



Uploaded to the VFC Website

▶▶▶ 2019 ◀◀◀

This Document has been provided to you courtesy of Veterans-For-Change!

Feel free to pass to any veteran who might be able to use this information!

For thousands more files like this and hundreds of links to useful information, and hundreds of "Frequently Asked Questions, please go to:

[Veterans-For-Change](#)

If Veterans don't help Veterans, who will?

Note:

VFC is not liable for source information in this document, it is merely provided as a courtesy to our members & subscribers.



A person wearing a dark suit jacket and a light-colored shirt is shown from the chest down, placing a white ballot into a brown cardboard ballot box. The background is a solid dark blue.

Nextgov

ELECTION SECURITY **TESTED**

Federal agencies raced to secure vulnerable systems in time for the 2018 midterms, but the job's not done.

NOV 2018

Introduction

We've learned a lot about election security in the two years following the 2016 presidential election, and most of it is not confidence-instilling. U.S. voting systems, like any other electronic systems, have vulnerabilities.

In the months following the election, the intelligence community concluded a foreign power meddled in our election while the tech companies that oversee important social media platforms did little to identify or stop a large foreign influence campaign. The U.S. imposed retaliatory sanctions on Russia and Special Counsel Robert Mueller charged 13 Russian nationals and three Russian companies with crimes related to the hacking. But that's the past, focus had to shift to preventing future attacks for the 2018 midterms.

Federal agencies and state, local and county partners had to work on building strong working relationships to share pertinent threat information with each other. The Homeland Security Department, for example, stood up an Election Day chatroom where local election officials could flag unusual behavior or issues in real time. The midterms brought only false alarms, but securing elections is a marathon, not a sprint.

In this ebook, we look at the issues that need continued attention.



Frank Konkel
Nextgov Executive Editor

Lenovo™



DATA PROTECTION GOVERNMENT CAN RELY ON TO BETTER SERVE ITS CITIZENS.

Lenovo provides the technology required to protect the confidentiality, integrity, and availability of government data.

Learn more about Lenovo's government solutions [here](#).



Contents

What Hackers Found Probing U.S. Voting System.....5

JOSEPH MARKS

Government's Relationship With Social Media is Still Complicated.....8

JACK CORRIGAN

Trump Administration Preps Sanctions Against Foreign Election Interference.....11

JOSEPH MARKS

DHS Cyber Unit Fields False Alarms But No Hacks on Election Day.....14

AARON BOYD

An Overlooked Threat: Online Ballots.....17

JOSEPH MARKS

After Midterm Elections, a Focus on Securing Campaigns.....19

JOSEPH MARKS

What Hackers Found Probing U.S. Voting Systems

The report from DEF CON's Voting Village found one bug that alone could flip the Electoral College. Another has gone unfixed for 11 years.

By Joseph Marks

The number and severity of hackable vulnerabilities in voting machines across the U.S. is "staggering," according to a report from computer security researchers at the DEF CON cybersecurity convention, which took place in August in Las Vegas.

Among other vulnerabilities, the [report](#) cites a voting tabulator that can be remotely hacked and is in use in 23 states.

"Because the device in question is a high-speed unit designed to process a high volume of ballots for an entire county, hacking just one of these machines could enable an attacker to flip the Electoral College and determine the outcome of a presidential election," the report states.

Another vulnerability, which was present on voting machines used in 2016, contains a vulnerability that was first disclosed to the public in 2007, the report states.

The report was released during a conference in Washington. Rep. Jackie Speier, D-Calif., who opened that conference, criticized

voting machine companies for not allowing ethical hackers to probe their machines for vulnerabilities.

"The veracity of our voting system has been inadequate for a very long time and we have not taken it seriously," Speier said.

Speier called the conference one of the "two most important things happening in our country," a reference to the Senate Judiciary hearing focused on sexual assault allegations against Supreme Court nominee Brett Kavanaugh happening at the same time.

Congress [allocated](#) an additional \$380 million for states and localities to improve election systems earlier this year.

Homeland Security Department officials have said that funding is likely [insufficient](#) for all the necessary upgrades and many upgrades will not be complete before the 2018 midterms.

The DEF CON report cites vulnerabilities produced by the supply chain for voting machine parts, which is "global and has essentially no



📷 A child watches as a polling worker waves over an early voter to an open booth at the Franklin County Board of Elections, Monday, Nov. 7, 2016, in Columbus, Ohio./ John Minchillo, AP file photo

process identifying what sources machine parts come from.” That opens up the possibility of malware or spyware implanted by U.S. adversaries, the report states.

State and local election officials often claim that critical voting functions are “air-gapped,” meaning they’re not accessible via the internet, but DEF CON hackers were frequently able to remotely access those systems, the report found.

In one case, hackers found a vulnerability affecting an electronic card that millions of Americans use to activate voting terminals that could be remotely reprogrammed with a mobile phone.

Ethical hackers [found](#) a similarly broad slate of vulnerabilities during the 2017 conference. [N](#)

SECURE YOUR ELECTIONS WITH AKAMAI AND DLT



Interested in protecting your infrastructure this election season at no cost? Akamai will work with your current security infrastructure to help protect your elections network from the following threats:

Phishing: Allowing employees to unknowingly access phishing links

Data Exfiltration: Exposing sensitive data and credentials to foreign and domestic hackers

Malware: Allowing malware to access external command-and-control servers and tampering with elections data

Ransomware: Succumbing to ransomware attacks and networks being held hostage until payment is made



TOP CONTRACTS



Government's Relationship With Social Media is Still Complicated

Facebook and Twitter executives are open to the government helping them stop foreign influence campaigns, but it's unclear what that would look like.

By Jack Corrigan

Despite the strides Facebook and Twitter are making in stopping foreign actors from manipulating their platforms, executives recognize the companies can only get so far without the government's involvement.

But with Russia, Iran and other adversaries working to sway the upcoming midterm elections, lawmakers are urgently trying to figure out what that role should entail.

"The era of the Wild West in social media is coming to an end. Where we go from here is an open question," Senate Intelligence Committee Ranking Member Mark Warner, D-Va., said Sept. 5.

Testifying before the committee, Twitter CEO Jack Dorsey and Facebook Chief Operating Officer Sheryl Sandberg owned up to their companies' failure to stop Russian actors from using their sites to meddle in the 2016 election. Since then, executives told lawmakers that their organizations made technical and policy changes to significantly curb nefarious activity on their sites.

Sandberg said Facebook blocks millions of attempts to register fake profiles every day and disabled nearly 1.3 billion illegitimate accounts worldwide between October and March. Twitter similarly now challenges some 10 million accounts suspected of deceptive activity every week, more than triple the weekly investigations in September 2017, Dorsey said.

But while platforms step up their game, so too do the foreign actors trying to manipulate them, and Chairman Richard Burr, R-N.C., reiterated that many of the vulnerabilities that allowed misinformation operations to thrive remain unaddressed.

"We have identified the problem—now it's time to identify the solution," he said. "Whatever the answer is, we've got to do this collaboratively and we've got to do it now."

Lawmakers took turns grilling panelists on what those solutions might look like.

Both executives expressed support for Warner's proposal that users should know when they're interacting with bots or otherwise

“I would urge both your companies or any company like yours to consider whether or not they want to be partners in the fight against our adversaries ... as opposed even-handed or neutral arbiters.”

SEN. TOM COTTON, R-ARK.

automated accounts, but Dorsey noted Twitter still struggles to identify more advanced fake accounts. Sandberg also agreed that Facebook has a “moral and legal” obligation to remove accounts that incite violence and didn’t oppose Warner suggesting platforms that don’t do so could face sanctions.

They also both told Sen. Ron Wyden, D-Ore., they see personal data rights as “a national security priority” and would support efforts to strengthen protections.

Dorsey said increased information sharing with federal law enforcement would improve Twitter’s ability to combat influence campaigns. More regular meetings with government officials would help Twitter act faster on the latest manipulation efforts and having a single point of contact in government would save

the company time collecting information from multiple agencies, he said.

But he implied there would be limits to the data Twitter shares back with government. After Sen. Tom Cotton, R-Ark., questioned the company’s decision to limit the intelligence community’s access to data, Dorsey said Twitter has a global policy against supporting constant surveillance.

“I disagree with any imperative to be consistent between the government of China and Russia on one hand and the government of the United States on the other,” Cotton said. “I would urge both your companies or any company like yours to consider whether or not they want to be partners in the fight against our adversaries ... as opposed even-handed or neutral arbiters.”




Twitter CEO Jack Dorsey, accompanied by Facebook COO Sheryl Sandberg, testify before a Senate Intelligence Committee hearing on Capitol Hill. / Jose Luis Magana, AP

While social media platforms and lawmakers work to hammer out what Sandberg called “the right regulation,” both parties need to keep in mind misinformation campaigns can impact far more than just elections, said Megan Stifel, a nonresident senior fellow at the Atlantic Council and former international cyber policy director for President Obama’s National Security Council.

“We obviously should tackle what’s happening with elections, but we need to talk about how to combat other malicious misuse of these platforms for other public policy concerns,” she told *Nextgov*. “We need to think broadly how to address this problem.”

One approach she suggested would be consolidating the practices Twitter and Facebook have implemented into a set of policies that could apply broadly across platforms.

“Working with the companies, I think the government needs to figure out where the appropriate line is,” she said. “If after the midterms it becomes even more clear that what the companies have done still is not enough, I suspect ... that will change the dynamic.” 

Trump Administration Preps Sanctions Against Foreign Election Interference

The executive order describes a process for sanctioning digital interference, propaganda and any other efforts to meddle in U.S. elections.

By Joseph Marks

Nations, organizations and individuals that attempt to influence U.S. elections will face a slate of sanctions under an executive order signed by President Donald Trump Sept. 12.

The order, which does not name particular countries, includes both digitally tampering with elections or campaign infrastructure and the sort of digital disinformation campaigns that Russian agents launched on social media in advance of the 2016 presidential contest.

The order is primarily designed to assess interference and design sanctions after an election is concluded but could also be used to impose sanctions if there's evidence of interference during an election campaign, National Security Adviser John Bolton told reporters during a conference call.

"This is intended to be a very broad effort to prevent foreign manipulation of our electoral process," Bolton said.

The order directs the intelligence community to launch a 45-day review after each election

for evidence of foreign interference. Anything the intelligence community finds would then be forwarded to the Justice and Homeland Security departments for another 45-day review.

If Justice and Homeland Security determine there's genuine evidence of interference, they'll forward that information to the State and Treasury department for sanctions.

Those sanctions could include blocking foreigners' property in the U.S. and limiting their right to export to the U.S. and access to U.S. financial institutions, Bolton said. The order also directs State and Treasury to develop a system to calibrate how significant the interference is and what sanctions would be appropriate, he said.

The public would most likely learn about the meddling after sanctions are imposed, Bolton said, noting that evidence of the meddling is likely to come from highly classified sources that could burn intelligence sources and methods if it was revealed.

“We must make sure Vladimir Putin’s Russia, or any other foreign actor, understands that we will respond decisively and impose punishing consequences against those who interfere in our democracy,”

SENS. MARCO RUBIO & CHRIS VAN HOLLEN

The order comes less than two months before the 2018 midterm elections and after nearly two years during which Trump has failed to consistently acknowledge Russian interference in the 2016 contest.

Bolton insisted that Trump’s wavering on Russia’s 2016 interference and criticism of his unusually friendly relationship with Russian President Vladimir Putin had “zero” influence on the new sanctions authority.

“The president has said repeatedly that he is determined that there not be foreign interference in our political process ... and today he signed this executive order, so I think his actions speak for themselves,” Bolton said.

The order is weaker than some legislative efforts, including the Cyber Deterrence and Response Act, which passed the House in early September and would impose automatic sanctions for election meddling.

A Senate companion to that bill has not been marked up yet.

Another bill, the Defending Elections from Threats by Establishing Redlines, or DETER, Act would also impose automatic sanctions.

That bill’s sponsors, Sens. Marco Rubio, R-Fla., and Chris Van Hollen, D-Md., praised the Trump order for “recogniz[ing] the threat of election interference,” but said the order “does not go far enough to address it.

“We must make sure Vladimir Putin’s Russia, or any other foreign actor, understands that we will respond decisively and impose punishing consequences against those who interfere in our democracy,” the senators said in a statement.

Director of National Intelligence Dan Coats repeated that intelligence officials have not yet seen Russia’s intense efforts to upend the 2016 presidential contest repeated in the 2018




📷 President Donald Trump. / Susan Walsh, AP

midterms. He warned, however, that a full-blown interference effort is “only a keyboard click away.”

Coats warned that China, Iran and North Korea also have the capability to interfere in U.S. elections but did not say if the intelligence community has evidence those nations have actually attempted to interfere.

The Trump order bears some similarities to an Obama [action](#) from December 2016, which authorized sanctions against nations, individuals and organizations that use digital disinformation or altered information to undermine election processes or institutions.

That action, however, did not describe the same extensive process for identifying election meddling. The first target of the expanded authority was Russia’s meddling in the 2016 presidential contest.

The Obama action amended a 2015 executive order that came in the wake of the Sony Pictures Entertainment breach and document release by North Korean hackers. That executive order authorized sanctions for destructive or disruptive cyberattacks or digital theft. 

DHS Cyber Unit Fields False Alarms But No Hacks on Election Day

Incidents flagged as potential attacks turned out to be malfunctions or accidents, according to Homeland Security officials.

By Aaron Boyd

As Americans exercise their hard-won right to choose their leaders on Election Day Nov. 6, the Homeland Security Department is poised to chase down any potential cyberattack or compromise of election infrastructure—and debunk rumors, if necessary.

Officials said they do not expect a real attack, but are ready to address rumors that could seriously affect turnout or undermine people's confidence in the results.

The department is coordinating with other federal agencies—namely the FBI—as well as state and local officials throughout the day, including keeping at least one official stationed in every state available to respond to major concerns.

While Homeland Security officials—especially those working in the National Protection and Programs Directorate—are focused on protecting the nation's infrastructure from cyberattacks Election Day, they are more worried about false claims of cyberattacks undermining American's faith in the electoral system.

"We continue to monitor what's going on across the country. Nothing significant yet to report at this point," a federal official told reporters on a 9 a.m. call, adding that, no matter how unlikely, they are preparing as though there will be a major infrastructure attack, just in case.

However, the official said they have seen continued information campaigns, particularly from Russia.

"That's to divide Americans," the official said. "But there's a lot of noise out there and a lot of it being pushed is propaganda in some cases. For the most part it's all garbage."

But that "garbage" can have a significant effect if people think their vote won't be counted properly. That kind of disenfranchisement can lead to lower turnout and mistrust in the results of the election.

"It's not necessarily the substantive or actual attacks against infrastructure" that election officials are most worried about on Election Day, "but it would be someone, an actor, getting on social media or other forms

of communications and saying that they're doing that," the Homeland Security official said. "What we're looking to accomplish through the situational awareness rooms is identifying those issues as they pop up, getting the appropriate election official—the state or local election official in the relevant jurisdiction—to quickly assess, get to the root cause and be able to debunk those issues and issue statements."

Here's how the rest of Election Day progressed for the department:

9 A.M. BRIEFING

Officials across the country are also keeping in touch using the National Situational Awareness Room, a web portal to enable real-time communications on potential issues. As of 9 a.m., some 20 states had logged in to the portal. Homeland Security officials expect that number to grow as polling stations begin to open.

12 P.M. BRIEFING

Homeland Security officials have seen little to no hacking attempts and only a few isolated issues with voting systems so far on Election

Day, they said in a noon update with reporters. Instead, they are seeing "run-of-the-mill activities" like system scanning.

"I liken it to pulling up Google Maps street view and looking at the house from your computer," one official said. "It's not anything that's intrusive. It's a drive-by of a website to see what it looks like."

Voting machine vendors in communication with the Federal Election Commission said they have been seeing typical machine issues throughout the day but no more so than any other election.

"They did not share any widespread trends or growing trend with any specific machines," a Homeland Security official said of those conversations. "Just sparse issues with machines that they would typically see on Election Day."

Even though Homeland Security is only getting reports of low-level shenanigans and minor issues so far, officials said that is exactly what they wanted to happen.

"We encourage our partners to establish a very low threshold—or bar—for reporting so that any little thing can help us get that bigger, over-the-top, national picture," they said.

3 P.M. BRIEFING

As of 3 p.m., officials from 45 states had joined the situational awareness room. In total, 271 people had engaged with the web portal to exchange information about potential voting issues they have seen throughout the day.

6 P.M. BRIEFING

There have been no reported hacking incidents so far on Election Day, Homeland Security officials said during the evening briefing. However, they have seen quite a bit of misinformation being disseminated online.

As returns begin to come in and early results are reported, federal official reminded citizens that these will be unofficial results until verified by local authorities, which can take hours, days or even weeks. The official warned everyone to be wary of results being reported by dubious sources.

“Be sure to get official results from state and local election officials—those are the trusted sources here,” they said. “And know that, again, there are actors that may be trying to spread misinformation, disinformation, propaganda ... garbage. Know your sources and think before you pass along information.”


9 P.M. BRIEFING

Despite a few scares, there is no evidence of any cyberattacks against election infrastructure Nov. 6, Homeland Security officials said.

As expected, federal officials spent much of the day chasing down anomalies that appeared to have a cyber angle, though all turned out to be typical malfunctions or accidents.

For example, in several states earlier in the day, voters were receiving text messages reminding them to “vote tomorrow”—a day late. The text messages were reported to Homeland Security officials who determined that a flaw in a third-party provider’s API sent the message a day later than intended.

Another official offered a hypothetical example to watch for tonight on state and local election websites, where unofficial results will be posted.

“The resource requests that will be descending upon those pages in some cases may exceed their current capacity,” causing the page to crash from too much traffic, the official said. “Don’t automatically assume that it’s a [distributed denial-of-service] attack by a malicious actor, by the Russians, whatever. In some cases, it is just a technical configuration of those websites.” 

An Overlooked Threat: Online Ballots

At least 100,000 online ballots—including the votes of overseas military personnel—were cast in 2016.

By Joseph Marks

The government's extensive effort to secure election systems after a Russian assault on the 2016 contest missed one glaring vulnerability: online ballots, according to a [report by voting security experts](#).

Online voting is not common in the U.S., but Americans cast at least 100,000 online ballots in the 2016 election, according to the authors' tally. Many of those ballots were cast by military members overseas taking advantage of state laws that allow them to return ballots by email or digital fax.

In total, 32 states allow some subset of residents to return ballots by email, fax or through an internet portal, and Alaska and Hawaii offer electronic ballot return for all voters, according to the report from security experts at the Association for Computing Machinery US Technology Policy Committee, Common Cause Education Fund, the National Election Defense Coalition and the R Street Institute.

States began offering online voting options to overseas service members in the early 2000s when the Pentagon was working on developing an online portal for overseas voting, the report

states. That plan was scrapped in 2015 after researchers concluded the portal could not be developed securely, according to the report.

Online voting creates multiple cybersecurity challenges, the report states. To begin with, emailed or faxed ballots could be hacked and altered at multiple points on their journey between the voter and the election office.

"It would not be difficult to create an automated process for discarding ballots with undesired votes and replacing them with forgeries," the report states. "In this process, the sender's original message and any other attachments, such as a voter's declaration and signature, could be maintained, producing a forged ballot that would appear perfectly authentic to any unsuspecting election official."

Criminals or adversary nation-states could also use email ballots to deliver malware into an election system network, allowing them to spy on or even disrupt other election operations.

Or, they could use an online ballot system to launch a digital denial of service attack against the election office.



© Bibit Unggul / Shutterstock.com

The report mirrors years of warnings about the dangers of online voting.


Ultimately, the report concludes, the benefits of allowing some Americans, including overseas service members to cast online ballots does not outweigh the potential harm.

“Military voters ... deserve any help the government can give them to participate in democracy equally with all other citizens,” the report states. “However, in this threat-filled environment, online voting endangers the very democracy the U.S. military is charged with protecting.”

The report urges that states drastically curtail online voting before the 2020 election.

In advance of the 2018 contest, state and local election administrators should ensure that systems that accept online ballots are fully segregated from other election systems and running on different Wi-Fi networks.

They should also scan all incoming fax and email ballots for malware and print them out rather than passing them to vote counters electronically, the report states.

The report also urges overseas voters to print out and mail their ballots if at all possible. 

After Midterm Elections, a Focus on Securing Campaigns

The Homeland Security Department hopes campaigns can cooperate on cybersecurity rather than compete.

By Joseph Marks

The Homeland Security Department and a cybersecurity non-profit plan to ramp up efforts to share cyber threat information and best practices with political campaigns after the midterm elections.

The Center for Internet Security, or CIS, which manages a cyber threat information sharing program between the federal and state and local governments, hopes to begin offering similar services to political campaigns, the organization's executive chairman John Gilligan told reporters Oct. 30.

CIS reached out to campaigns about the idea in recent months but found they were too busy to launch a new program so late in the election cycle, Gilligan said after a panel discussion about election security hosted by the Center for Strategic and International Studies.

CIS hopes that the comparatively slower pace of 2019 will allow it to get the program off the ground, Gilligan said. He described the plan

as "informal" at this point, but said he hopes it will be well established before the presidential and congressional elections in 2020.

Campaigns could significantly benefit from the program because they typically operate on shoestring budgets, especially early in a race, and aren't able to hire cyber experts, Gilligan said. The long run up to 2020 will give CIS and the campaign organizations time to build trust, he said.

The goal would be to run the program at almost no cost by simply piggybacking off of state and local cyber threat information sharing that CIS is already doing. The program would only deal with unclassified threat information, Gilligan said.

The Homeland Security Department, which is leading election security work for the federal government, also hopes to establish better ties with campaigns between 2018 and 2020, said Bob Kolasky, who leads the department's National Cyber Risk Management Center.



📷 The Department of Homeland Security page on a monitor screen through a magnifying glass./ Shutterstock.com

Homeland Security has vastly improved cyber information sharing and threat detection with state and local election administrators since Russian efforts to undermine the 2016 elections. That effort was spurred by a late Obama administration decision to define election systems as critical infrastructure, similar to airports, banks and hospitals.

The department has met with the Republican and Democratic national committees but is not broadly sharing threat data with House and Senate campaigns.

Hackers linked to the Russian government penetrated Democratic nominee Hillary Clinton's campaign in 2016 and released the stolen data

to WikiLeaks, according to indictments from Special Counsel Robert Mueller.

Chinese hackers also reportedly penetrated both the Obama and McCain campaigns in 2008.

Ultimately, Kolasky said, he hopes Democratic and Republican campaigns can cooperate on cybersecurity similar to how companies in critical infrastructure sectors do.

"How do we cordon off the security imperative from the political imperative?" he asked. "I'd like to get to a point where campaigns work together on security, work with the government and don't compete on security."

N

About the Authors



FRANK KONKEL, Executive Editor

Frank Konkel is *Nextgov*'s executive editor. He writes about the intersection of government and technology. Frank began covering tech in 2013 upon moving to the Washington, D.C. area after getting his start in journalism working at local and state issues at daily newspapers in his home state of Michigan. Frank was born and raised on a dairy farm and graduated from Michigan State University.



JOSEPH MARKS, Senior Correspondent

Joseph Marks covers cybersecurity for *Nextgov*. He previously covered cybersecurity for Politico, intellectual property for Bloomberg BNA and federal litigation for Law360. He covered government technology for *Nextgov* during an earlier stint at the publication and began his career at Midwestern newspapers covering everything under the sun. He holds a bachelor's degree in English from the University of Wisconsin in Madison and a master's in international affairs from Georgetown University.



JACK CORRIGAN, Staff Correspondent

Jack Corrigan covers emerging government technology and IT policy. He joined *Nextgov* as an editorial fellow in the summer of 2017 and previously wrote for publications around his hometown of Chicago. He is a graduate of Northwestern University.