's nuclear weapons, this is the most serious threat that our country faces today and we are not adequately dealing with it.

And please expunge from your lexicon the word "whole-of-government." Every time I hear that I think: That means none of government. I want to hear who's in charge and what they're going to do about that.

So, Secretary Nielsen, I think you're in a key position. And I hope you'll read this classified report because——

Secretary NIELSEN. I look forward to it.

Senator KING [continuing]. It will terrify you. And then, of course, this is just one aspect of this attack on us. So I believe this is an incredibly important area.

Now, let me ask a more specific question. You mentioned earlier—we talked about clearance of State officials and only 20 have been cleared. I hope that can be accelerated, because we've already had several primary elections and we're headed into many more this spring. Do you have plans to try to accelerate that clearance? Because communication won't work if you can't tell them.

Secretary NIELSEN. We do, yes, sir. It is a problem that is not unique, unfortunately, to this particular stakeholder set, so I do look forward in general——

Senator KING. No, you're right. 791,000 clearances that we're behind.

Secretary NIELSEN. I know.

But what we have done is we've worked out the processes whereby, if we have actionable information, we will provide it to the State and local officials on a day read-in. So we are not letting the lack of a clearance hold us back. We're in contact with them. If we have information to share with them with respect to a real threat, we will do so.

Senator KING. Let me make a modest suggestion, because we're going to have State officials here soon; we've had State officials before. The general reaction is—and I don't want to over-characterize it, but the general reaction is: We're doing a pretty good job; we're in good shape. I get the same thing in the Energy and Natural Resources Committee from utility executives: Don't worry; we've got it in hand. I don't believe that.

You have the capability—this is my modest suggestion: Create a red team in DHS, a group of really skillful hackers, and hack some of these states and show them how vulnerable they are. Because I don't think they're going to believe it until you show them what your people can do. And that may mean—this country has to wake up, and I just suggest that as a possible technique. You've got some skilled people you can work with, NSA or CYBERCOM, and develop a red team that will kind of shock people into the realization of how serious and how vulnerable they are. Would you consider that suggestion?

Secretary NIELSEN. We will consider it. We do try to currently get at that through our risk and vulnerability assessments. We have continued to encourage states to take us up on that. That is a comprehensive assessment we do on site. It includes pen testing; it includes wireless access; it includes database. So it gets at some of what you're saying.

But yes, sir. We need to help them understand where they've vulnerable, absolutely.

Senator KING. Well, I appreciate your leadership and really urge you to go back with your hair on fire.

Secretary NIELSEN. You have an advocate here.

Senator KING. This is an urgent matter.

Mr. Secretary, it's good to see you. Seeing you back reminds me of the old country song: "How Can I Miss You If You Don't Go Away?"

[Laughter.]

It's nice to see you, sir.

Thank you, Mr. Chairman.

Chairman BURR. Senator Risch.

Senator RISCH. I think that was meant as a compliment. You need to study the country songs genre a little more, Senator.

Look, we've all, you and everybody on this panel have looked at thousands of pages, and done the interviews, and reviewed everything there is.

A simple question I have for you. Right now, we pretty much know what happened and everybody's got an idea of what's happened. The question I have for you is: Are either one of you aware, or has it been suggested to either one of you, or have you seen any evidence of any kind that any U.S. person was involved in this scheme?

Ms. Nielsen.

Secretary NIELSEN. Not to my knowledge. No, sir.

Senator RISCH. Mr. Johnson.

Mr. JOHNSON. You have to—I'm sorry to be a lawyer here. Which scheme are you referring to?

Senator RISCH. I'm talking about the Russian scheme to do what they did as far as attempting to interfere in the elections, the kinds of things we've been talking about this morning, the attacks, the penetrations, and what have you.

Mr. JOHNSON. My recollection of the Special Counsel's indictment is that there were some U.S. citizens included in it. That's my recollection, but I could be wrong about that.

Senator RISCH. You want to follow up on that?

Secretary NIELSEN. Just I have no knowledge, if we're talking about the topic of this hearing, which is the hacking of elections, I have no knowledge that a U.S. citizen was involved in that.

Senator RISCH. Thank you very much.

Thank you, Mr. Chairman.

Chairman BURR. Senator Manchin.

Senator MANCHIN. Let me just follow up on that very quickly, if I may. Do you all, either one of you all, have any doubt whatsoever, from what your knowledge and talking to the intelligence communities, that the Russians were involved at a higher level than they've ever been involved before?

Secretary NIELSEN. I have no doubt.

Mr. JOHNSON. No, sir. No doubt.

Senator MANCHIN. Okay. And as a result of the Russians meddling in 2016, I'd fought to ensure the bill passed out of the Senate Appropriations Committee included a directive for DHS to provide technical assistance to State and local law enforcement to secure networks against cyber attacks. And before our committee this past year I was shocked to learn that multiple Federal agencies, including DHS, could not confirm that they did not have Kaspersky software in their system after we recognized the threat it posed to our national security.

So my question would be, if our own Federal Department of Homeland Security has trouble finding a reliable vendor and relates to a Russian vendor such as Kaspersky, wouldn't you think our cash-strapped states and local partners might have the same problems?

Secretary NIELSEN. The short answer to that is yes. As you know, we issued a binding operational directive to remove all such

products from Federal systems. We do not have authority to mandate that states do that, but we have taken it——

Senator MANCHIN. Have you removed Kaspersky from yours?

Secretary NIELSEN. Yes, sir, and we have taken it of the GSA catalogue, as you know, which would allow states to purchase it with Federal funds.

Mr. JOHNSON. I generally agree with what the Secretary said.

Senator MANCHIN. The other thing, Russia or any other country that has been found guilty of meddling in our elections, which I think that we have confirmed by all our intelligence communities, what punishment or what recommendations of punishment or sanctions would you all recommend that would be stringent enough to prohibit that from happening or any other country going down this path that Russia has gone down?

Secretary NIELSEN. Sir, I can just tell you I think it's a very important question because we have a multifaceted relationship with Russia. We still seek their cooperation when it comes to North Korea, Syria, Iran, for example. So, the consequences and what we do in reaction to their meddling in the election needs to be proportionate, but also needs to be driven in a way that they understand the specific behavior that we are seeking to avoid.

And as the Secretary said, you know, the hope in general is that the international community continues to recognize that affecting and attacking critical infrastructure of another nation is a red line. As an international community, we all need to hold each other to that and recognize that that is a red line.

So from a U.S. government perspective, we've looked at everything from sanctions back from the Obama Administration, to sanctions now, to the PNG'ing of diplomats, to indictments. We need to do more. We need to continue to make the point.

Senator MANCHIN. Well, let me expand on that. Should we treat a cyber attack or intrusion on our government, on our country, if sponsored or directed by a foreign government, which we know was, an act of war?

Secretary NIELSEN. We need to look at that very carefully. As you know, we have not made that decision as a country, either as a policy perspective or a congressional perspective. But I hope that we can work together and with other parts of the Administration and decide where is that red line.

Senator MANCHIN. Secretary Johnson, do you think that we have deterred Russia from continuing their operations as far as trying to infiltrate our election system for the 2018 election?

Mr. JOHNSON. No, we have not, based on the testimony in this room last month from our intelligence chiefs.

Senator MANCHIN. So we're facing the same, if not worse?

Mr. JOHNSON. Correct. Yes, sir.

Senator MANCHIN. Secretary Nielsen.

Secretary NIELSEN. Yes, there's no reason to believe they will not attempt again.

Senator MANCHIN. Well, if that's the case then we have a nuclear weapons retaliation policy; shouldn't we have a cyber retaliation policy?

Secretary NIELSEN. I think that's what some of the members have asked about. Yes, we have an Executive Order 13800 Mr.

King was mentioning and Mr. Heinrich, what we need to do in terms of being very specific with respect to our deterrence. You have an advocate here. I will go back to my colleagues and the President and make sure that we get that done very soon.

Senator MANCHIN. We're coming down to the wire on the election, as you all know.

Secretary NIELSEN. Agree.

Senator MANCHIN. The primary, most of our states have primaries very shortly, and November election coming up, and we're faced with the same. And our states don't have the wherewithal in order to deter this if they're hooked to the internet in any way, shape, or form.

Secretary NIELSEN. I'm happy to take that message back. As you know, DHS does not do offensive cyber——

Senator MANCHIN. Do you believe the Federal Government should be involved in helping secure the election process State by State?

Secretary NIELSEN. Oh, we are, yes, sir. We are. At their request, we're working State by State, locality by locality.

Senator MANCHIN. How much money do you all have targeted for this?

Secretary NIELSEN. We've asked for another $25 million specifically to help our own resources. But as I've mentioned earlier, we've prioritized these.

Senator MANCHIN. Do you all have a final recommendation on how you're advising the states to secure their system?

Secretary NIELSEN. Oh, yes. We have many, many, depending on all of those different parts that I mentioned earlier.

Senator MANCHIN. Have they spoken back to you about the money, they don't have the money to either meet the requirements or suggestions you've made?

Secretary NIELSEN. In some cases, yes, they have. Of course they have resource constraints. Some of the machines themselves are old, as you know.

Senator MANCHIN. But it's a concern for the 2018 election?

Secretary NIELSEN. Yes, sir.

Senator MANCHIN. Thank you.

Chairman BURR. Thanks, Senators.

Secretaries, we've come to the end of this hearing. And, Secretary Johnson, I'm not a lawyer, so I had to turn to our counsel. Of the four individuals that have been indicted by the Special Counsel, two were on lying to the FBI; the other two was a mix of bank fraud, wire fraud, mail fraud. So no individual that's been indicted by the Special Counsel.

The other indictments—the other charges were directly at the IRA, the Russian facility that carried out. So if that helps to clarify your memory.

And let me say to Senator Manchin that it's my understanding that the appropriators have taken care of, in the omnibus bill, an amount of money to be grants and other items—I don't want to speak for what their language is going to be—that mirrors the research that this committee did.

And I want to thank Shelley Moore Capito, who chairs that Appropriations Committee, for working with our staff, and hopefully

I've made a commitment to Secretary Nielsen that we would be more than open to address any other needs as we see those as we move up to 2018 or to 2020.

I want to thank both of you for your testimony today and your willingness to appear together. Everybody's said something about it and I think it sends a strong message that the integrity of our election system is not a partisan issue and it's truly the heart of the strength of our democracy.

The committee's investigation found ample evidence to agree with DHS's assessment in 2016 that Russian government actors scanned an estimated 21 states and attempted to gain access to a handful of those. In at least one case, they were successful in penetrating a voter registration database. We've heard our witnesses confirm that assessment today. Despite that activity, I need to reiterate that the committee found no evidence of any vote totals that were changed, a finding that was confirmed by our witnesses also today.

The committee also discovered that Russian activities directed at the states fell in a seam of our national intelligence infrastructure. It was a foreign activity, but carried out on the United States inside the United States, where our intelligence agencies have limited authorities. And I can't stress that enough, that we've got to consider that as we go forward.

The intelligence community was therefore almost entirely dependent on the states for the insight into these activities. The committee found that DHS and FBI alerted states to the threat in the summer and fall of 2016, but in a limited way.

Our witnesses today confirm that they provided warnings to state IT staff, but notifications to election officials were delayed nearly a year. States therefore understood that there was a cyber threat, but not the seriousness of the scope of that threat.

This committee intends, hopefully before the end of the week, to produce an overview of our report that's sanitized, that can be released. The committee's full findings and recommendations on election security will be reviewed for declassification and possible redaction and, when that is complete, released to the American people so that they can make their own judgments about involvement and attempts to intrude into our system.

Once again, I want to thank both of you for being here. I want to conclude our first panel. A two-minute break as we bring the second panel up.

[Pause.]

Chairman BURR. I'd like to welcome our second panel here today and I'll say to each of you, thank you for your willingness on a snowy day to either come to Washington, because I know some of you made the trip or to travel through this town that sometimes understands snow removal, sometimes doesn't. So it's always a crapshoot.

Our second panel is comprised of: Jeanette Manfra; National Protection and Programs Directorate, Assistance Secretary for the Office of Cyber Security and Communications at the Department of Homeland Security. The only thing that's changed is "Acting" is no longer in front of that, and I'm glad for that.

Jim Condos, President-elect of the National Association of Secretaries of States and Vermont Secretary of State. Jim, thanks for bringing this weather today.

Amy Cohen, Executive Director of the National Association of State Elections Directors.

And Eric Rosenbach, Co-Director of the Harvard Kennedy School Belfer Center for Science and International Affairs.

I might add for the record that we also invited a representative of the Federal Bureau of Investigation to participate in today's hearing, but the committee's request was declined.

You are the experts on cyber security and elections. And while we just received the big picture assessment, and we're going to rely on you to provide us a great deal more fidelity. Jeanette, I'd like you to provide some details on the services DHS is providing to states and local election officials and what additional resources DHS may need to provide these services comprehensively.

Jim and Amy, I hope you'll provide a candid view from the states and from those on the ground who actually run elections. It's critical that we hear what states really need and whether all of this help from D.C. is proving to be valuable.

Eric, the Belfer Center has done an in-depth look at states' cyber security posture and has run table-top exercises with election officials. And I look forward, very forward, to hearing your outside assessment of how the partnership between DHS and the states is working.

In the interest of time, I'll end my remarks and go straight to the Vice Chairman. But when I recognize you, we will go Manfra, Condos, Cohen, and Rosenbach.

Vice Chairman WARNER. Well, thank you, Mr. Chairman. I just want to make two brief remarks. I think the first panel was very good, but I understand this is a collaborative relationship with the states and localities.

But I do think, as Senator King has mentioned and I mentioned in terms of my State, there are enormous vulnerabilities. Based on the Hackathon of last summer, I made sure in Virginia that we took out voting machines that didn't have auditable paper trails. So, recognizing the collaboration particularly between the State and DHS—I'd love to have all your comments on this—how do we make sure that we appropriately noodge or perhaps we as policymakers, we have to call out states and localities who don't participate, who don't upgrade their systems, who don't realize the seriousness of this problem. Not in the way that will fracture the relationship between DHS and the states, but leave that perhaps to us or others.

I'd also like to hear your comments on—we focused a lot on the states and localities itself. But there are clearly a whole host of vendors who manage voter files, who provide the equipment. How do we make sure, again, they are actually using best practices; and those that are not, that the states and localities who might hire those vendors are notified that they are not meeting standards of security that are appropriate?

So those are the kind of questions I'm going to hope to drill down on. Thank you, Mr. Chairman. I look forward to your testimony, everybody.

Chairman BURR. Thank you, Vice Chairman.

Jeanette, the floor is yours.

STATEMENT OF JEANETTE MANFRA, ASSISTANT SECRETARY, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, OFFICE OF CYBER SECURITY AND COMMUNICATIONS, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. MANFRA. Thank you, sir. Chairman Burr, Vice Chairman Warner and members of the committee: Thank you for today's opportunity to testify, on this lovely D.C. spring day, regarding our ongoing efforts to assist with reducing and mitigating risks to election infrastructure.

Before I discuss elections, however, I want to take a moment to thank Congress, Chairman McCaul and Ranking Member Thompson of the House Homeland Committee, Chairman Johnson and Ranking Member McCaskill, the Senate Homeland Security and Government Affairs Committee, and this committee in particular, for your long and continued support and legislation in granting DHS the authorities that we need to not only secure the integrity of our elections, but also to do our job in protecting Federal networks and critical infrastructure.

These efforts highlight the importance of the creation of the Cyber Security and Infrastructure Security Agency, at DHS, which would see our organization, the National Protection and Programs Directorate, become a new agency under DHS. This change reflects the important work we carry out every day on behalf of the American people to safeguard and secure our critical infrastructure. Again, we strongly support this much-needed effort and we appreciate Congress' action and look forward to becoming the Cyber Security Infrastructure Security Agency.

Though I was appointed to this position in July of last year, I have spent the last decade of my career after leaving the Army to advance the Department's cyber security mission within the Department of Homeland Security. During my time at DHS, I have personally witnessed the commitment, dedication and tireless efforts of the men and women to secure Federal networks, critical infrastructure systems and most recently our election systems.

During the 2016 elections, the Department used every resource based off of the information that we had to ensure that election officials were receiving the information we could provide them and the services we could provide them to secure their infrastructure.

As cyber threats continue to evolve in times of calm and in times of crisis, our network defenders at DHS will never waiver in their duty to protect the homeland. And I'm honored to have the privilege of leading that organization today. I would like to publicly thank them for their service and their excellence, and I look forward to continuing to lead and serve alongside them.

Since I last appeared before this committee, the National Protection and Programs Directorate at DHS has continued to lead an inter-agency effort to provide voluntary assistance to State and local officials. This inter-agency assistance brings together the Election Assistance Commission, the FBI, the intelligence community, NIST, other DHS partners and is modeled on our work with other critical infrastructure sectors. Importantly, it also depends on

our partnership with the representatives on the panel, whether that's from academia, the National Association of Secretaries of State, or the National Association of State Election Directors.

Since 2016, we have learned much from our State and local partners; and in the efforts we undertook to assist them in 2016, we've worked to refine and improve our partnerships and our services. Securing the Nation's election systems is a complex challenge and a shared responsibility. There's no one size fits all solution. Our Nation's election systems are managed by State and local governments in thousands of jurisdictions across the country and they must remain that way.

State and local officials have already been working individually and collectively to reduce risks and ensure the integrity of the elections they're responsible for running. As threat actors become increasingly sophisticated, DHS sands in partnership to support the efforts of these officials.

Through these collective efforts, we've made significant progress by creating government and private sector councils who collaboratively work to share information, promote best practices, and develop strategies to reduce risks to the Nation's election system. The recently formed Election Infrastructure Information Sharing and Analysis Center, facilitates the sharing of near-real-time information about potential cyber incidents. Additionally, 38 states are receiving feeds of actionable cyber threat indicators provided by the Department.

We are sponsoring up to three election officials in each State for security clearances. And while not all of them have submitted the paperwork, we have been able to grant security clearances to 21 individuals in 19 states.

We have increased the availability of free technical assistance by reprioritizing resources that were previously dedicated to securing Federal networks to the priority of securing election infrastructure. And we will continue to offer those services, whether those are cyber security assessments, red teaming, intrusion detection capabilities, information sharing, incident response, or training and career development free of charge to all State and local officials.

We will continue to collaborate, coordinate and support State and local officials to secure our election infrastructure for the 2018 primary, special, and general elections. Cyber actors can come from anywhere, internationally or within the U.S. borders.

We are committed to ensuring a coordinated response from DHS and its Federal partners to plan for, prepare for, and mitigate risk to any threat to our critical infrastructure. We understand that working with the election stakeholders is essential to ensuring a more secure election.

Our voting infrastructure is diverse, subject to local control and has many checks and balances. As we work collectively to address these and other challenges, the Department will continue to work with Congress and industry experts to support our State and local partners.

I look forward to further outlining our efforts to help enhance the security of elections which are administered by our State and local partners. Thank you and I look forward to your questions.

Chairman BURR. Thank you very much.

Jim, the floor is yours.

STATEMENT OF JIM CONDOS, VERMONT SECRETARY OF STATE

Mr. CONDOS. Thank you. First, I'd like to just say thank you for this warm welcome with the weather outside. It makes me feel right at home. And just to give you a perspective, it was minus 11 on the first day of spring in Vermont.

Chairman BURR. When your flight is canceled, I hope you'll hold us equally as——

Mr. CONDOS. I don't have a flight now until tomorrow night.

Good morning, Chairman Burr, Vice Chairman Warner, and distinguished members of the committee. Thank you for this opportunity to appear before you representing the Nation's secretaries of state, 40 of whom serve as chief State election officials in their respective states.

My name is Jim Condos and I am the Vermont Secretary of State. I am also President-elect of the non-partisan National Association of Secretaries of State and a member of the Department of Homeland Security's new Election Infrastructure Government Coordinating Council. That's a mouthful.

NASS President Connie Lawson of Indiana was not able to be here today, but I want to acknowledge her outstanding leadership in leading our organization. Our organization is comprised of members with strong and very diverse opinions. But when we speak for NASS, we speak with one voice.

Voting is the very core of our democracy. We are in the 2018 election cycle, with November's general election only eight months away. I want to assure you and all Americans that election officials across the states, across the country, are taking cyber security very seriously. While it is important to ask what really happened in 2016 and learn from it, we believe it is even more important for us to be discussing what lies ahead.

The 21 states that were not notified until September of 2017, one year after the supposed scans. No votes were changed, as you have heard. But let me be clear. Secretaries of state across this Nation are diligently working each day to safeguard the elections process.

When former DHS Secretary Jeh Johnson announced the "critical infrastructure" designation for election systems in January of 2017, our members raised many questions and expressed serious concerns about potential Federal overreach into the administration of elections. With the "critical infrastructure" designation in place, we are focused on improving communications between the states and with DHS to achieve our shared goal of election security.

Under DHS Secretary Kirstjen Nielsen's leadership, we are now working well together. NASS is committed to facilitating this relationship. State and local autonomy over elections is our best asset against cyber attacks. Our decentralized, low-connectivity electoral process is inherently designed to withstand and deter threats.

States use many resources available to them to bolster cyber security. Some utilize resources provided by DHS, others use private sector security companies, and still others partner with colleges and universities.

Mr. Chairman, in your press conference yesterday you and other Senators outlined cyber security recommendations. I would like to highlight that states are already implementing many, if not all, of the committee's recommendations, including in my own home state.

In Vermont—and let me go to my Vermont home State—we completed a thorough review of our cyber posture back in 2014, and we completed both physical and cyber. In 2015, we implemented a new election management platform. Because the system was new and it was nearly designed, it included built-in cyber risk assessments.

Some of the acknowledged best practices that we use in Vermont are: paper ballots, post-election audits, no internet connection of our vote tabulators, daily backup of our voter registration database, daily monitoring of traffic to our site, blacklisting of known problem or suspected IP addresses, additional penetration testing.

We also have same-day voter registration and automatic voter registration. And we are planning, we're in the process of planning a statewide cyber security forum to be held in our State.

We have no less than three levels of security between the outside internet and our cyber systems and they're monitored on a daily basis. We have joined the Multi-State Information Sharing Analysis Center, better known as MS–ISAC. We receive weekly DHS cyber hygiene scans, and we have met with both DHS and FBI contacts. We have also recently ordered an Einstein monitor to attach to our systems to help us monitor.

Secretaries and their staffs are also working to secure more funding for improved cyber security, new voting machines, and to strengthen our existing election systems. These efforts have become much more challenging as election officials have to work now to counter cyber security in addition to our election's administration.

To ensure the integrity of our systems, my colleagues and I do have a prepared ask for you. One of the most critical resources that Congress could provide to the states, is the remaining $396 million from the Help America Vote Act of 2002. It was allocated, but never completely appropriated. Meeting the ongoing demands for updated equipment and ongoing cyber security upgrades requires funding that the states simply do not have within their own budgets.

I must say, the new and immediate funds are absolutely critical as we are now only eight months away from the November general election. If we do not receive this money until August, it's too late for this year. We need the money now.

As election officials work to fulfil this commitment and to improve voter confidence, we ask Congress to fulfil that commitment. We ask that Congress, DHS and others help us improve America's confidence in our election systems by promoting State and local efforts in providing clear, accurate risk assessment.

I want to again thank the members of this committee for holding this hearing and giving me this opportunity to speak to you on this important matter. On behalf of NASS, I look forward to answering your questions.

[The prepared statement of Mr. Condos follows:]

Statement from the

Honorable Jim Condos

Vermont Secretary of State

President-elect, National Association of Secretaries of State

Member, Election Infrastructure Government Coordinating Council (EIS-GCC)

Before the U.S. Senate Select Committee on Intelligence

Open Hearing: Election Security

March 21, 2018
Washington, D.C.

National Association of Secretaries of State
444 North Capitol Street, NW – Suite 401
Washington, D.C. 20001
202-624-3525 Phone/202-624-3527 Fax
www.nass.org

Hon. Jim Condos, Vermont Secretary of State
Statement Before the U.S. Senate Select
Committee on Intelligence
March 21, 2018 | Washington, D.C.

Thank you for the chance to appear before you today to represent the nation's Secretaries of State, 40 of whom serve as the chief state election official in their respective states.

My name is Jim Condos, and I am the Vermont Secretary of State. I am also president-elect of the nonpartisan National Association of Secretaries of State (NASS), and a member of the Department of Homeland Security's (DHS) new Election Infrastructure Government Coordinating Council (EIS-GCC).

NASS President Connie Lawson of Indiana was not able to be here today, but I want to acknowledge her outstanding leadership. Our organization is comprised of members with strong and often differing opinions, but when we speak for NASS, we speak with one voice.

It is an honor to be here with my fellow panelists to discuss what states are doing to secure state and locally-run elections from cyber threats. We are in the 2018 election cycle with November's General Election only eight months away. I want to assure you – and all Americans – that election officials across the U.S. are taking cybersecurity very seriously. While it is important to ask what really happened in the 2016 cycle and learn from it, we believe it is even more important for us to be discussing what lies just ahead.

As you know, DHS reported to this committee in June 2017 that 21 states were targeted during the 2016 election cycle. The 21 states were then notified by DHS in September 2017. Of the 21 states, NASS is aware of only one actual breach – a breach of a state voter registration system. **No votes were changed.** It is also important to note that **all 50 states consider their election systems a target**. Secretaries of State across the nation are diligently working each day to safeguard the elections process with their own IT teams, private sector security companies, the federal government, and other partner organizations.

I. CRITICAL INFRASTRUCTURE DESIGNATION AND STATE AND LOCAL ELECTION CYBERSECURITY EFFORTS

When former DHS Secretary Jeh Johnson announced the "critical infrastructure" designation for election systems in January 2017, our members raised many questions and expressed serious concerns about the potential federal overreach into the administration of elections – a state and local government responsibility.

While NASS members remain concerned with potential federal overreach, we understand that the "critical infrastructure" designation is in place. Therefore, we are focused on improving communication between the states and with DHS to achieve our shared goal of election security. We believe that federal agencies have more information and resources to share and help mitigate cyber threats.

Under the leadership of DHS Secretary Kirstjen Nielsen, we are working together to correct incident notification procedures, receive security clearances, and utilize new federal resources available to the states. NASS is committed to facilitating this relationship.

State and local autonomy over elections is our best asset against cyberattacks. Our decentralized, low-connectivity electoral process is inherently designed to withstand and deter threats.

Ensuring the integrity of the voting process is central to our role as chief elections officials. We work every day to improve our cyber preparedness and contingency planning, and to provide administrative and technical support for local election officials. The processes and procedures surrounding our election systems incorporate both cybersecurity and physical security. For example, while cyber defenses are employed for digital systems, secure storage facilities for equipment such as voting machines and electronic poll books are vitally important as well.

States use many resources available to them to bolster cybersecurity. Some utilize resources provided by DHS, such as cyber-hygiene scans, risk and vulnerability assessments, penetration testing and consulting. Others use the private sector security companies for these services; and still others partner with colleges and universities.

States have and are implementing cybersecurity best practices developed for their own state systems, but have also taken advantage of broader cyber best practices and incident response plans developed by civic-minded organizations like Harvard's Belfer Center, the Center for Internet Security, and numerous federal agencies. These tools include checklists for cyber practices, table top exercises and sample incident response plans. These organizations also convene forums throughout the year for state officials to share experiences and discuss challenges.

In Vermont we began a thorough review of our cyber posture in 2013, when we issued an RFP for both physical and cybersecurity risk assessments which was completed in 2014. In the fall of 2015, we completed implementation of a new election management platform providing for our election night reporting, voter registration, overseas and military voting, etc. Because this system was new, it included built-in cyber security risk measures.

Some of the acknowledged "best practices" that Vermont uses include:

- Paper ballots
- Post-election audits
- No internet (Wi-Fi or hard-wire) connection of our vote tabulators
- Daily backup of our voter registration database
- Same day voter registration
- Automatic voter registration
- Daily monitoring of traffic to our site
- Blacklisting of known problem or suspected IP addresses
- Additional penetration testing

We have no less than three firewalls between the outside internet and our cyber systems as well as:

- Joining the Multi-State – Information Sharing Analysis Center (MS-ISAC),
- Receiving weekly DHS cyber-hygiene scans,
- Having met with both DHS and FBI Contacts

I would be glad to elaborate during the question and answer portion of this hearing or anytime in the future.

As a result of the "critical infrastructure" designation, an Election Infrastructure Government Coordinating Council (EIS-GCC) was established to improve communications between state and local officials and the federal government and to share resources. The EIS-GCC is comprised of 29 members, of which 24 are state and local election officials. **This is the first group of its kind** and helps us stay on the same page and share vital information. Through the EIS-GCC, a number of states have participated in a pilot program to share election-specific threat indicators. Additionally, a full Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) will be operational by May 2018. States will have the option to put monitors on their election-networks to track traffic, detect anomalies and share with other states.

Secretaries and their staffs are also working with their legislatures to try and secure more funding for improved cybersecurity, new voting machines and to strengthen existing election systems. These efforts have become more challenging as election officials work to counter cybersecurity threats to election systems.

II. FEDERAL FUNDS TO FURTHER AID STATES IN BOLSTERING ELECTION CYBERSECURITY

Presuming that the members of this committee want to know how Congress can assist state and local officials in ensuring the integrity of our election systems, my colleagues and I have a prepared "ask." **One of the most critical resources that Congress could provide to the states is the remaining $396 million in Help America Vote Act of 2002 (HAVA) funds.**

NASS and its members have repeatedly called on Congress to appropriate these previously-approved funds so that states could conduct the necessary work to implement additional cybersecurity protections and begin to purchase new voting systems. Every state in the country would benefit. Timing is absolutely critical as we are only eight months from the November General Election.

HAVA was the first piece of federal legislation to provide funding for election administration improvements, and states used the opportunity to enhance the security, accessibility, accuracy and reliability of election systems. Implementation of HAVA was a success, and it helped improve the voting experience for all Americans over the last 15 years.

Our existing election infrastructure is aging and election officials are increasingly required to modernize

and innovate in order to ensure that elections continue to be administered in a secure and efficient manner. Meeting the ongoing demands for updated equipment and ongoing cybersecurity upgrades requires funding that the states simply do not have within their own budgets.

Providing the remaining funding under HAVA will not solve all of the challenges election officials face, but it will help states enhance the efficiency and security of elections, including the purchase of new voting systems, the implementation of additional cybersecurity tools, and the hiring of additional IT professionals.

Election officials make every effort to ensure elections are administered in a secure manner, whether it is protecting voter registration data from cybersecurity threats or making sure that the votes cast are protected from tampering or manipulation. As election officials work to fulfill this commitment and to improve voter confidence, we ask Congress to fulfill its commitment to states by fully funding HAVA.

III. THE 2018 ELECTION CYCLE AND RESTORING VOTER CONFIDENCE

Safeguarding the integrity of our elections process will require the ongoing commitment and vigilance of the federal, state and local governments and our public and private partner institutions. We must collaboratively work to guarantee secure elections, thus restoring voter confidence in our systems and in our democracy.

We ask that Congress, DHS and others such as the Election Assistance Commission, help us rebuild America's confidence in our election systems by promoting state and local efforts and providing clear, accurate risk assessments.

In conclusion, there is no doubt that more can – and WILL – be done to bolster resources, security protocols, and technical support for state and local election officials heading into future elections.

I want to again thank the Members of this Committee for holding this hearing and giving me the opportunity to speak about this important matter on behalf of NASS.

I look forward to answering any questions you may have for me.

Chairman BURR. Jim, thank you very much. I'm not going to speak for the Appropriations Committee and I haven't read the omnibus bill. But there is a sizable chunk of money. It matches about what you're mentioning.

Mr. CONDOS. We appreciate that.

Chairman BURR. Where that goes, I'll leave that up to the instructions of the appropriators. But I feel fairly confident that the committee, the appropriators and DHS are all on the same page on this one.

Amy, the floor is yours.

STATEMENT OF AMY COHEN, EXECUTIVE DIRECTOR, NATIONAL ASSOCIATION OF STATE ELECTION DIRECTORS

Ms. COHEN. Thank you, Chairman Burr, Vice Chairman Warner, and distinguished committee members, for the opportunity to submit this testimony on behalf of the National Association of State Election Directors.

My name is Amy Cohen and I'm the Executive Director of NASED. NASED's members are the State election directors in all 50 states, the District of Columbia, American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, Puerto Rico and the U.S. Virgin Islands. Our members are the nonpartisan professionals who administer and implement election-related policies, procedures and technologies. And NASED's mission is to promote accessible, accurate and transparent elections in the United States and territories, which we do by sharing information and best practices. Since elections were designated "critical infrastructure" in January 2017, our efforts have become more important than ever before.

In 40 states, the secretary of state or lieutenant governor is the State's chief election official. And in the remainder, the chief election official is the executive director of a board or commission. Beyond differences in leadership and other obvious differences in policies, the states also differ in the way elections are conducted. In eight states, elections are conducted at the township level instead of at the county level. Wisconsin alone has 1,853 local clerks responsible for conducting elections, in addition to the State election office. I highlight these differences as a reminder of how complex the administration of elections truly is.

Every State election official, though, is a planner. They have spent every day since the 2016 election learning how to improve for the future, and the "critical infrastructure" designation has given us access to resources many did not know were available previously. Now, approximately 15 months into the designation of elections as "critical infrastructure," we've made great strides as a field.

State election directors must communicate basic information to their voters to ensure that every eligible voter who wants to cast a ballot can do so. And election officials must give them confidence that their vote will then be counted as they intended. Effective communication with local election officials who serve as the boots on the ground in running elections is also paramount. States run regular trainings and provide information and resources year-round every year to make sure that local officials have access to

the information, tools, and skills they need to do their jobs effectively.

State election directors must also communicate with our colleagues in the Federal Government. Until 2016, this was primarily with the members and staff of the Election Assistance Commission, who provide an invaluable service to our field through their guides and best practices, informed by both qualitative and quantitative data.

Communication with DHS was new to NASED members in 2016 and is an area where we have seen significant improvement. In October 2017, DHS, the National Association of Secretaries of State, NASED and local election officials convened the first meeting of the Government Coordinating Council as a mechanism for sharing information about elections infrastructure threats across State, local, and Federal Governments. Since then, the GCC has met several times by telephone and again in person at the NASS and NASED winter conferences. The executive committee of the GCC, which has representatives from NASS, NASED, local election official organizations, and DHS, meets every other week by telephone.

The GCC voted unanimously in February to adopt goals and objectives for the elections infrastructure sector. Working groups are doing the challenging work of writing a strategic communications plan, to develop guidelines around communications, and of writing a sector-specific plan to formalize the strategic goals of the elections infrastructure sector for the next several years.

In addition, the Elections Infrastructure Sector Coordinating Council was launched in December 2017 with representatives from private sector vendors and nonprofit organizations.

The GCC and the executive committee of the GCC are critical to distributing information to all 50 states, the District of Columbia, and the territories, as well as disseminating critical cyber security information to the more than 8,000 local election officials.

The GCC also voted at the February meeting to formally recognize the Multi-State Information Sharing and Analysis Center as the elections infrastructure ISAC. While all 50 states, the District of Columbia and the U.S. territories were members of the MS–ISAC prior to 2017, election officials were not privy to the information shared by the ISAC and thus could not act on any of the information shared about the 2016 election.

As of today, however, the EI–ISAC, which is free for election offices to join, counts 38 State-level election offices and more than a 100 local election offices as members. NASS, NASED and the executive committee of the GCC strongly encourage all State and local election jurisdictions to join and are developing a strategic outreach plan to make sure every one of our State and local election officials understands the benefits of participation and joins.

DHS has also facilitated secret-level security clearances for State chief election officials, as well as additional election office staff, including State election directors. Our hope in doing so is to ensure that any future information-sharing will not be hindered or delayed by the information's classification. As you are aware and have heard about this morning, processing for security clearances can take time, but we continue to make progress with DHS in this area.

Finally, DHS hosted more than 60 election directors and staff, representing 43 states, D.C., and two territories, for a secure briefing with the Office of the Director of National Intelligence and the Federal Bureau of Investigation in conjunction with our February conference.

It would be naive to say that we received answers to all of our questions, but the briefing was incredibly valuable and demonstrated how seriously DHS and others take their commitment to the elections community as well as to our concerns.

There have of course been challenges, but we have taken incredible leaps forward in a relatively short amount of time. Since the November 2016 elections, states have hardened the defenses of their voter registration databases and other IT systems against intrusion. This has included taking advantage of free resources such as vulnerability and risk assessments from DHS, cyber security services offered by State branches of the National Guard, and utilizing services offered by other branches of State government.

Several private sector vendors have made tools and resources available to State and local election officials providing additional defenses. The Belfer Center at Harvard and the Center for Internet Security have provided practical guidance and tools for State and local election officials to use to strengthen their cyber security posture. Election officials have long taken steps to build resiliency and redundancy into their systems, and all states are evaluating the steps they take in light of the cyber security threats we face today.

Aging voting equipment has been at the forefront for election officials for years. The Presidential Commission on Election Administration report, released in 2013, highlighted the impending crisis in voting technology. The voting technology problem and its effect on cyber security is multi-faceted. First, I mentioned earlier that states run their elections differently. Local election officials are strapped for resources and are sometimes reliant on vendors or contractors for IT support. This can make it difficult for local jurisdictions to make smart technology purchases and adds an additional layer of complexity to maintaining a defensive cyber security posture. Many are taking advantage of in-State academics or national resources, including those at the EAC, to make sure that purchases comply with best practices.

Second, many jurisdictions purchased their current voting equipment with Federal funds received under the Help America Vote Act of 2002, meaning that the equipment and software often predate parts of our lives we now take for granted, such as smartphones. Without additional funding, jurisdictions cannot afford to purchase new technology. We're encouraged to hear that Congress may release some outstanding HAVA dollars in the omnibus appropriations bill.

Third, a handful of states still use voting technology that does not have a paper record or a voter-verified paper audit trail. These states are reliant on the accuracy of their voting machines, because in the event of a recount their records only exist in the machine. To be clear, we have seen no evidence that voting machines or election results have been manipulated or compromised in any election. But election officials must remain vigilant.

Understanding these risks is important, but we should not overlook the safeguards currently in place to protect the existing technology. Elections are decentralized. There are thousands of jurisdictions, hundreds of thousands of voting locations, and many more hundreds of thousands of voting machines. The diversity of equipment used and the sheer number of precincts and machines creates obstacles to a large-scale attack on voting equipment. Voting machines themselves are not connected to the internet, making them less susceptible to intrusion.

And results released on election night are not the official results. Every State and every local jurisdiction for elections run at the local level conducts an official canvass of results several days after election day to complete the official tally of results. In addition, an increasing number of states are doing post-election audits and many more are considering risk-limiting audits.

In summary, the field of election administration has made great strides since the 2016 presidential election, and State and local election officials cannot do this alone.

If 2016 taught us anything, it is that we need a whole-of-government approach, with strong coordination and communication across the Federal, State, and local players.

We appreciate this committee's recommendations released yesterday and are pleased that many of those are already underway in many states. Thank you for the opportunity to share NASED's thoughts and opinions with you, and I am happy to answer any questions.

[The prepared statement of Ms. Cohen follows:]

Written Testimony of Amy Cohen
Executive Director
National Association of State Election Directors

United States Senate Select Committee on Intelligence
March 21, 2018

Thank you Chairman Burr, Vice Chairman Warner, and distinguished committee members for the opportunity to submit this testimony on behalf of the National Association of State Election Directors (NASED). My name is Amy Cohen, I am the Executive Director of NASED.

NASED members are the state election directors in all 50 states, the District of Columbia, American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, Puerto Rico, and the U.S. Virgin Islands. Our members are the nonpartisan professionals who administer and implement election-related policies, procedures, and technologies, and NASED's mission is to promote accessible, accurate, and transparent elections in the United States and the territories, which we do by sharing information and best practices across our jurisdictions. Since elections were designated critical infrastructure in January 2017, our efforts have become more important than ever before.

In June 2017, Michael Haas, the former Administrator of Elections for Wisconsin testified before this committee on behalf of NASED and shared several of the lessons learned from 2016. As Mr. Haas discussed at that time, there are significant differences in election administration across the states. In 40 states, the secretary of state or lieutenant governor is the state's chief election official, and in the remainder, the chief election official is the Executive Director of a board or commission. Beyond differences in leadership and other obvious differences in policy, the states also differ in the way elections are conducted – in eight states, elections are conducted at the township level instead of at the county level; Wisconsin alone has 1,853 local clerks responsible for conducting elections, in addition to the state election office. I highlight these differences as a reminder of how complex the administration of elections truly is.

While I sit here today representing an incredibly diverse group, every state election official is a planner. They have spent every day since the 2016 election learning how to improve for the future, and the critical infrastructure designation has given us access to resources many did not know were available previously.

Mr. Haas' testimony last year focused on three key lessons from the 2016 presidential election. First, he noted that state election offices faced a new challenge of communicating not just with their local election officials, but also with employees of the Department of Homeland Security (DHS), who in 2016 were brand new to the nuances and complexities of election administration. Second, he noted that 2016 highlighted additional steps that states can take to secure their voter registration databases and tools they can use to improve their voter registration lists. Finally, he discussed the ongoing efforts that state and local election officials take to secure equipment used to cast and count ballots.

We are now approximately 15 months into the designation of elections as critical infrastructure, and nearly nine months removed from Mr. Haas' testimony. As a field, we have made great strides in that time.

For state election directors, communication is a significant part of the job. They must communicate basic information to their voters to ensure that every eligible voter who wants to cast a ballot can do so, and election officials must give them confidence that their vote will then be counted as they intended. Effective communication with local election officials, who serve as the boots on the ground in running elections, is also paramount. States run regular trainings and provide information and resources year-round every year to make sure that local officials have access to the information, tools, and skills they need to do their jobs effectively. Most voters will not interact with state-level election officials directly, but will with their local election official, so it is important that everyone act as a team. And, state election directors must communicate with our colleagues in the federal government. Until 2016, this was primarily with members and staff of the Election Assistance Commission (EAC), who provide an invaluable service to our field through their guides and best practices informed by both qualitative and quantitative data.

Communication with DHS, however, was new to NASED members in 2016, and is an area where we have seen significant improvement. In October 2017, DHS, the National Association of Secretaries of State (NASS), NASED, and local election officials convened the first meeting of the Government Coordinating Council (GCC) as a mechanism for sharing information about elections infrastructure threats across state, local, and federal governments. Since then, the GCC has met several times by telephone and again in-person at the NASS and NASED Winter Conferences here in Washington, D.C. last month; the Executive Committee of the GCC, which has representatives from NASS, NASED, local election official organizations, and DHS, meets every other week by telephone.

The GCC voted unanimously in February to adopt goals and objectives for the Elections Infrastructure Sector, and working groups are doing the challenging work of writing a strategic communications plan to develop guidelines and norms around communications and of writing a Sector Specific Plan to formalize the strategic goals of the Elections Infrastructure Sector for the next several years. In addition, the Elections Infrastructure Sector Coordinating Council (SCC) was launched in December 2017 with representatives from 25 private sector vendors and nonprofit organizations. The GCC and the Executive Committee of the GCC are critical to distributing information to all 50 states, the District of Columbia, and the territories, as well as disseminating critical cybersecurity information to the more than 8,000 local election officials.

The GCC also voted at the February meeting to formally recognize the Multi-State Information Sharing and Analysis Center (MS-ISAC) as the Elections Infrastructure ISAC (EI-ISAC). The purpose of an ISAC is to serve as a central resource for gathering, analyzing, and disseminating information related to critical infrastructure, and to facilitate two-way cybersecurity threat information sharing between the public and the private sectors. While all 50 states, the District of Columbia, and the U.S. territories were members of the MS-ISAC prior to 2017, election offices were not privy to the information shared by the ISAC and thus could not act on any information shared about the 2016 election. As of today, however, the EI-ISAC, which is free

for election offices to join, counts 38 state-level election offices and more than 100 local election offices as members. NASS, NASED, and the Executive Committee of the GCC strongly encourage all state and local election jurisdictions to join and are developing a strategic outreach plan to make sure every one of our state and local election officials understands the benefits of participation and joins.

DHS has also facilitated secret-level security clearances for State Chief Election Officials, as well as additional state election office staff, including state election directors. Our hope in doing so is to ensure that any future information sharing will not be hindered or delayed by the information's classification. As you are aware, processing for security clearances can take time, but we continue to make progress with DHS in this area.

Finally, DHS hosted more than 60 election directors and staff representing 43 states, the District of Columbia, and two territories for a secure briefing with the Office of the Director of National Intelligence and the Federal Bureau of Investigation in conjunction with our February conference. It would be naïve to say that we received answers to all of our questions, but the briefing was incredibly valuable and demonstrated how seriously DHS and others take their commitment to the elections community, as well as to our concerns.

There have, of course, been challenges as we have worked with DHS, but we have taken incredible leaps forward in a relatively short amount of time.

Since the November 2016 election, states have hardened the defenses of their voter registration databases and other IT systems against intrusion. This has included taking advantage of free resources such as vulnerability and risk assessments from DHS, cybersecurity services offered by state branches of the National Guard, and utilizing services offered by other branches of state government. Several private sector vendors, including Cloudflare and Google, have made tools and resources available to state and local election officials, providing additional defenses. The Defending Digital Democracy Project of the Belfer Center at Harvard and the Center for Internet Security have provided practical guidance and tools for state and local election officials to use to strengthen their cyber security posture. Election officials have long taken steps to build resiliency and redundancy into their systems, and all states are evaluating the steps they take in light of the cybersecurity threats we face today.

In addition, states continue to explore means to improve their voter registration list maintenance practices. While those of us in the field know to update our voter registration record in the event of a move or a life change, many Americans do not know to do this, or they think that updating their information with one government agency updates it at all government agencies. Inaccurate lists cause a variety of administrative headaches but can also make it easier to misuse outdated voter records.

Aging voting equipment has been at the forefront for election officials for years; the Presidential Commission on Election Administration (PCEA) report, released in 2013, highlighted the "impending crisis in voting technology" and we are now several years from that. The voting technology problem and its effect on cybersecurity is multifaceted.

First, I mentioned earlier that states run their elections differently; in some states, this extends to voting machines. In practice, this means that in some states, the state purchases voting equipment for all of its local election jurisdictions, while in other states, each county is responsible for its own election technology purchases. Local election officials are strapped for resources and are sometimes reliant on vendors or contractors for IT support. Combined, this can make it difficult for local jurisdictions to make smart technology purchases and adds an additional layer of complexity to maintaining a defensive cybersecurity posture. However, the national focus on election cybersecurity has given state and local election officials access to more information and experts. Many are taking advantage of in-state academics or national resources, including those at the EAC, to make sure that technology purchases comply with best practices.

Second, many jurisdictions purchased their current voting equipment with federal funds received via the Help America Vote Act of 2002 (HAVA), meaning that the equipment and software often predate parts of our lives we now take for granted, such as smartphones. Without additional funding, jurisdictions cannot afford to purchase new technology and are stuck trying to maintain old equipment and software on outdated, insecure operating systems. At the state and local level, elections must compete for funding with education and public safety to name just a few. We are encouraged to hear that Congress may release the outstanding HAVA funds in the Omnibus Appropriations bill.

Third, a handful of states still use voting technology that does not have a paper record or a Voter Verified Paper Audit Trail (VVPAT). These states are reliant on the accuracy of their voting machines because in the event of a recount, the records only exist in the machine. Claims abound that these machines are susceptible to malicious attack because there is no paper trail or opportunity for the voter to verify that their ballot was cast as intended. To be clear, we have seen no evidence that voting machines or election results have been manipulated or compromised in any election, but election officials must remain vigilant.

Understanding these risks is important, but we should not overlook the safeguards currently in place to protect the existing technology.

- Elections are decentralized. There are thousands of election jurisdictions, hundreds of thousands of voting locations, and many more hundreds of thousands of voting machines. The diversity of equipment used and the sheer number of precincts creates obstacles to a large-scale attack on voting equipment.

- Voting machines themselves are not connected to the internet, making them less susceptible to intrusion.

- Results released on election night are not the official results. Every state – and every local jurisdiction for elections run at the local-level – conducts an official canvass of results several days after Election Day to complete the official tally of results. In addition, an increasing number of states are doing post-election audits, the most basic of which randomly select precinct results and contest results to compare hand-counted results to the machine results. Still other states are doing Risk Limiting Audits, pioneered

by Colorado, in which statistical methods are used to select the number of ballots that must be examined for a particular contest.

In summary, the field of election administration has made great strides since the 2016 presidential election. State and local election officials cannot do this alone; if 2016 taught us anything, it is that we need a whole of government approach, with strong coordination and communication across the federal, state, and local players.

Thank you for the opportunity to share NASED's thoughts and opinions with you. I am happy to answer any questions.

####

Chairman BURR. Thank you, Amy for that testimony.

Eric, the floor is yours.

STATEMENT OF ERIC ROSENBACH, CO-DIRECTOR, BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS, HARVARD KENNEDY SCHOOL

Mr. ROSENBACH. Chairman Burr, Vice Chairman Warner, other distinguished members of the committee: Thank you very much for the invitation to testify. The committee is one of the very few bipartisan efforts to address threats to the integrity of our democracy right now, and your leadership is crucial to charting the course forward. As a former professional staff member on the Senate Intelligence Committee, I have great respect for your bipartisan approach to what you're doing and genuinely thank you and your hardworking staff for all the work you're doing and your service.

Our response to Vladimir Putin's ongoing attempts to undermine the strength of American democracy will be a defining issue of our digital age. Putin's attacks are not limited only to our election systems. Recent reports from the Department of Homeland Security make clear that Russian military intelligence operatives continue to conduct the preparatory steps needed for a major cyber attack against our energy infrastructure, including pre-placing the same malware in the United States that they used to take down the electric grid in Ukraine, twice.

Imagine, if you would, that during the Cold War we found out that Soviet military intelligence operatives had placed secret explosives that could take down the electric grid all around the United States. Would our leaders have stood by and debated the nature of the threat or would we act?

Unfortunately, over the past three years and both Administrations our national response to Russian cyber and info attacks both against the United States and our allies has been too weak. America and democracies around the world need action and, given the current environment in Washington, the Senate Intelligence Committee will need to play a leading role in driving that action.

In the summer of 2017, a little team up at the Harvard Kennedy School set on a mission with one primary goal: to do as much, as quickly as possible, to help lower the risk of cyber and information attacks on the 2018 mid-term elections. So this project, known as the Defending Digital Democracy Project, is a bipartisan initiative that I co-lead with Robby Mook and Matt Rhoades. And we're developing real-world practical solutions to try to defend against cyber and information attacks.

It's a diverse team. We have technical experts, political operatives, public affairs ninjas, and a hardworking team of Kennedy School students who are working very closely with NASS, NASED and the Department of Homeland Security to support our project. They've been truly outstanding partners, including several secretaries of state, Mac Warner in West Virginia, Denise Merrill in Connecticut, and Alison Lundgren Grimes in Kentucky, all part of the team.

Since then, our team has conducted field research in 34 State and local election offices, observed the November 2017 elections in three states, and conducted a nationwide survey on cyber security

in 37 states and territories, and engaged State and local elections officials in a tabletop exercise at a national level three different times.

Based on that research and our observation, we have released four different practical election-related security playbooks, including for political campaign staffs, local election officials, and two specific playbooks on incident response.

Next week, up in Cambridge, Massachusetts, we'll host over 160 State and local election officials from 38 states to run them through a series of crisis simulations that are structured to train and empower them to improve their cyber defenses and incident response capabilities, and to provide them with the tools to run these exercises back in their home states. The so-called "train the trainer" exercise, a traditional military, Army way of doing things, we'll follow up then with a hackathon, where we sponsored a national competition for student teams from around the country to compete for three $10,000 prizes which will be awarded to the best developed tech and policy options to counter Russian information operations.

Now, I would like to tell you a little bit about our observations of the states. Chairman Burr, you asked about that. And the bottom line is this: State and local election officials are on the front lines of the effort to defend against nation-state attacks on our democracy. They accept this mission admirably. Our team has always been impressed with their professionalism and dedication. But, that said, the states need more help. They simply are not equipped to face the pointy end of the spear of cyber attacks and information operations from advanced nation-states.

One often underemphasized issue is that the states, along with the Federal Government and outside organizations, need to continue to develop the capabilities for public incident response to information operations. So not just the hacks, but along the lines of what Senator Rubio mentioned, an information operation trying to sow distrust in the outcome of the election even if a hack were not successful. One of the few real antidotes to aggressive information operations like the Russians regularly conduct is effective public communications about the true state of affairs.

The work we've done at the Kennedy School is really just a small part of the assistance that the states need and deserve to defend themselves. They need extra help. Specifically, it will require a four-cornered effort an all-of-nation effort, not just government. There's a lot that people not in the government can do now.

The first is the State governments, which I think you've heard a lot about and so I won't reiterate. Second of all, we need to pay attention to political campaigns. They're the soft underbelly of this system right now. Their cyber hygiene generally is not good, and the overall chaotic environment in which they operate is not conducive to good cyber security.

Social media companies, who must accept that our adversaries will continue to manipulate their platforms unless they dramatically change their organizational culture and their operational paradigm.

And finally, the Federal Government, which must better support State and campaign efforts, oversee social media, and lead in cre-

ating the credible national defensive posture equal to the cyber and information threats that our elections face.

Thank you very much. I look forward to answering any questions you have about any of our research, and I promised your staff that I wouldn't go over five minutes.

[The prepared statement of Mr. Rosenbach follows:]

Defending Digital Democracy: The Four Corners of Election Security

Prepared Statement
by
Honorable Eric Rosenbach
Co-Director of the Belfer Center for Science and International Affairs at the Harvard Kennedy School; former Chief of Staff to the Secretary of Defense and Assistant Secretary of Defense for Homeland Defense and Global Security

Before the

United States Senate Select Committee on Intelligence

Hearing on

Russian Interference in the 2016 US Elections

March 21, 2018

Chairman Burr, Vice Chairman Warner, and distinguished members, thank you for the invitation to testify. As one of the very few bipartisan efforts to address the cybersecurity challenges to our country right now, this Committee is crucial in charting the course forward. As a former professional staff member on the Senate Intelligence Committee, I have great respect for your bipartisan approach and genuinely thank you for your service.

Our response to Vladimir Putin's ongoing attempts to undermine the strength of American democracy will be a defining issue of our digital age. The most important lesson we should internalize from Russia's interference campaign in 2016 is the price of complacency: we ignore continued cyber attacks and insidious information operations at our own peril.

Putin's attacks are not limited to our election systems. Recent reports from the Department of Homeland Security make clear that Russian military intelligence operatives continue to conduct the preparatory steps needed for a major cyberattack against our energy grid.

Imagine if we found out during the Cold War that Soviet intelligence operatives had placed secret explosives that could take down the electric grid all around the United States. Would US leaders stand by and debate the nature of the threat, or would we act?

Unfortunately, our national response to Russian cyber and info attacks—both against the US and our allies—has been too weak. America and democracies around the world need action. This should not be a partisan issue: we must shift gears from examining the problem to taking

assertive steps to address it. Given the current environment in Washington, the Senate Intelligence Committee will need to play a leading role in driving action and solutions.

Russia's actions underscore the urgency to pursue a whole-of-nation strategy that involves the four key players in our election ecosystem: states, campaigns, tech companies and the federal government. A "four-cornered" effort involving these actors would focus on four primary goals:

1. Bolster our domestic cyber defenses and systemic resilience;
2. Develop and rehearse a coordinated, national incident response plan;
3. Develop precise and legal offensive cyber capabilities that will disrupt cyber and information attacks at their source; and
4. Adopt a clear, public deterrence posture, which definitively signals that we will not accept threats to, or attacks on, our democratic institutions and critical infrastructure.

The Problem

Our country's reliance on digital technologies, coupled with our open and transparent information ecosystem, has created significant vulnerabilities. We increasingly live in a digital "glass house" that must be much better protected. The glass house analogy illustrates three important points.

- As technology advances and we become more connected, we become more vulnerable. This is because cyber warfare is asymmetric: a small nation with an offensive cyber capability can have an outsized effect on a larger power. In fact, the greater the technology gap between us and an adversary, the greater our vulnerability. For example, the US is significantly more vulnerable to cyberattack than North Korea, a nation where most citizens do not even have an internet connection. North Korea, however, has advanced offensive cyber capabilities.

- Democracies' transparent, open societies also make them vulnerable to foreign information operations. In democracies, free speech is protected, and internet accessibility is high. In contrast, authoritarian societies often control the media, censor the internet and shield their nations from outside information through national firewalls, such as the Great Firewall of China. America's enemies have learned to weaponize free speech.

- The vulnerabilities caused by openness are exacerbated by the way in which modern communications technologies facilitate near-instantaneous information sharing, the proliferation of online networks and communities, and the creation of massive troves of information and data. These factors enable information operations at a scale, and level of personalization, previously unimaginable.

The Russian Government was a first-mover in fully understanding the vulnerabilities in a digital democracy. As early as 2014—and possibly before—President Putin authorized a widespread campaign with the strategic goal of undermining trust in democracy and inciting political and social discord.

The facts about Russia's action in 2016 are now widely understood. Russian intelligence operatives and their thinly-disguised proxies stole and leaked sensitive information from political campaigns and employed hundreds of operatives in "troll farms" to spread and amplify toxic content on social media, and to orchestrate divisive political rallies on American soil. They used bots to further spread their narratives, and drown out legitimate voices. They also tried to hack, or at least test, vulnerabilities in multiple states systems.

Most of the digital tools Russia did use were cheap, and did not require technical sophistication. Russia also relied more on information operations than it did on cyberattacks. But the hybrid nature of cyber and information operations was effective and provides a model for attacks in the future. Without a major shift in US policy, this problem is not going away. Instead, we should expect Russia, and other actors emboldened by Russia's success, to conduct increasingly potent cyber and information attacks against our elections and other core systems that underpin our democracy.

Defending Digital Democracy Project

The Defending Digital Democracy Project, a bipartisan initiative I co-lead at Harvard's Belfer Center along with Robby Mook and Matt Rhoades, is developing real-world, practical solutions to defend against cyber and information attacks. The team has breadth and depth of talent—including cybersecurity experts from government and the private sector, technologists and political operatives. Ahead of the 2018 midterms, we have released practical election security guides, including for political campaign staff, state and local election officials, and for election cyber incident communications teams.

Through our work, we have come to believe that election security can only be achieved by a whole-of-nation effort. Specifically, it will require a four-corned effort by:

1. State governments, whose election officials are now front-line defenders of our democratic systems, and must adopt cybersecurity best practices, and lead on incident response to cyber and information operations.
2. Political campaigns, who must internalize their responsibility to adopt good cyber hygiene and bolster their own cyber defenses.
3. Social media companies, who must accept that our adversaries will continue to manipulate their platforms unless they dramatically change their organizational culture and operational paradigm.
4. The federal government, which must better *support* state and campaign efforts, *oversee* social media and *lead* on creating a credible national defensive posture equal to the cyber and information threats our elections face.

State Governments

States run and control elections in the United States. That puts local election officials on the front lines of the effort to defend against nation-state attacks on our democracy. They accept this

mission admirably: the Defending Digital Democracy team has been consistently impressed by the professionalism, and dedication of state and local election officials. And I would like to acknowledge my fellow panel member Secretary Condos for the work he has done up in Vermont and will continue with his service as the future President of the National Association of Secretaries of State.

Our team conducted field research at 34 state and local election offices, observed the November 2017 elections in three states, conducted a nationwide survey on cybersecurity with 37 states and territories, and engaged state and local election officials in three national "tabletop exercise" simulations.

This research revealed the complex and decentralized nature of the US election system. Every state has to protect and monitor an election ecosystem that is an interconnected "system of systems." This ecosystem includes core election systems—like registration databases, voting machines, and counting and reporting systems. But it also includes non-core systems, like state and county administrative and office databases, email systems, public-facing websites, and third party vendor systems.

On top of this, the fact that election decision-making is delegated to multiple counties, and in some cases municipalities, results in several hundred, if not thousands, of different election processes across the country. Conventional wisdom leads many officials to claim that this makes our democracy more secure; however, my time serving as the "Cyber Czar" for the Department of Defense convinced me that security through complexity is a myth. In fact, complexity is a force multiplier for our adversaries. It creates a huge attack surface that is difficult to patch, monitor, and defend. To succeed in destroying Americans' trust in democracy, Russia doesn't need to successfully attack the entire voting infrastructure. A cybersecurity incident in just a handful of counties could undermine public confidence in the national electoral process.

State election officials clearly understand that they are at risk and, in many cases, under attack. Many state election officials worked to improve their cyber defenses well before the Russian attacks in 2016, but nearly all of them have significantly upped their game over the past six months. That said, the states need more help: they simply are not equipped to face the pointy-end of the spear of cyber attacks from advanced nation-states.

The primary goal of the Defending Digital Democracy team is to provide as much assistance as possible to the states and campaigns. Last month, we released an Elections Cybersecurity Playbook, which sets out measures we believe are essential: using audits to maintain trust in the system; isolating sensitive systems; and requiring paper vote records.

One important, underemphasized issue is the ability of state and federal governments to respond publicly to cyber and information operations. Understandably, many election officials' initial instinct is to not talk to the press, or otherwise communicate. However, in elections, perception is reality. An adversary does not need to engage in actual cyber operations to manipulate the outcome of an election. They can erode trust in the process by using information operations to make the public believe that the election was manipulated or fraudulent. One of the few real

antidotes to aggressive information operations is effective public communications about the true state of affairs. We developed an additional public communications incident response playbook for the states with this in mind.

Next week, the Defending Digital Democracy team will host over 160 state and local election officials from 38 states to run them through a series of crisis simulations and training exercises to train and empower them to improve their cyber defenses and incident response capabilities.

The work we've done at the Harvard Kennedy School is really just a small part of the assistance that the states need—and deserve—to defend themselves. The states need additional support in the following areas:

- **Funding for election security.** Many states adopted digital voting systems after the 2000 presidential elections, but have not received the funding needed to keep these systems upgraded and secure. The most frequent concern noted by election officials in our nationwide security survey was insufficient resources to secure elections, especially in smaller counties. Funding could be tied to states following best practice cybersecurity recommendations, and could also be given in the form of grants for incident response planning, and "red team" exercises.
- **Access to information.** The Department of Homeland Security is working hard to increase intelligence sharing to the states through the multi-state Information Sharing and Analysis Center, and to grant security clearances to some officials. However, we need a paradigm shift in this area. Unlike nearly every other national security threat, federal agencies are the support, not the lead, on election security. Collecting intelligence therefore has limited utility if it is not shared with the state officials on the frontline. One option: strengthen the role that state-run fusion centers play in election-related threat information sharing. Threat intelligence from private sector cybersecurity and tech firms will also be key to any information sharing arrangement.
- **Cybersecurity expertise.** All sectors of the American economy are starving for additional personnel with cybersecurity expertise and states are no different. Working with the private sector, the country needs to find ways to surge more cybersecurity expertise to the states in the run-up to the 2018 midterms and the 2020 presidential vote. One option: the Defending Digital Democracy team is working to develop a Democracy Defense Service of deployable experts who could help states in need. Built on the model of the Defense Digital Service, this could provide states with help when they need it...without creating unnecessary bureaucratic organizations.
- **Vendor security.** In many states, vendors design and maintain hardware and software that affect voter registration, vote capture and tallying, electronic pollbooks, election night reporting, and public communication. In our nationwide security survey, 97% of states and territories used a vendor in some capacity. Some vendors service multiple states—meaning an attack on one vendor could affect many jurisdictions. One option: states should demand explicit security stipulations in requests for proposals and all acquisition and maintenance contracts. Congress should bolster this by requiring vendors to provide notification of any system breach immediately after they become aware of it.

Campaigns

Political campaigns are the soft underbelly of the American election process. Unfortunately, even after the cyberattacks on 2012 and 2016 presidential campaigns, many campaign workers do not yet fully appreciate the important role they have in improving the integrity of our elections.

Russia did not need sophisticated cyber-weapons to hack into the Democratic campaign in 2016. It used spear phishing—which requires persistence, more than technical capability. This points up the urgent need for campaigns to adopt basic standards of cyber hygiene. The Defending Digital Democracy team has developed a "Top Five Checklist," as part of a broader Campaign Cybersecurity Playbook, specifically designed for resource-constrained campaign workers. At a minimum, campaigns need to move data to the cloud, and require two-factor authentication on all important accounts. We are pleased to see that Kentucky and West Virginia's Secretaries of State have officially issued the Playbook to candidates in their states.

Campaigns can significantly improve their cyber defenses by following cybersecurity best practices, but they can't fight our adversaries' national intelligence services on their own. The most urgent need for campaigns is much better access to threat information and intelligence. Unlike the states, currently no Information Sharing and Analysis Center or information sharing arrangement exists to facilitate the flow of threat information from the government and private sector to campaigns. This type of assistance is complicated by current campaign finance law. Robby Mook and Matt Rhoades are leading the Defending Digital Democracy effort in this area, where we've developed several blueprints for campaign information sharing architectures that could work within the existing realities of law and politics.

Social media

Imagine how Americans in the 20th century would have reacted to news that our manufacturing titans were building weapons, on American soil, for US adversaries, or that broadcast television networks were providing a megaphone to Soviet spies. Social media companies have revolutionized communication and commerce in the 21st century, and they are an essential aspect of American economic power in the Information Age. But social media companies have also created tools and systems which can be used to subvert democracy.

Government oversight has not kept pace with these changes. But, more significantly, neither have the leadership and organizational culture essential to organizations that wield so much power and influence in a digital democracy. Their very business models are enabled by the democratic protections afforded by the American system of government, including the First and Fourth Amendments. Simply put: Facebook and Twitter are no longer scrappy start-ups that can move fast, break things, and beg forgiveness later. They are some of the world's most powerful, and capitalized corporations and they should act that way.

Noting this, Facebook and Twitter must:

- **Transform their organizational culture.** Leading tech firms need to internalize the role they play in protecting democracy, and ensure that their business models do not damage the very democratic protections that have enabled their success. Transparency will be an essential component in rebuilding trust in these organizations.
- **Adjust their algorithms to reflect their role in democracy.** Because of their market dominance, Twitter and Facebook do not just house public discourse; they shape it. Currently, social media algorithms are optimized for user engagement, because clicks and views maximize revenue. As a result, Facebook, YouTube and Twitter often promote and prioritize controversial information—something that Russian trolls and bots exploited to great effect. However, it is possible—and necessary—to adjust these algorithms.
- **Increase human involvement in decisions.** Real humans must be involved in flagging problematic content and accounts. Autonomous agents are still easily fooled, and, despite growing excitement about the promises of artificial intelligence, for the foreseeable future there will remain no substitute for human language processing and cognition when it comes to addressing national security threats.

Congress should also ensure that social media is treated in the same way as other industries which create negative externalities for society. In particular, Congress should strongly consider legislation to:

- **Enhance transparency.** Users have a right to know when they are seeing paid political advertisements, and, in some cases, why they are being targeted by particular political or social campaigns. Congress should pass legislation that mandates the same disclosure for political ads on social media as for traditional media.
- **Strengthen data protection rules.** Data collected by social media companies is extraordinarily powerful, and social media firms have proved themselves unable to properly protect it. This was reinforced by allegations concerning the transfer of sensitive Facebook user data to Cambridge Analytica. We do not permit hospitals or financial institutions to monetize sensitive consumer data without consent, and we hold them accountable when sensitive information is leaked. The data collected by social media firms can be just as sensitive since we now know it will be used to created detailed psychological profiles of users. And its misuse has even broader implications for society, since those profiles can be harvested and "weaponized."

Government

Protecting democratic institutions from cyber and information attacks by nation-states is an inherently governmental role. Unfortunately, our national response to Russian cyber and info attacks—both against the US and our allies—has been too weak. The recent move by the Trump Administration to increase sanctions on Russian entities involved in cyber attacks against Ukraine and the US is a step in the right direction, but not nearly enough.

The US and international community must respond to cyber and information operations with actions that are sufficiently visible and serious to deter future attacks. Given the depth of the

"glass house" problem I outlined above, our weak response puts America in a very vulnerable position.

Thus, the US must urgently act to bolster its deterrence posture by both raising the costs of attacks and decreasing the benefits to hostile actors of engaging in this conduct. In addition to a host of non-cyber foreign policy options, the US should pursue the following initiatives:

- **Bolster Cyber Command's capability to address information operations.** The US military lacks the structure and capability necessary to defend the nation from future attacks. Special Operations Command has historically led Department of Defense efforts in information operations, but the lead must now shift to Cyber Command in order to strengthen the nexus of cyber and information operations capabilities necessary for the Information Age. That said, the DoD's recent efforts to combat ISIS through a joint SOCOM-CYBERCOM effort, known as Task Force Ares, represents an outstanding model for future operations.
- **Strengthen indications and warning of cyber and information operations attacks.** The Intelligence Community, and the National Security Agency in particular, need to bolster the "early warning" system for information operations which target US democratic institutions. This will require better collaboration with the private sector, which should shed its post-Snowden reluctance to cooperate with the government on pressing national security issues.
    - LTG Paul Nakasone is an outstanding leader who is absolutely the best person to lead CYBERCOM and NSA in an effort to accomplish both of these recommendations.
- **Continue to strengthen DHS information sharing and cybersecurity capacity.** Under the leadership of Secretary Nielsen and Under Secretary Krebs, DHS has prioritized and improved information sharing with the states. The Department's efforts to provide cybersecurity scans and risk assessments to the states have been productive and help to mitigate risk. Congress should strongly support these efforts and provide DHS with the resources it needs to bring them to full maturity, while DHS should broaden and strengthen efforts to support the cybersecurity of political campaigns.

Conclusion

This Committee has rightly observed that a whole-of-government response is required to address the problems of election security. I completely agree, but would go further: this must be a whole-of-nation effort, which involves each of the four key players in our election ecosystem. But, this four-cornered effort needs leadership, and the Senate Intelligence Committee is the team most likely to provide that cross-cutting, bipartisan leadership in the current environment.

Chairman BURR. Eric, thank you.

Mr. ROSENBACH. Yes, sir.

Chairman BURR. Thank you for your service on this committee. Senator Hagel would be proud of you, as we are.

I would note that today we're highlighting one slice of the Russian effort into the U.S. democracy. It's the election process. When we've completed our investigation, which has been extensive, hopefully it will expose all of the portals that Russia used to sow chaos and societal chaos and everything else that they did.

But you also mentioned a lot of things at the beginning that have not historically been on the plate of the Senate Intelligence Committee, that are now front and center, not because of the lack of interest of other committees, but because of the unique expertise of the staff on this committee and the interests of the members. And so we're juggling a lot of balls in the air right now.

With that, I'd like to recognize Senator Lankford for the first round of questions.

Senator LANKFORD. Thank you, Mr. Chairman.

Thank you all for being here and the time you've dedicated to this already.

Let me ask just, Mr. Condos, about the recommendations that this committee has made on trying to make changes for cyber security, whether that be systems that can be audited, whether that be—obviously being separate from the internet during voting times, attentive when there are updates for software even when you're not connected to the internet for those machines, having a way to be able to do risk-limiting audits, security clearances for individuals when they—so we have a point of contact with DHS so they can do rapid communication. Any of those—are any of those concerns to you or to your organization?

Mr. CONDOS. Let me speak on behalf of personally and the State, not——

Senator LANKFORD. Sure.

Mr. CONDOS [continuing]. Not NASS on this, because we have actually not taken a formal position because we just barely got the recommendations. But let me just say that we have long believed that having paper ballots, having an audit—we've been completing audits since 2006 and to date we've not had any anomalies from those audits.

In fact, the audit that we do now, that started in 2014, now we call it a 100 percent census because we do the entire set of ballots for a particular town. We do a series of towns, randomly picked, and we do the entire ballot bag for that town that were cast, and then we also do every race that's on that ballot from President on down.

We believe that having audits is critical to this and we are completely in agreement with that. I think that some of the other recommendations that you have put forth are excellent recommendations. We're already implementing many of them in Vermont and will be—like for instance, we're adding two-factor authentication for our local towns. We do not have county government in Vermont. We go straight from the towns to the State, so we're looking now at putting two-factor authentication between now and probably May or June.

Senator LANKFORD. Can I ask you if DHS has been proactive to be able to help your State over the past year in communication and ideas.

Mr. CONDOS. So let me just say that I think there was a lot of trepidation between the states and DHS in the beginning, but over the last——

Senator LANKFORD. When you say "in the beginning," are you talking about that August 15th call?

Mr. CONDOS. Well, I'm talking about from August 16th—August 2016 to sometime last fall. Since that time we have really improved communications and we're working well together. You know, there's the obvious ups and downs that you have, but we are working well together, and I think that communication has improved tremendously.

Senator LANKFORD. Has DHS been an asset to you?

Mr. CONDOS. Yes. We do use the weekly hygiene scans. Many of the other products that they give, we've already done and we will continue to do. I don't want to leave the impression that just because we're not doing it with DHS, we're not doing it.

Senator LANKFORD. No, I understand. They're a resource that will be available to you if you choose to use those.

Mr. CONDOS. Correct.

Senator LANKFORD. There is the concern that some of us have that if an individual State is attacked, that State identifies, I'm getting in some certain attack, and that information, whether it be the IP address or the type of malware or whatever it is, that the State picks up, if that's not shared with DHS there's not the opportunity for other states to also be able to check their system.

How can we improve the trust level, that when a State identifies, I'm getting an attack that's unique, that they share that with DHS and so other election systems can also check for it?

Mr. CONDOS. Well, let me explain what we've done in Vermont. When we see an anomaly, what we think of as an anomaly in our daily monitoring of our systems, if we encounter something like that, we will automatically count our FBI, DHS partners, and MS–ISAC to let them all know. And once we have—they will tell us what they need from us and then we provide that to them so that they can look at it.

But I definitely, I think where you were going is the fact that if one State is attacked, all states are attacked.

Senator LANKFORD. Right.

Mr. CONDOS. And that's the way we have to approach this.

Senator LANKFORD. And one of the issues that we have is, if one State is attacked, the other states might have already been attacked, they just didn't pick it up and you did.

Mr. CONDOS. Possibly.

Senator LANKFORD. So it's exceptionally important that we get the chance to have that two-way communication going, again voluntarily. But it is good participation whether it's just to be able to make sure that we can help each other.

You mentioned as well duplication in your voter rolls. You said you do that every single day, to be able to duplicate voter registration rolls?

Mr. CONDOS. Yes, we back up our system daily. It's kept for a period of time before it's cycled out. So at any given point in time, we could always go back to that date and re-establish, and then we only have a small sliver that we have to authenticate after that.

We also have same-day voter registration so nobody will be denied at the polls.

Senator LANKFORD. Okay. I just want to make one quick comment and I want to yield back to the Chairman as well. Thank you for all the work. You've been in quite a few meetings with our team and with Homeland Security that Senator Harris and I have both seen you on oftentimes. You've done a lot of work on a lot of these issues, boots on the ground, and we do appreciate your daily work on this. You've had some long days with your team, being able to work through some issues, so I appreciate your work on it.

I yield back.

Vice Chairman WARNER [presiding]. Senator Harris.

Senator HARRIS. And I couldn't agree more with Senator Lankford. Miss Manfra, every day it seems like we're seeing you on one of these committees, so thank you for your work.

Mr. Rosenbach, as everyone understands, achieving cyber security will be extremely difficult. In fact, some say we should—we're never going to actually achieve security, but we will try to do as best as we can. But there are no absolutes in this realm.

So the concern I have is that I think that there's a very real chance that when we're talking about HAVA, which is the Help America Vote Act of 2012—2002, that it may be a simplistic approach to suggest that the HAVA grant program is the solution to election cyber security.

One of the concerns that I have heard and I'd like your opinion about it, is that there is a very real chance that states could acquire a new batch of insecure systems—and Miss Cohen actually spoke a bit about that concern as well—because they just don't have the resources and it may be the technical resources or advice or support to make the best decisions about acquiring the best and most secure equipment.

So what is your perspective about that? And should states be required also to use those funds only for cyber security improvements versus other needs they may have?

Mr. ROSENBACH. Yes ma'am. I think, to start with your idea and highlighting that risk mitigation in cyber needs to be much broader than just the technical cyber security issues. So you talk about an incident response plan——

Senator HARRIS. Right.

Mr. ROSENBACH [continuing]. And leadership at the top. Vermont seems like a model in terms of a secretary of state who can talk about two-factor authentication and is doing all these things. That's what you want.

Senator HARRIS. And he's at this table for that very reason.

Mr. ROSENBACH. Exactly, but that's a rare thing.

Senator HARRIS. Yes.

Mr. ROSENBACH. And the states take this very seriously, but that level of knowledge is a rare thing.

Senator HARRIS. Right.

Mr. ROSENBACH. So the money will do one thing, but it's leadership that's even more important, and rehearsing what happens when you do get hacked or if you don't get hacked, but the Russians manipulate your information, that is very important.

I do think having outside technical expertise that has no vested interest can be helpful to the states in trying to determine maybe how to allocate resources. I don't think that you want to make it bureaucratic because we need to move fast and things are already bureaucratic enough in government. But some way to help the states I think would be appropriate.

Senator HARRIS. And so, as you think about that, as Congress considers appropriating this money, do you have some thoughts about how we can make sure that grant recipients use it in the best way, the most efficient way?

Mr. ROSENBACH. Yes, ma'am. I think you definitely should appropriate it. There's no doubt about that. And a couple options would be something almost like the NIST framework, where it's an agreed-upon framework. You would never try to stipulate specifically what they should do because the diversity of systems is so great, it would never be exactly right. It would also change in two years. That broad type of approach, with some outside technical expertise, may be one option.

Senator HARRIS. Assistant Secretary Manfra, do you agree that there's a certain type of election interference that we should be concerned about, that would target the so-called swing states or those jurisdictions within states that have been identified as perhaps making all the difference in terms of the outcome of a national election. I know we've talked a lot about the diversity and the number of jurisdictions that hold elections. But some perhaps are more pivotal than others, as we have seen.

Ms. MANFRA. Yes ma'am, thank you for your question. While our focus is on the security, not the political dynamics of elections, we do take a risk-based approach to everything that we do with critical infrastructure in terms of how we prioritize. So what we seek to understand is how would the adversary, if their end goal was to—whether that's to sow chaos and discord or to manipulate a voting process—what would be the most likely way that they would do that?

So we would definitely include consideration of that scenario that you described as to how we would think about a risk-based approach to prioritizing, if that answers your question, ma'am.

Senator HARRIS. It is, but so that we can just take it out of the theoretical, there's pretty much consensus about what are the so-called "swing states" and "swing counties." What I really hope and would like to know is that you and DHS has identified those perhaps as being priorities, knowing that foreign adversaries, Russia for example, all they have to do is pick up the paper to figure out where they should target if they actually want to manipulate the outcome of the national election.

Ms. MANFRA. Yes ma'am, we would consider those priorities.

Senator HARRIS. Great. And my understanding is that basically if a State election agency is hacked, you pretty much send out a hazmat team to get right out there on the ground, boots on the ground, and do whatever is necessary to help the State in terms

of getting back up and also figuring out in a forensic way, maybe in an investigative way, what you need to determine in terms of who was responsible, who the perpetrator is, where the specific breaches are and so on. Is that correct?

Ms. MANFRA. Yes ma'am. There's two models. One would be where we know whether the State has—and this is applying our model that we use for all critical infrastructure and Federal networks to states. But one scenario where a State or an entity reports that they have had some type of unauthorized access and they voluntarily request our assistance, our priority then would be, yes, to deploy a team. Sometimes we can do it remotely, but we deploy a team, work with them to gain access to their system, and then our responders would help first identify the presence and how wide scale that presence is.

We need to be careful not to evict them too quickly, because we want to understand completely how much of the network or the systems that they're on. Once we've identified that, then we work with the victim organization to remove the malicious actors from the system and then, importantly, help them get back up and running very quickly.

In other scenarios where we have maybe intelligence or other information, where we think someone may have been a target, but we don't know, we do something that's called a hunt, and that is also voluntary, but we work with that target. Ideally, they would voluntarily let us connect to their system, and we attempt to search for any evidence of that adversary. Sometimes we find them; sometimes we find that they were effective, the entity blocked that potential intrusion.

Senator HARRIS. And if I may, and I'm over my time, but all of that happens, all of that work happens, when and if you have been notified by the State, correct?

Ms. MANFRA. In the former case, it would require notification by the State. In the latter case, it would be usually something from the intelligence community, though it could be from the State or say from the MS–ISAC.

Senator HARRIS. Okay. And—and, Mr. Condos, I think you would agree—that DHS is best able to do its job if there's that kind of notification and cooperation.

Ms. MANFRA. Yes, ma'am.

Senator HARRIS. Thank you.

Chairman BURR. Thank you, Senator.

The Chair would recognize himself, then the Vice Chairman, and then members by seniority. If Senator Heinrich or Collins come back, we will work them in since this is their lead.

Jim, let me ask you a simple question. When you leave here today, are you thoroughly convinced that the United States government does not want to take over the election process of states and localities?

Mr. CONDOS. I am in that position right now.

Chairman BURR. Okay.

Mr. CONDOS. Yes.

Chairman BURR. We have accomplished a lot based upon where we started.

Jeanette, let me ask you. It seems it took a while for DHS to come to a solid estimate about the number—or a solid number about the number of states that were actually targets of Russian attention and activities. The scanning activity ran through the fall of 2016. What's your confidence level in that assessment?

Ms. MANFRA. What I would say, sir, is that, based off of the visibility that we had at the time, which has increased since 2016, but based off of the partnership with MS–ISAC, with states and the intelligence community, we are confident that that 21 number is accurate.

Chairman BURR. I'll ask you a very broad question. Have you seen things running up to the 2018 election, activities that concern you that an adversary might be testing the systems?

Ms. MANFRA. Not at this time, sir.

Chairman BURR. Okay.

Jim, to you and Amy. State election officials reviewed with our staff two of the DHS conference calls with states. One was in August of 2016. What was shared with us was that states say about that call that they didn't understand why DHS was contacting them in August 2016; there was little context to the call or to any threat relayed. Is that what you hear from your members?

Mr. CONDOS. I would say that in the August call, it kind of caught us out of the blue. We knew we were invited to this call, we were on the call, and when Secretary Johnson spoke to us about some of what was going on, we weren't sure what was happening.

When he talked, when he spoke about the critical infrastructure, we really pushed back. I will say that we pushed back. Red states and blue states were pushing back because we were looking at potential for a Federal overreach.

Chairman BURR. So when I suggested to him today that just the mere mention of State elections being under the critical infrastructure, that this was a passionate point for the states, I didn't understate that, did I?

Mr. CONDOS. No, you did not. I will say, though, when Secretary Johnson actually declared, made the designation in January of 2017, it was not until July when we met in East Greenbush, New York, at the MS–ISAC Center, that we actually got a presentation on what critical infrastructure designation was going to be about. Up to that point, we still didn't—so almost a year later, we still didn't know what was happening until then.

Chairman BURR. So I think we would all agree on this committee that communication was poor. Jeanette, you sort of inherited, one, the state of mind that they were in. Eric, you've had an opportunity to look at it as well. And you were tasked with, come up with a plan that solves this.

In the September 17 call, DHS for the first time announced 21 states had been scanned and that State election officials might not know their states were targeted. States told our staff that they felt shocked and waited for one-on-one calls with DHS to find out if they were one of the 21. Many then reported that they were surprised by additional lack of details.

What's changed since then and what assurance can you give the states that not only we're on top of the number, we're confident of the number, and, more importantly, we got a plan in place?

Ms. COHEN. Yes sir. Looking back on some of the lessons learned over the past couple of years, our policy has always been, in order to notify a target or a victim of a potential cyber intrusion, to prioritize communicating with that. In the partnership with the MS–ISAC, which all 50 states participate with and have sensors, the primary interlocutor, I guess we'd say, was usually the states' CIO for the MS–ISAC.

So we prioritize per existing protocol notifying those victims. What we didn't fully appreciate at the time and through those multiple conversations in 2017 in particular, was that just by notifying that victim that didn't necessarily mean that that senior election official who's responsible for that overall administration received that notification.

It was at their request that we undertake that broad notification in September. So while we did notify the potential targets or the victims when we saw the activity, it was notifying those senior election officials and giving them more insight.

The other issue which is always a challenge in cyber incidents or targeting, is we don't always have perfect information. So we prioritize notifying a target even if we in the intelligence community don't fully understand what's going on, because, frankly, by having a conversation, by being able to deploy our incident response teams, it will help the intelligence community and DHS learn more about what's going on.

So when we first notified in 2016, we didn't fully understand what was happening, who was actually targeting those states. We just knew that it was coming from suspicious servers and a company. So now what we have done is, working with the Government Coordinating Council and the representatives, is defining who are those points of contacts. The states provide those points of contacts at the State level, and we have the appropriate mechanisms to ensure that we get that information and.

And again, we're not waiting for clearances. If there's information that we can't declassify, we will provide one-time read-ins to those organizations to ensure that, even if we can't declassify, we can provide them additional context, frankly, even if we're not completely sure at the time.

So those are some of the things that we've improved over the past couple of years.

Chairman BURR. Thank you for that.

Eric, brief question, brief answer. As an outside entity looking at this process, what letter grade would you give us collectively on the progress that's been made based upon the threat that you saw?

Mr. ROSENBACH. That, sir, is a hard question. You know, this is what I would say. I would give you all B, and it's mostly——

Chairman BURR. Not us, but collectively.

Mr. ROSENBACH. But I'm talking about the whole government. In particular, it's a B because DHS in particular over the last year has been working very hard to rebuild that trust with the states and with other organizations so that they can do better. And just working hard can overcome maybe not having a lot of capacity or, coming from DOD, having a $600 billion budget. DHS, they're not like that. But, it's not as good as it should be.

Chairman BURR. I think we all agree we've got more to do.

Vice Chairman.

Vice Chairman WARNER. Thank you, Mr. Chairman.

Let me say I understand probably the concerns that were raised by the states when they got the call from Secretary Johnson. But I think history has shown that designation was correct, and I am appreciative of the recognition. Miss Manfra, you had to receive some of my concerns last June at the hearing, but the notion that we've worked through some of the security clearance issues and that there is this better communication, I want to commend your efforts.

My first question is for you, Miss Manfra, and you, Mr. Rosenbach, and it's a bit of a speculative question. Try to answer fairly brief, though. Which is: We know how vulnerable now our systems were. I know that the Hackathon that took place last year, where virtually every machine was broken into fairly quickly—I had to really raise heck to make sure we changed out machines in Virginia before our election system.

One of the things I've always wondered: With the capabilities that clearly Russia has and the level of sophistication of their cyber activities, the fact that they scanned 20 states and only broke into one. Would you speculate whether their goal was to actually go in and change voter totals in 2016 or whether it was just in a sense to leave digital dust that might then be interpreted as outside interference, that somehow could then be used to stir up dissension and the kind of concerns that Senator Rubio raised about his scenario, which I think was potentially very real? Either one of you want to try on that?

Ms. MANFRA. I could start, sir. I would say that what the Russians were trying to do, which we've talked about a lot, was sow chaos and confusion and discord. And I believe, while—and this is my opinion—that by scanning systems, they were looking for vulnerabilities, they were looking for weak points. And the good news is most of the states deflected it, and I think that's something that doesn't get talked about a lot. But you know, they scanned, they looked for weak spots, and the State systems deflected that.

That doesn't mean that there aren't continued vulnerabilities. But I believe that's what they were likely looking for, is weak spots to get into systems.

Chairman BURR. Mr. Rosenbach.

Mr. ROSENBACH. Yes, sir. I'd start by saying, I've been working in cyber and intel and on the Russians for almost 20 years, and I just don't believe when someone tells me we know everything about what the Russians did or didn't do. So I want to be very clear. I'm not basing this on intel and it is speculation, but I have to be honest: I don't believe that there isn't more to the Russian story, and that they may not have penetrated more than we know right now.

That's always been the case when I've seen these advanced Russian actors, and the GRU in particular, and just like we learned more about them being in the energy grid.

So my fear is that, if you look at the Gerasimov doctrine and the way Putin is now recently re-elected, that this is all about something even bigger, which could be when there's an escalation of tensions and they know they have malware in our grid and they have malware in our election infrastructure, that there will be a threat

and a type of coercion that advances broader national security interests.

So I don't want to sound, you know, shrill, but that's my assessment.

Vice Chairman WARNER. I agree, and I think, again, one of the reasons why the very good work so many members on this committee have done in a bipartisan way to try to help alleviate this issue and lay out specific recommendations.

One of the question I raised on the earlier panel and I want to raise again, Mr. Condos and Miss Cohen, is how do we make sure that your vendors—my understanding was that the Belfer study showed that over 60 percent of American voters cast ballots on a system operator owned by a single vendor. I think it was back in 2012, but there are still these large, large vendors.

How do we ensure that, working with DHS, that they're up to security? Are you auditing that, that they're guarding your voter files in an appropriate way?

Mr. CONDOS. Let me start by just saying that the simple way is that we build it into our contracts with the vendors. So we require them to meet NIST standards. If we're buying new equipment, it has to be EAC certified. So those are the ways that you can do that, is to get them involved in it. But then we also have our own independent security folks that will do penetration testing, will do risk assessments, to determine whether what we've got is what we hope to have to defend, as was pointed out.

So I think many of the states, the idea of putting in stuff into the contract, requirements into the contract, I think that has changed over the last few years. When we first proposed it, we were told, oh, nobody does that. Then, now it's becoming standard, at least in our State for all IT contracts. So we are moving in that direction to try to protect ourselves.

Ms. COHEN. I'd add that many of the changes that we've seen in the election technology space have been consumer-driven over time. And Secretary Condos' point is a good one, that as we educate State and local election officials to better understand what they're putting in their contracts and give them resources like the EAC, like the Belfer resources and others, to make sure that they're putting good things in their RFPs and in their contracts, we will start to see a shift in the vendor area.

Vice Chairman WARNER. My time has expired, but I would also commend my colleagues the work the Belfer Center has done, what Eric has done. On the question around campaigns, these are the ultimate start-ups and huge vulnerabilities. We obviously have a whole segment of our government, the Secret Service, that oftentimes protects candidates. I do think we're going to need best practices and think about how we can put at least best practices out there in terms of protecting campaigns, because this could be a next layer of vulnerability. Having been involved, and probably everybody up here on the panel being involved in campaigns, at least in the past, cyber security has probably been one of the last items you look at as you try to put together—and I commend your good work there.

Chairman BURR. I'm just sitting here thinking. If you thought we saw pushback from State elections officials, I can't wait to see the pushback from campaigns.

[Laughter.]

But I would also agree that they are an extremely vulnerable part of our whole election process right now.

Mr. ROSENBACH. I think they're the most vulnerable. Quite frankly, it's very chaotic, resource constrained, all the things that lead to really poor cyber hygiene.

Chairman BURR. I'm going to turn to Senator Blunt, but as I do that, the likelihood is that when we return from the Easter work period Senator Blunt will then be Chairman of the Rules Committee, where a majority of the Federal statute changes relative to elections will fall. So I thank Senator Blunt for being integrally involved in this process, because he will be integrally involved in the next generation of this as well.

Senator BLUNT. Well, thank you, Chairman. We'll see how that works out. If it does work out, we'll expect to see all of you back and all of you back when we actually look at legislation.

I want to see if I can't cover a couple of topics with the whole panel. One was, you can probably tell—you were all here for the earlier testimony on notification and public notification. As you can tell, we've dealt with this in other areas before and have generally come to the conclusion that public notification was not necessarily helpful and generally not desired by the people you were encouraging to report in.

What's your view of that topic of whether states and local entities are less likely, more likely, helped by some public disclosure that someone attacked your system. Or does that make it a different kind of decision when you report in what you report in and why you report in?

So let's just start, Miss Cohen, with you. Your view of, if we made that or DHS made that, we required them to report when you reported to them?

Ms. COHEN. State and local election officials balance the right to know and transparency with also impacting voter confidence in the system. I can't comment specifically about whether I think they should or should not make it public, but it is a difficult balance for all election officials because the public does have a right to know, as we've discussed throughout this hearing. But balancing voter confidence and not impacting people's confidence in their election system and the outcome is something that has to be taken into consideration.

Senator BLUNT. Mr. Secretary, what are you and your NASS colleagues likely to think about that?

Mr. CONDOS. Well, I'll speak for myself. I won't speak for my NASS colleagues on that. But I think that I will say that, as Miss Cohen has just said, it's a balance between transparency and privacy, and I think we have to be careful about that. I do think that if some of our citizens' information was actually accessed, they deserve to know that.

If it was just a target or a scan—and by the way, I do want to say that it is important that we use the right words. I think during that discussion about the 21 states, they we talked about targeted,

scanned, hacked, breached; and it was a scan or a target, which is similar to a burglar walking up to your house and trying the doorknobs or looking through the windows. I think we have to be careful about how we use those words because they do matter.

So I do think that there's some likelihood that there will be some public announcement if people's information was actually accessed, and I caution that we have to be careful. You also want the incentive to be on the states to notify their partners that things have occurred or may possibly have occurred. And you don't want to have it be a disincentive.

Senator BLUNT. Secretary Manfra.

Ms. MANFRA. I would agree with my colleagues. I think this isn't just an issue just for this sector. It's across all sectors. We very much would like them to voluntarily report incidents to us, particularly if we've published a document asking industry to look or State and locals to look for indicators of compromise, and let us know, because that just benefits everybody. It benefits the government, it benefits our defense.

I would say, as far as publicly talking about it, I agree that individuals have a right to know when their information has been stolen or tampered with, and a lot of states have different laws governing that. I do think we always have to balance, as Ms. Cohen noted, the public confidence in our system.

Also, as I mentioned before, often you know the fact of an incident, but you don't know everything about it, and you don't know what was taken, you don't know all these different pieces around who did it; and it's hard to convey a lot of that nuance publicly.

So I know it's complicated, it's challenging. I look forward to continuing to work with you on this issue, but I guess I would prioritize notification to the Departments over public notification.

Senator BLUNT. I might point out here, too, that, in case anybody is paying attention to this, the information in your voter registration file usually is not nearly as extensive as the information in lots of other files. So your Social Security Number, things like that, that we've seen large segments of information be accessed improperly, the voter registration file doesn't have a lot of that in it.

Let's get a final response.

Mr. ROSENBACH. Yes sir. I'll be real quick. I would say it matters most if it's a compromise. If it's a compromise, it's something different. That definitely requires disclosure to the Hill for certain, and I think you have to disclose it to the public. And here's why. You all know this. It's almost impossible to keep a secret, and when something like that comes out in a leaked way it undermines the public's confidence in the government and what they're doing. So, although it's very hard, I think you just have to err on the side of publicly communicating about these things and giving as many facts as possible and doing that over and over.

Otherwise, you create a new seam for the Russians to try to get in and sow this disinformation.

Senator BLUNT. It would be another area where how you define "compromise" matters, too. Was information shifted around, people have reason to believe they're going to be directed to the wrong place, anything like that, as opposed to there was an attempt to get into this information, we are confident that attempt failed, but we

want to report it because other entities might also be having the same kind of attempt.

At some point—we don't have time today, but the whole idea of the audit system, the paper trail, all of those things and who is doing that, who's not, provisional voting, things that can give voters some sense that, no matter how many of these things go wrong, they on election day are going to be able to cast the ballot they intended to cast and without a government that stands in the way of doing that.

Thank you, Chairman.

Chairman BURR. Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman.

Ms. Manfra, to just recap a little bit from this morning, I talked with Secretary Nielsen about the 43 percent of Americans who vote with voting machines that researchers say have serious flaws, including backdoors, which would make them obviously susceptible to frauds and hackers. She claimed, to her credit, that this is now a national security problem. She said best practices are paper ballots. That's encouraging.

I just want to go a little bit further, and I think this is an area that might be part of your expertise. So I've written to the major manufacturers of the voting machines to get basic answers to their cyber security practices. I asked, for example, if they employ cyber security experts, if there were audits and if they had ever been hacked.

Most of the companies have just been stonewalling. So this is how almost half of America votes. There is essentially no accountability over these companies.

My first question would be: If the voting machine companies do not employ cyber security experts and they don't have independent audits of their products, how confident are you that the election technology they sell to the states follows cyber security best practices?

Ms. MANFRA. Sir, I'll do my best to answer those pieces. While we've been talking a lot about our work with the State and local entities that administer our elections, we have also worked with the industry that supports election officials, most recently setting up a sector coordinating council, which—it allows us to use our critical infrastructure partnership authorities to have non-public conversations with industry on security issues.

Those manufacturers and others are participating in that. Our partnership with them is more nascent than with the State and locals, as my colleagues have talked about the importance of State and locals and, frankly, businesses everywhere in ensuring that they require cyber security best practices for their vendors is important.

I can't comment on the specific statistic. I'm not familiar with that statistic.

Senator WYDEN. You don't have to comment. The question is, though, ma'am, how confident are you as of this afternoon that the election technology that they're selling to the states follows cyber security best practices?

Ms. MANFRA. Sir, it's just hard for me to judge right now. I don't have perfect insight into the machines that the states buy. What

I can tell you is that many of those manufacturers have submitted their equipment through a voluntary compliance process, run by the EAC and NIST and now DHS, that includes things like a code review—so they've voluntarily submitted those for compliance. And that many states use whether it's a voluntary voting standards, guidelines or similar mechanism for assuring the security of those systems, whether they mandate it or they do it voluntarily.

I can also tell you that many of those machines that researchers say have vulnerabilities or other issues, that those can only be exploited when an individual has physical access to those machines. And election officials have other mechanisms that they've put in place to ensure that that physical access is not possible.

Senator WYDEN. Well, let me be——

Ms. MANFRA. Yes sir.

Senator WYDEN. Let me be specific on it. There have been press reports that that biggest company actually stipulated that remote access software be installed in the machine. Now, if that's correct—and that's why I very much want your agency to get back to us. I think my time is almost out. I would like to have you get back to me with a written response to my question, of how confident you are that this technology they sell to the states follows best practices.

I heard about the voluntary certification and the like, because when you read press reports that the biggest seller of voting machines is doing something that violates Cyber Security 101, is actually directing that you install remote access software which would make a machine like that a magnet for fraudsters and hackers and the like, you say, "Boy, we've got to really beef up what we're doing."

The Secretary, to her credit, said,"Hey, this is a national security, you know, issue." She wants best practices, to include paper ballots.

Can you get back to me with an answer within a week with respect to how confident you are of the technology they sell as following best practices?

Ms. MANFRA. Yes sir, although if I could add, remote access software is only useful to an attacker if there is an internet connection, which the states do not allow. But I will absolutely get back to you, sir.

Senator WYDEN. If the press reports are talking about it, I think we ought to at least get an assessment from you——

Ms. MANFRA. Yes, sir.

Senator WYDEN [continuing]. With respect to how confident you are.

Ms. MANFRA. Yes, sir.

Senator WYDEN. Thank you, Mr. Chair.

Chairman BURR. Jim, you look like you maybe wanted to comment on that. Do you?

Mr. CONDOS. Thank you. Going by the press reports, the press reports initially stated that there was remote access software, but I believe there was a follow-up from perhaps that software company that—or the machine company—that said that they don't use that. That was something that was done at one time, but is not any longer used.

Senator WYDEN. Well, let's just hear from Ms. Manfra and that would be in writing within a week, and we'll go from there.

Thank you, Mr. Chairman.

Chairman BURR. Senator King.

Senator KING. Thank you, Mr. Chair.

Mr. Rosenbach, I want you to be shrill. You said you don't want to be shrill. I want you to be shrill. Tell us in 30 seconds about General Gerasimov.

Mr. ROSENBACH. General Gerasimov believes that the most powerful weapon you can use is information combined with——

Senator KING. He's a Russian general, right?

Mr. ROSENBACH. He was the second ranking person on the Russian general staff. I'll tell you a story about this. You know, I used to be in charge of cyber at the Pentagon and there was a time when we actually talked to the Russians and the guy I was talking to was a three-star, he was like the number three ranking guy in the Russian military.

He was taunting me, because he said, "You guys are so dumb; you're building a Cyber Command that doesn't even have information operations and information operations is the way that you take a country down."

Senator KING. And they in fact hacked the Pentagon, they hacked the White House, they hacked the Joint Chief of Staff, they hacked the Democratic National Committee. I mean—I don't believe we're—you're grading on a curve, man. You said it was a B. I think you're giving us too much credit.

Mr. ROSENBACH. It's a B for effort, but that doesn't mean that we can sleep well.

Senator KING. Yes. Where I come from, effort doesn't count.

Mr. ROSENBACH. No, but it doesn't mean you can sleep well. I mean, the Russians, remember, they're very good, which means they have capability, and they're mean, and they have interests that are directly opposed to the United States, so they have motive. Those are the two things you look at.

Senator KING. Mr. Condos, welcome from Vermont. We in Maine think of Vermont as the West Coast of New England. We're glad to have you here.

I understand that in Senator Lankford's bill originally there was a red team provision—you heard me describe that—that would have had a hacking team at DHS or somewhere practice; and that the states furiously opposed this and that it was dropped out. Is that true?

Mr. CONDOS. I am not aware of it being—I can't answer that. I don't know if that was true or not.

Senator KING. Do you think it would be a good idea?

Mr. CONDOS. I think many of the states, if not all of the states, are going through penetration testing already, which is I think the same thing as what you're talking about, is professional folks who try to hack into your systems. We're already doing it. We've done it already in Vermont and we are continuing to do it as we go.

Senator KING. Well, I just hope it's being done at the highest possible level, because I understand there was a so-called Hackathon last summer where every State or every State that they tried, they

managed to penetrate. The results were devastating. So, I just hope that this is something that's really been taken seriously.

I just worry. I have to say, I just have to worry that there's an overconfidence here in terms of the sophistication of our adversaries.

Mr. CONDOS. If there was a hack last year that hit 50 states, the 50 states don't know about it.

Senator KING. I don't know about 50 states. It was a number of states. I don't know if it was 50 states.

Also, you mentioned that you thought one of the strengths—and frankly, I thought this, too—of our system was that it was so decentralized. Do you know how many election system vendors there are, anybody?

Mr. CONDOS. I do not know how many vendors there are.

Senator KING. Does anybody know?

[No response.]

My sense is that there are not very many, and that they're getting fewer, fewer and fewer all the time.

Anybody know how many election systems have foreign owners?

[No response.]

No?

Ms. MANFRA. Sir, I don't have it with me, but we can get back to you.

Senator KING. Could you get that for us, yes?

Ms. MANFRA. Yes, sir.

Senator KING. That's just what I was going to ask you. If you could——

Ms. MANFRA. Yes, sir.

Senator KING [continuing]. Give us a report on how many vendors there are and what the ownership structure of those vendors are.

I think a point that's been made that ought to be reiterated: They don't have to change votes to win; they just have to sow lack of confidence, and people lose confidence in the electoral system, they lose confidence in the democratic process.

We haven't talked too much about registration lists or election night reporting. What if they hack into that system and the election night reporting turns out to be all wrong the next morning? That would be rather chaotic. So I think that's something.

I understand the issues of transparency, but I think we have to understand that they don't have to actually get in and change votes in order to achieve the result that they're seeking.

Mr. Rosenbach, do you agree with that?

Mr. ROSENBACH. Yes sir. I was just going to say they've done that. They did that in Ukraine. They hacked the web page used to publicly announce the final vote, used misinformation, and Ukraine was left in chaos for days afterwards trying to figure out who won. So we need to look at that playbook. They will do it to us.

Senator KING. So it could be—we're not necessarily talking about voting machines not connected to the internet. How about the lines from the Associated Press to CNN, because it may be that that may be a place where there could be mischief.

Ms. MANFRA. Yes sir. And I know we've focused mostly on voting machines, but that is not our exclusive focus. We're concerned

about the entire process, as Secretary Nielsen outlined, everything from registering to the final certification of the vote.

And as former Secretary Johnson talked about, the Associated Press engagement. We remain focused and thinking about if an adversary is trying to undermine confidence, what are the ways to do that? We've published best practices on voter registration systems. We've worked with states on everything from voting machines to election management systems, which can include tallying, how we secure the secretary of state website, how we think about unofficial election night reporting, how we think about crisis communications, if there is misinformation on the day of an election or immediately following.

So we are trying to take a very holistic approach and not just thinking about voting machines. In fact, using this risk based approach to it and thinking about the difficulty in actually trying to manipulate a vote itself is why we prioritize engagement on those systems that are connected to the internet, like voter databases and others, that could cause that misinformation issue.

Senator KING. Thank you.

I know I'm out of time, but, Mr. Rosenbach, yes or no: Do you agree with the contention that we, this country, aside from all of these defensive measures, needs to develop a cyber deterrence strategy in order so that our adversaries know that there'll be a price to be paid for these kinds of incursions?

Mr. ROSENBACH. Yes sir. I could not agree more strongly at all.

Senator KING. Thank you.

Thank you, Mr. Chairman.

Chairman BURR. Senator Collins.

Senator COLLINS. Thank you Mr. Chairman.

Secretary Manfra, Senator Heinrich and I wrote a letter to the Department asking specifically whether or not you needed new statutory authority or funding in order to help State election agencies and ensure the integrity of our elections systems and the voting process. I personally am surprised that the Department has not been more proactive in that area in submitting requests to the Congress.

What is your answer to that question? Does DHS need additional authorities or additional funding in order to assist states and ensure the integrity of our voting systems?

Ms. MANFRA. Yes, ma'am; thank you for the question. On the authorities piece, we have the authorities we need right now to do our job. Thanks to the work of this committee and the Homeland Committees, frankly, over the last few years, we have very broad authorities that we can apply.

We're continuing to build the capacity and the capability to fully execute those authorities. We have reprogrammed money. We have reprioritized money. That does mean that we have had to lower the prioritization of other entities receiving our services, whether those were Federal or other critical infrastructure, but we felt it was appropriate for the risk. We have spoken with appropriators and others to ensure that we do have the resources that we need to continue to prioritize elections in addition to our other missions.

Senator COLLINS. Well, you certainly need to prioritize elections, but you also have to be cognizant of other critical infrastructure

such as the power grid and natural gas pipelines. So more specifically, are you going to and have you requested additional funding to ensure the integrity of our elections?

Ms. MANFRA. Yes, ma'am, we have spoken to the appropriators and requested additional.

Senator COLLINS. And how much additional funding have you requested?

Ms. MANFRA. Approximately $25 million.

Senator COLLINS. Well, I would note, Mr. Chairman, that I believe the bills that many of us have co-sponsored called for far more funding than that, like $386 million; and I know you've worked hard to get it into the omnibus bill.

Secretary Condos, I apologize for being out for part of your testimony and much of the Q and A due to another commitment that I have. It's my understanding that, at least until recently, you've been pretty disappointed with the level of communication between the Department and your office. I'm curious whether you're one of those lucky 21 of the 150 State election officials who has received a security clearance.

Mr. CONDOS. First, let me say yes, I have received my clearance, so I'm fully cleared at this point.

Secondly, I will say that I'm not sure that that's being lucky or not.

Senator COLLINS. I was being facetious actually.

[Laughter.]

Mr. CONDOS. But I think that the communication levels between the states and Department of Homeland Security have improved greatly, specifically in the last six months, and I think we're on the same page and we're working to secure our election systems.

Senator COLLINS. Finally, let me ask you: State election officials have expressed apprehension about the risk that being too public about the threat that we face might provoke exactly the impression that they're endeavoring to dispel, that is, that the Nation's voting systems are insecure and subject to compromise, and thus may help the Russians and other foreign adversaries achieve their goals.

I would note, to counter that, that when the French and the Germans made very public what the Russians were trying to do in their elections, it had a beneficial impact on the public, and the public was much more weary of fake news stories or other issues.

In your view, how do we strike the right balance for public communications concerning threats to our election infrastructure?

Mr. CONDOS. As far as the threats themselves, I think that we should be communicating with the public to let them know what's going on. I will say that in our State we are right now preparing for an early April cyber summit that we're going to do in Vermont for the media, for the public, for our legislature, so that they are fully aware of what is going on and where we are going and how we are set up to fend off in the attacks.

I think it's also very important to know that the bad actors that tried to hack us yesterday are going to try a different way today and they're going to be different tomorrow. They evolve probably—not probably. They evolve far quicker than any government can set up. So what you need to do is make sure that you have the proto-

cols in place, that you have the processes in place, and that you have the defenses in place, in hopes to be able to fend those off.

No computer, no computer, is safe from a hack. Every computer can be hacked if it's out there. What you want to do is make sure you have the proper defenses in place.

Senator COLLINS. Thank you.

Mr. Chairman, thank you, and Vice Chairman, for this excellent hearing. My final message to DHS is again to stress the urgency. Everyone seems focused on the November hearings. We're having elections right now. We're having the by-elections, we're having special elections, we're having primaries coming up now. We can't wait. We can't just be focused on November.

Thank you Mr. Chairman.

Chairman BURR. Thank you Senator Collins.

We have exhausted the questions. I'm going to turn to the Vice Chairman briefly.

Vice Chairman WARNER. I want to first of all thank the panel. I want to echo what Senator Collins has said, but I do think, echoing what has Eric said, there's been some progress. At least there is a recognition of how significant it is.

I think in the omnibus, because of the work frankly that has been done by members on this committee, that some of the resources that our State partners are looking for will be there. We're going to want to see regular milestones on how we move forward on that.

I want to echo what Senator King has said. We've spent a lot of time in closed sessions on this, and that is the need for our country to have an articulated cyber doctrine. I think that's going to raise a lot of tough questions. I think it's going to raise questions about where does the responsibility lie to report and how far down does it go.

It may raise questions around the whole question of software liability, which has been an area that has been not talked about for years. But in this new realm with the level of vulnerabilities we have, it may have to be explored.

Again, I know I gave Secretary Manfra some challenging times last year, but this question, not just with election security, but across the government, of the slowness of getting security clearances. We had a good hearing on this again yesterday. We had a public hearing a couple of weeks back. This just has to be a higher priority. We're 700,000 in arrears. We've got only a few of the election security officials. I would argue, frankly, we need Fortune 1,000 chief security officers to have security clearances as well. So a lot of work to be done.

I do want to just close before I turn it back to the Chairman, though, and not all of the members are here, but thank all of those members particularly from both parties who have worked so diligently on putting together a legislative effort that I'm proud to cosponsor, that I think shows the kind of commitment of this committee to not only investigate looking backwards, but to also try to lay out some solutions sets going forward.

I would point out again, yesterday at the press conference we had on this we had virtually every member of the committee at-

tending, and that's a credit to the good work of a lot of folks on this committee.

With that, thank you Mr. Chairman.

Chairman BURR. I thank the Vice Chairman and, more importantly, I thank this panel. You have provided us some great insight, not just today, but on an ongoing basis, and we're grateful for that.

I will note at this time that the Lankford-Harris legislation is not legislation from this committee, but it is important legislation. And there's others out there, and Senator Blunt and probably Government Oversight will jurisdictionally have pieces of it. I have joined Senator Warner in co-sponsoring the legislation now that we've finished this portion of our investigation.

I want to thank each of you for being here. In 2016, states faced a threat they never expected to confront: a hostile nation seeking to invade networks essential to the functioning of our democracy. While our collective insight is still limited and based in large part on states' self-reporting when they saw a problem, the committee has found that the actual damage was limited. No votes were changed and only one State reported an actual penetration of voter registration database.

Still, given the capabilities and the intent of Russia and other potential cyber adversaries, the lack of resources available to most states, the committee remains concerned about potential future attacks. States should not be asked to stand alone against a nation.

We heard today from DHS how they learned, course-corrected, and have become a true partner with the states. We commend you for that. DHS needs to continue to rise to the challenge, with more resources if needed; and they need to tailor their assistance to where the State needs are.

We've heard from NASS and NASED how the states feel about suddenly being in the cross-hairs of a hostile foreign power. We've also heard what states need to do to secure their election systems. Our witnesses lined up today made clear the strength of decentralized vibrant election systems at the State and local level, paired with capability and resources at the Federal level.

However, we also need to have in place a solid deterrent, a deterrent to activities like this in the future. Any hostile power who seeks to undermine the fundamental structures of our democracy should be prepared to pay a hefty price.

The close of this hearing concludes chapter one of our committee's investigation. I believe we've shown through our work today and over the past year that these issues go beyond party politics. We may disagree on some things, but we all agree on this committee that we must take steps to ensure elections are secure. We've investigated and uncovered the full scope of a sobering threat. We now hand this over to the Rules and the Government Affairs Committee to consider legislative approaches within their jurisdiction.

I'd also like to take a moment to thank the committee staff for their work. The staff involved in this effort has worked tirelessly with few days off over the last 14 months in a politically charged and demanding environment. They are talented, they are professionals, and they are focused, and they have done outstanding

work for the committee and, more importantly, for the American people. While their names won't be on the report and probably and hopefully will never be released publicly, they should know just how much we appreciate their hard work and how beneficial this has been to states, localities, and to the American people.

Once again, thank you for your testimony today. This hearing is adjourned.

[Whereupon, at 12:37 p.m., the hearing was adjourned.]

Supplemental Material

U.S. Senate Select Committee on Intelligence

Hearing on Election Security Testimony
Wednesday, March 21, 2018

Good morning Mr. Chairman, Mr. Vice Chairman and distinguished members of the committee. Thank you for the opportunity to offer testimony this morning.

My name is Thomas Hicks. I am the Chairman of the U.S. Election Assistance Commission, better known as the EAC. The Commission was established by the Help America Vote Act (HAVA) and is a bipartisan, independent federal agency tasked with helping election officials and the voters they serve.

Our mission is as critical now as it has ever been, in part because it is difficult to identify an area of public service that has changed as much as election administration in the past 15 years. Against the backdrop of voters who expect more 'on demand' service, election officials have to keep pace with emerging technology, evolving election and access policies, enhanced security protections and new industry standards.

The election official of today is also expected to do more with less and have the industry knowledge of a variety of different fields in order to pull off the logistically demanding task of administering an American election. For example, election administrators have always had the challenge of working with the press as well as a public relations professional, understanding poll worker recruitment and training as well as a human resources manager, knowing mail regulations and schedules as well as the postal service, and identifying accessible and legal polling places as well as any city planner. Increasingly, however, election officials must also be information technology experts, as many election officials manage larger numbers of complex information systems, data, vendors and technical staff than any other department within their jurisdiction.

Election officials also operate under a tremendous amount of pressure. They have one chance to administer an election and ensure that it accurately reflects the will of the voters they serve. There is no margin for error. Election officials must get it right every time.

While election officials are at the heart of this work, the EAC provides considerable resources to state and local election officials looking to strengthen their ability to prevent, detect and recover from potential cyber-attacks. For as long as we have had elections, there have been threats to the election process. Election officials have long developed protections and procedures to ensure integrity in our elections.

Election security, both physical and technological, is not a new concept for election officials. Since the implementation of electronic voting systems and statewide voter registration databases more than a decade ago, election officials have focused on ways to better secure the election process.

One crucial way the EAC does this is through our Testing and Certification program that ensures voting machines are tested against the most up-to-date standards possible. The most recent

version of these standards, the Voluntary Voting System Guidelines 2.0, were adopted by the EAC's Technical Guidelines Development Committee in September 2017. The new voting system testing guidelines will be previewed at our Standards Board and Board of Advisors meetings next month and then will come before the commissioners for adoption. Once released, these guidelines will be the most comprehensive set of standards against which voting systems can be tested in the United States.

The EAC also provides IT management training focused on the mindset, knowledge base and resources needed by election officials to manage their dependent, yet disparate systems. The EAC works with individual states and jurisdictions to mold the class to each audience's specific and unique needs. The EAC has conducted these trainings in eight states in the last twelve months alone, with at least two more planned this year.

Another important part of the EAC's work is to educate the public about election security. Three weeks ago in San Antonio, we premiered a short video explaining the complex and multi-layered security measures in place to protect elections. It is our hope that understanding the steps election administrators use to secure elections will bolster voter confidence, and I would be happy to provide members of this committee with a link to the video and its accompanying presenter materials.

As a key component of the EAC's HAVA-mandated clearinghouse responsibilities, the Commission also provides a wealth of other resources to help election officials. These include best practices guidance, election preparedness checklists, election database support, guidance on contingency planning, and more. The Commission recently expanded on the secure voting system procurement help it already provides election officials and developed new cyber incident response planning tools for jurisdictions. In addition, as election officials evaluate election technology purchasing decisions, the EAC provides request-for-proposals development guidance. We also produce cybersecurity documents and plans, as well as host forums to bring cybersecurity experts together with election officials.

Increasingly as part of this work, the EAC has ensured election officials are able to draw on the expertise and intelligence of other federal agencies.

Following the Critical Infrastructure designation, the EAC acted as an intermediary to help DHS officials better understand elections and the most impactful ways to help election administrators protect U.S. elections from cybersecurity threats. The EAC also ensured that state and local officials had, and will continue to have, a voice at the table as DHS works to further develop the critical infrastructure subsector that will support election systems.

Last summer, the EAC convened an Election Infrastructure Subsector Working Group, consisting of state and local election officials, to meet with DHS Critical Infrastructure staff. That group led to the successful establishment of the Elections Government Coordinating Council, or GCC, in October 2017, and the EAC was a key driver in its successful launch. The GCC will establish information sharing protocols between election officials and DHS on issues, such as cyber and physical security, and are currently drafting a sector specific plan. The EAC's

Chairman serves on the executive committee of that group, its Vice Chair serves as an official member of the committee, and the third EAC commissioner serves as an ex-officio.

The EAC has also routinely invited members of the Department of Homeland Security to speak at roundtables, public meetings, and most recently, the EAC Summit for election officials in January of this year. Next month, representatives of DHS will also speak on panels about election security at the EAC's Standards Board and Board of Advisors meetings. These opportunities have been natural outgrowths of the relationship between the EAC and DHS.

I conclude my brief remarks today by assuring you that American elections are administered by dedicated and masterful project managers who go above and beyond their responsibilities to increase the security, accessibility, and efficiency of our systems. The EAC will continue doing all it can to provide support to election administrators as they work to ensure American elections have integrity and deliver results that reflect the will of the people.

I thank you for holding today's committee hearing to examine an issue of critical importance, and I look forward to answering the Committee's questions.

○