S. HRG. 115–862

THE DEPARTMENT OF DEFENSE'S ROLE IN PROTECTING DEMOCRATIC ELECTIONS

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY

OF THE

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

FEBRUARY 13, 2018

Printed for the use of the Committee on Armed Services

Available via: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
44–117 PDF WASHINGTON : 2021

COMMITTEE ON ARMED SERVICES

JOHN MCCAIN, Arizona, *Chairman*

JAMES M. INHOFE, Oklahoma	JACK REED, Rhode Island
ROGER F. WICKER, Mississippi	BILL NELSON, Florida
DEB FISCHER, Nebraska	CLAIRE MCCASKILL, Missouri
TOM COTTON, Arkansas	JEANNE SHAHEEN, New Hampshire
MIKE ROUNDS, South Dakota	KIRSTEN E. GILLIBRAND, New York
JONI ERNST, Iowa	RICHARD BLUMENTHAL, Connecticut
THOM TILLIS, North Carolina	JOE DONNELLY, Indiana
DAN SULLIVAN, Alaska	MAZIE K. HIRONO, Hawaii
DAVID PERDUE, Georgia	TIM KAINE, Virginia
TED CRUZ, Texas	ANGUS S. KING, JR., Maine
LINDSEY GRAHAM, South Carolina	MARTIN HEINRICH, New Mexico
BEN SASSE, Nebraska	ELIZABETH WARREN, Massachusetts
TIM SCOTT, South Carolina	GARY C. PETERS, Michigan

CHRISTIAN D. BROSE, *Staff Director*
ELIZABETH L. KING, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY

MIKE ROUNDS, South Dakota, *Chairman*

DEB FISCHER, Nebraska	BILL NELSON, Florida
DAVID PERDUE, Georgia	CLAIRE MCCASKILL, Missouri
LINDSEY GRAHAM, South Carolina	KIRSTEN E. GILLIBRAND, New York
BEN SASSE, Nebraska	RICHARD BLUMENTHAL, Connecticut

CONTENTS

FEBRUARY 13, 2018

THE DEPARTMENT OF DEFENSE'S ROLE IN PROTECTING DEMOCRATIC ELECTIONS

TUESDAY, FEBRUARY 13, 2018

UNITED STATES SENATE,
SUBCOMMITTEE ON CYBERSECURITY,
COMMITTEE ON ARMED SERVICES,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:34 p.m. in Room SR–222, Russell Senate Office Building, Senator Mike Rounds (chairman of the subcommittee) presiding.

Subcommittee Members present: Senators Rounds, Fischer, Sasse, Nelson, McCaskill, Gillibrand, and Blumenthal.

OPENING STATEMENT OF SENATOR MIKE ROUNDS

Senator ROUNDS. Good afternoon.

The Cybersecurity Subcommittee meets this afternoon to receive testimony on the Department of Defense's (DOD) role in protecting the U.S. election process.

The witnesses are Mr. Bob Butler, Co-founder and Managing Director of Cyber Strategies, LLC; Adjunct Senior Fellow at the Center for a New American Security; Senior Vice President of Critical Infrastructure Protection Operations for AECOM; Ms. Heather Conley, the Senior Vice President for Europe, Eurasia, and the Arctic and Director of the Europe Program at the Center for Strategic and International Studies; Dr. Richard Harknett, head of political science at the University of Cincinnati and a former scholar in residence at U.S. Cyber Command and the National Security Agency; and Dr. Michael Sulmeyer, the Director of the Cyber Security Project at the Harvard Kennedy School.

At the conclusion of Ranking Member Nelson's comments, we will ask our witnesses to make their opening remarks. After that, we will have a round of questions and answers.

There is no dispute about what Russia did during the 2016 election cycle. There is clear evidence that Russia attempted to undermine our democratic process through the hacking of independent political entities, manipulation of social media, and use of propaganda venues such as Russia Today. Evidence to date indicates that no polls or State election systems were manipulated to change the outcome of the vote. However, there was evidence of Russian probing of certain election systems in 21 states.

The Department of Defense has a critical role to play in challenging and influencing the mindset of our cyber adversaries and defending the homeland from attacks, attacks that could include cyber attacks by other nations against our election infrastructure.

We look forward to the Department approaching these issues with a heightened sense of urgency.

The threat is not going away. Just a couple of weeks ago, the Director of the Central Intelligence Agency warned that Russia will seek to influence the upcoming midterm elections. The White House National Security Advisor stated that they will seek to influence the Mexican presidential campaign as well. This is all in addition to Russian attempts to influence the elections in France and Germany last year.

Each of us on this panel has been quite vocal about the need for a strategy that seizes the strategic high ground in cyberspace. Whether you call it deterrence or something else, we need a strategy that moves out of the trenches and imposes costs on our adversaries. The lack of consequences for the countless attacks over the past decade has emboldened our adversaries and left us vulnerable to emboldened behavior. The attacks we experienced during the 2016 election are just the latest rung on that escalation ladder. As long as our adversaries feel that they can act with impunity, they will press further.

Our witnesses offer unique perspectives on the challenges we face. We look to them to help us understand why our posture restraint has not worked, if we can reverse the damage already done, and what it will take to develop and implement a strategy that limits our exposure and imposes costs on malicious behavior.

We invited Dr. Richard Harknett to explain his theory of cyber persistence, specifically on how our failure to tailor our strategies to the uniqueness of the cyber domain limits our ability to confront challenges we face. Our adversaries actively exploit us because they see great benefit and little consequence in doing so. I agree with Dr. Harknett that the Cold War models of deterrence will not work and look forward to hearing what he believes it will take to influence the mindset of our adversaries.

In addition to his writings on cyber deterrence and election attacks, Dr. Michael Sulmeyer has focused a great deal of his research on the organizational challenges we face as a government. We understand that Dr. Sulmeyer is working on a paper addressing some of the challenges we examined during our full committee hearings in October on the whole-of-government approach to cybersecurity. We look forward to hearing more from Dr. Sulmeyer on the gaps and the seams he sees in our organizational model and what lessons we can learn from analyzing like the British.

Ms. Heather Conley provides an expertise in Russian politics and foreign policy. Russia has yet to face serious consequences in the cyber or other domains for its 2016 elections interference. We look forward to Ms. Conley's testimony on how the United States can tailor and implement these penalties and how the Department can best deter or dissuade further Russian election meddling.

We also look forward to the testimony of Mr. Bob Butler who brings extensive cyber experience in both the Department of Defense and the private sector. Mr. Butler has been involved in numerous studies on the cyber deterrence, including the recent Defense Science Board Task Force on Cyber Deterrence.

Let me close by thanking our witnesses for their willingness to appear today before our subcommittee.

Senator Nelson?

STATEMENT OF SENATOR BILL NELSON

Senator NELSON. Thank you, Mr. Chairman.

First of all, I want to make sure that, since this is a hearing on elections, everybody understands that this Senator feels that this is about the foundation of our democracy and that we as a government ought to be doing more to defend ourselves.

The second thing I want to make sure everybody understands is that this is not a partisan issue. This can happen to either party or the non-party candidates as well. It ought to be all hands on deck.

The chairman and I in public and in closed meetings because of the clearance level—we have been quite disturbed about wondering if we are doing as much as we should as a government to protect ourselves. So in a recent closed hearing of this subcommittee, the Department of Defense demonstrated that it is not taking appropriate steps to defend against and deter this threat to our democracy.

So, Mr. Chairman, I join you in welcoming these witnesses and hope that some practical suggestions are going to come out. Now, I want to mention just a few things.

First, the Department has cyber forces designed and trained to thwart attacks on our country through cyberspace, and that is why we created the Cyber Command's National Mission Teams. Members of this subcommittee, Senator Blumenthal, Senator Shaheen—we all wrote to the Secretary of Defense last week that they, the Department, ought to be assigned to identify Russian operators responsible for the hacking, stealing information, planting misinformation, and spreading it through all the botnets and fake accounts on social media. They ought to do that. The Cyber Command knows who that is.

Then we ought to use our cyber forces to disrupt this activity. We are not.

We should also be informing the social media companies of Russia's fake accounts and other activities that violate those companies' terms of service so that they can be shut down.

Second I would ask us to look at that as the Department's own Defense Science Board Task Force on Cyber Deterrence concluded last year—we ought to show Mr. Putin that two can play in this game. We ought to consider information operations of our own to deter Mr. Putin like exposing his wealth and that of his oligarchs.

Third, I would suggest the Department should ensure that its active and reserve component cyber units are prepared to assist the Department of Homeland Security and the governors to defend our election infrastructure, not just after the attack but proactively before and during the Russian attacks.

Fourth, I would suggest that the Department must integrate capabilities and planning into cyber warfare and information warfare to conduct information warfare through cyberspace as last year's defense bill mandated. Our adversaries recognize the importance of this kind of integration, but today cyber warfare and information warfare are separated in the Department of Defense and involve multiple organizations.

Fifth, I would recommend, as one of our witnesses I think will testify today, the Department must help develop an effective whole-of-government response to Russia's strategic influence operation through things like a joint interagency task force and a fusion center. Our colleagues on the Foreign Relations Committee have proposed something similar. The threat is not going away. It is likely to intensify. As our intelligence community has been warning and as DNI [Director of National Intelligence] Coats has just testified to the Senate Intelligence Committee, that threat is not going away.

So the 2018 elections are upon us. We cannot sit idly by and watch this happen again.

Thank you, Mr. Chairman.

Senator ROUNDS. Thank you.

Welcome to all of our panelists here today, our witnesses. We would ask that, first of all, you limit your opening remarks to 5 minutes, but your entire statements will be made a part of the record. We would like to begin with Mr. Butler.

STATEMENT OF ROBERT J. BUTLER, COFOUNDER AND MANAGING DIRECTOR, CYBER STRATEGIES, LLC

Mr. BUTLER. Thank you, Mr. Chairman, Ranking Member Nelson, and distinguished members of the Cyber Subcommittee. It is a privilege to be here. Thank you for the invitation.

My views really represent my views and not that of any particular organization. I will just quickly hit the highlights of my written statement. They track very closely with a lot of the opening comments. My comments are really focused around my assessment of the threat in the electoral processes after interviewing a few different States; secondly, recommendations for the Federal Government partnered with a whole-of-America campaign; and then thirdly, what this subcommittee can do going forward.

I have been watching the Russian influence operations threat for some time in uniform and out of uniform. Our ability to counter Russian influence operations is not only a function of what we know about the threat but our willingness and our ability address that threat through hardening resilience and other countermeasures.

As I have looked at the election infrastructure in a few different States, we have learned from 2016, and our known vulnerabilities have been remediated. Whether you look at the voting registration systems in the election infrastructure proper, we are making progress there. However, the States do not know how to address the disinformation campaign. That is a struggle and the threat still remains very, very high.

From my perspective looking at this particular threat, what we are talking about today is one line of operation within what I think has to be addressed through a National Security Council-led task force, a whole-of-America campaign not too much dissimilar from the NCTC [National Counterterrorisim Center], but with a strong, empowered private sector element. Again, I go back to the idea of a whole-of-America process.

Two key components inside of this. One is the idea of having an element that is focused on strengthening States' election infrastruc-

ture and hardening American citizens, deterrence by denial some would say. A second component focused on cost imposition from botnet disruptions to other kinds of sanctioning activities, importantly reinforced multilaterally. I am a big proponent of an International Cyber Stability Board, a coalition of the willing, working to ensure the most effective way of doing cost imposition. Those two components then supported by an integrated fusion center that provides situational awareness, combines the best of intelligence both in the commercial and from the national security community with law enforcement and active defense actions, focused on a campaign that is centralized in its planning but decentralized in its execution.

From my perspective, it really requires both cultural and legislative enablers. Culturally the President must lead, must rally the nation. There are opportunities already this week that can be used to help with that. The infrastructure proposal is a great example. I do not see anything about resilience in the infrastructure proposal. We should have a way of incorporating, especially as we are building new infrastructure, methods and strategies and incentives for strengthening the infrastructure here in this country.

Additionally, we need to leverage the best of U.S. competencies across America. Defense is excellent at campaign planning and exercise. U.S. intelligence agencies, combined with web-scale companies, do a great job in intelligence generation and fusion. Web-scale companies are very good and growing in their ability to rapidly identify disinformation campaigns and response, and we will need some help from the legislative side.

Specifically for DOD [Department of Defense], five recommendations that track very closely with what Senator Nelson was talking about. I think to jump start this NSC [National Security Council]-sponsored task force, we should coordinate with the Secretary of Defense to immediately stand up a JIATF, a joint interagency task force. Inside of that, again empowered private sector players. We typically do not think about that, but this really is something where we need to work together in a public-private partnership. We need to make arrangements with State and local officials through DHS [Department of Homeland Security] and the National Guard Bureau.

The second recommendation really is to the NGB and working with the National Guard Bureau to really not only inventory what we have from a cyber and IO perspective. We have cyber units. We information operations units. But to begin to scale them to help the States and to help us as we think about incident response in general. I think they could be aligned with FEMA [Federal Emergency Management Agency] regions. I think they could be aligned in a lot of different ways, but we need to first get organized.

The third is to actually have a session where we discuss courses of action. It would have to be a closed session. But I think that is where the request for authorities, new authorities, requests for new resources come out. It really gets at the point of not only looking at offensive actions but defensively what we are in store for as we begin to move offensively and what we are going to do from a continuity of government, continuity of business perspective.

The last two relate to Senator Nelson's comments with regard to the DSB [Defense Science Board] task force. I think we should continue to push with the NDAA [National Defense Authorization Act] and operationalizing the rest of the Cyber Deterrence Task Force recommendations. I would advocate that this committee should have its own campaign of exercises to help it understand where the adversary is going and to be able to advance ideas with regard to looking at threat and countermeasures.

I stand ready to answer any questions that you have.

[The prepared statement of Mr. Butler follows:]

PREPARED STATEMENT BY ROBERT J. BUTLER

Mr. Chairman, Ranking Member Nelson, and distinguished members of the Cyber Subcommittee, thank you for inviting me to speak on the topic of countering Russian influence in the United States elections infrastructure. I would like to begin by noting that my opinions are mine and do not reflect the views of any organization.

For more than 37 years, my work life has been about Information Technology (IT) and its application across Defense and other sectors. Along the way, I was afforded the opportunity to help guide the evolution of information warfare; information and cyberspace strategy and operations within the Department of Defense (DOD); and the United States Government (USG) as a planner and commander. My work in DOD included the stand-up of information operations (IO) organizations, development of IO campaign plans, and serving as the DOD lead in the first USG negotiation with the Russians on cyber arms control in 1998. I was also privileged to serve as the Director of Intelligence at U.S. Transportation Command (TRANSCOM) during Operations Enduring and Iraqi Freedom. I culminated my military career by commanding the intelligence operations organization that is now commonly referred to as NSA–Texas.

After retirement from the United States Air Force (USAF), I served as the senior civilian executive for DOD's premiere joint information operations command before joining a U.S.-based global IT services firm as its Director of its Military Intelligence Programs. Returning to Government service in 2009, I served as the first Deputy Assistant Secretary of Defense (DASD) for Space and Cyber Policy. During my time as a DASD, I witnessed and was alarmed at the expansion of the cyber threat around the globe—specifically, China's rampant on-line theft of United States intellectual property and Russia's continued disruptive cyber-attacks in the Ukraine and other parts of the world.

Since leaving government service in 2011, I have spent most of my time in the private sector. As a corporate Chief Security Officer and now as an AECOM [1] security executive, I had the opportunity to build and implement enterprise security programs to countering foreign threats. Additionally, I have served and continue to serve as a consultant to various Defense Science Board (DSB) task forces including the recent cyber deterrence task force. It is from this experience base, I address you today. I've organized my remarks around three topics: 1) my assessment of the Russian threat, specifically to our electoral process; 2) my recommendations for what the federal—including DOD—and state governments, along with United States industry should do to further counter Russian or any other foreign government influence; and 3) my suggestions for how this committee could help in this national security work. While my testimony focuses on enhancing the resilience of the U.S. electoral process, I have also made some suggestions regarding the resilience of critical infrastructures more generally as the threats and responses overlap.

THE RUSSIAN THREAT AND OUR ELECTION PROCESS.

Our ability to counter Russian influence operations is a function of what we know about the Russian threat and our ability to address that threat through hardening, resilience, and other countermeasures. The National Security Strategy (NSS) and the National Defense Strategy (NDS) identify Russia as "attempting to erode American security and prosperity" including "using information tools in an attempt to un-

[1] AECOM is an American multinational engineering firm that provides design, consulting, construction, and management services to a wide range of clients. AECOM has approximately 87,500 employees, and is number 156 on the 2016 Fortune 500 list. (2018, January 01). About AECOM. Retrieved February 06, 2018, from *http://www.aecom.com/about-aecom/*

dermine the legitimacy of democracies."[2] As reported by our intelligence agencies, the Russian Federation has been engaged in a campaign aimed at interference with our 2016 presidential election process. Russian intelligence obtained and maintained access to elements of multiple United States state or local electoral boards. Russia's influence campaign has been multi-faceted and has included Russian Government cyber and media activities along with the use of third party intermediaries and social media "trolls."[3] Importantly, we have no indication that this Russian influence campaign against democratic elections has stopped. In fact, Russian Government interference in European national elections leads us to a very different judgment, namely that this type of Russian aggression is growing.[4] NATO assessments about Russia's capabilities and intent confirm this assessment.[5] CIA Director Pompeo has stated that Russia can be expected to meddle in the 2018 elections.[6]

A key focus of the Russian influence actions has been against the election infrastructure in our states. The threat to state electoral systems is dependent on the state election infrastructure architecture. Some states have highly automated infrastructure while others continue to employ paper ballot systems. In the latter case, digital interactions still exist with web interfaces for voter registration and election day voter verification along with the use of digital ballot counting machines which scan paper ballot and store results.

Based on my conversations with Government representatives from geographically dispersed states, the integrity and quality of election infrastructure has improved since 2016. States have reviewed the exposure and configuration of their end-to-end voting system, and known areas of technical and procedural weaknesses have been remediated.[7] Nonetheless, the *threat to electoral processes remains high.* For one, it is difficult to identify and nullify disinformation campaigns that are portrayed as news coverage.

RECOMMENDATIONS TO COUNTER RUSSIAN INFLUENCE IN OUR ELECTION PROCESS.

America has been and will continue to be involved in a campaign of continuous engagement and pressure from the Kremlin to weaken United States and allied critical infrastructure and democratic processes. To counter, we need a "whole of America" campaign approach aimed directly at preventing Russian or any other foreign government interference. This campaign must be led by a National Security Council (NSC)-sanctioned task force (not too dissimilar to the National Counter-Terrorism Center) with membership from empowered government agencies and industry representatives. One line of operation in this campaign is countering Russian interference to influence our electoral process.

This standing national task force needs to have two synchronized components—one focused on continuous strengthening of the states' election infrastructure as well as "hardening" American citizens to Russian media and other cyber-enabled influence operations. Importantly, these activities should include a partnership with industry to regularly red team state election infrastructure; share relevant intel with state election and cybersecurity officials; bar Russian or other foreign online election material (just as we bar foreign election contributions;) continuously identify fake and harmful messages; and quickly disseminate the truth about USG actions. As a starting point, this USG-industry partnership could build off the actions already underway to counter on-line terrorist propaganda.[8]

The second component of this task force should be focused to directly impose cost on the Russian Federation, including activities ranging from cyber-enabled social media operations and botnet disruptions to sanctions and other enforcement actions.

---

[2] Trump, D. (2017, December). National Security Strategy. *https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS–Final-12–18–2017–0905.pdf* pp. 2, 14.

[3] Director of National Intelligence. (2016, January). Background to "Assessing Russian Activities and Intentions in Recent U.S. Elections". *https://www.dni.gov/files/documents/ICA—2017—01.pdf*

[4] Greenberg, A. (2017, June 02). NSA Director Confirms That Russia Really Did Hack the French Election. Retrieved February 06, 2018, from *https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/*

[5] Giles, K. (2016, November). Handbook of Russian Information Warfare. *https://krypt3ia.files.wordpress.com/2016/12/fm—9.pdf*

[6] Cohen, Z. (2018, January 31). CIA director Pompeo met top Russian spies. Retrieved February 06, 2018, from *https://www.cnn.com/2018/01/30/politics/cia-director-pompeo-russia-spies/index.html*

[7] Department of Homeland Security. (2018, January). National Cyber Incident Coordination Center. *https://www.dhs.gov/national-cybersecurity-and-communications-integration-center*

[8] Robertson, A. (2017, June 26). Facebook, Microsoft, Twitter, and YouTube launch anti-terrorism partnership. Retrieved February 06, 2018, from *https://www.theverge.com/2017/6/26/15875102/facebook-microsoft-twitter-youtube-global-internet-forum-counter-terrorism.*

Importantly, these cost imposition measures, when and where possible, need to be multilateral in nature, involving other allied nations and coordinated with appropriate private sector organizations.[9] The formation of an International Cyber Stability Board (ICSB) of allied nations and industry partners could support rapid coordination and enforcement of actions across Internet infrastructure. The NSC staff should lead in the development of the ICSB.

The two components should be supported by an integrated fusion center that enables continuous situational awareness and engagement through human capital intelligence, intelligence at large, law enforcement, and active defense actions. Although centrally planned, execution of action must be decentralized to support persistent and agile engagement against Russian "trolls," bots, and other surrogates of the Russian Government.

To enable this type of organization and ensure its success will require both cultural and legislative changes. The President needs to rally the U.S. Government and U.S. industry. Infrastructure resilience and countermeasures need to be part of the President's "call to action" this year. Additionally, we need to leverage the best U.S. organizational core competencies to include the following:

- Defense for campaign planning and exercise,
- U.S. Intelligence Agencies and industry for rapid intelligence generation and fusion,
- Webscale companies for rapid identification of disinformation campaigns and response,
- Congress for potentially changing laws like the Computer Fraud and Abuse Act (CFAA) and enabling Government and industry to work together to actively defend this nation.[10]

On the international front, it is critical to align our efforts with our allies and identify appropriate "red lines" for actions. For example, these would include attempts to hack or disrupt our electrical grid and voting machines.[11]

PROPOSALS FOR THE CYBER SUBCOMMITTEE AND SASC.

To "jump start" the stand-up of an NSC-sponsored national task force, the SASC should coordinate with the Secretary of Defense in immediately establishing a joint interagency task force to begin and accelerate counter-Russian influence campaign planning. Key private sector elements from the Defense Industrial Base and webscale companies should be included as needed. Also, appropriate working arrangements with state and local officials through the Department of Homeland Security (DHS) and the National Guard Bureau (NGB) should be created. The SASC through its oversight jurisdiction should then monitor the progress of the task force.

To further support the stand-up of the new national task force for countering Russian or other foreign government influence, I recommend the SASC direct the NGB, in conjunction with U.S. Cyber Command (CYBERCOM), to inventory and certify all cyber capable National Guard assets that could augment state resiliency and federal efforts. Working with other committees, the SASC should then develop a statute to grow ten NGB "cross-state mutual assistance" teams as certified active defense teams to work alongside Federal Emergency Management Agency (FEMA) regional leads, other government and industry partners at the state and federal level.

The SASC should direct the Defense Leadership Team to develop Defense-Defense Industrial Base Courses of Action (COA) to support the new national task force, and to provide in a closed session a summary of these COAs along with new resources and authority requests to the Committee. Related to this point, the SASC should

---

[9] Frank Kramer, Bob Butler, and Catherine Lotrionte. (2017, November 06). Raising the Drawbridge with an "International Cyber Stability Board". Retrieved February 06, 2018, from *https://www.thecipherbrief.com/raising-drawbridge-international-cyber-stability-board.*

[10] McCain, U. S. (2017, October). Press Releases. Retrieved February 06, 2018, from *https://www.mccain.senate.gov/public/index.cfm/2017/10/mccain-klobuchar-warner-introduce-legislation-to-protect-integrity-of-u-s-elections-provide-transparency-of-political-ads-on-digital-platforms. https://tomgraves.house.gov/uploadedfiles/discussion_draft_active_cyber_defense_certainty_act_2.0_rep._tom_graves_ga-14.pdf.; https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/CCHS-ActiveDefenseReportFINAL.pdf.* and *https://www.mccain.senate.gov/public/index.cfm/2017/10/mccain-klobuchar-warner-introduce-legislation-to-protect-integrity-of-u-s-elections-provide-transparency-of-political-ads-on-digital-platforms.*

[11] Miller, J. (2018, January). Navigating Dangerous Pathways. Retrieved February 06, 2018, from *https://www.cnas.org/publications/reports/navigating-dangerous-pathways?utm_medium=email&utm_campaign=Project Pathways 3 Report Release&utm_content=Project Pathways 3 Report Release%2BCID_2bd61d40546a491ed2980e0568645014&utm_source=Campaign Monitor &utm_term=Navigating* Dangerous Pathways A Pragmatic Approach to United States–Russian Relations and Strategic Stability

work with the DOD and other Committees to update all statutes for enabling Defense counter-influence actions at home and abroad.

To deter further adversary action, we must harden our critical infrastructure. This includes the election infrastructure, but also all infrastructure which ensures national security, public safety and democratic processes. From a defense standpoint, this starts with the resilience of our nuclear strike capabilities, non-nuclear capabilities such as conventional strike, missile defense and offensive cyber. Specific recommendations are included in the 2017 DSB report on Cyber Deterrence.[12] The SASC should continue to act to operationalize these recommendations as part of developing the next National Defense Authorization Act.

Finally, the Committee should set up its own campaign of "table top" exercises that would help members to better understand different adversary scenarios which could involve defense capabilities and highlight the need to the Committee for other Congressional actions in countering Russian influence.

Thank you again for the opportunity to share these thoughts. I stand ready to help the Committee as we seek to better protect and grow our nation.

Senator ROUNDS. Thank you, Mr. Butler.

Ms. Conley?

STATEMENT OF HEATHER A. CONLEY, DIRECTOR, EUROPE PROGRAM, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

Ms. CONLEY. Thank you so much, Chairman Rounds, Ranking Member Senator Nelson, and esteemed colleagues. Thank you for this very timely opportunity to speak to you this afternoon and what a timely moment as United States intelligence agencies have now assessed that Russia will continue to make bold and more disruptive cyber operations focused on the midterm elections. CIA [Central Intelligence Agency] Director Mike Pompeo also stated publicly that he fully expects that Russia will attempt to disrupt the United States midterm elections. So we know they are doing it and will do it, but we as a nation are not prepared to effectively combat what I believe is an intensifying disinformation operation and influence operation.

I am a bit of a contrarian on this panel. I am not a cybersecurity expert. But what I am most concerned about is that we have 9 months, and the American people are not educated as to what is going to happen to them. That is where I think our focus must lie. I am less concerned about the mindset of President Putin. I know his mindset. I am more concerned about the mindset of the American people as we head towards this election.

You asked us what role DOD could play to protect the U.S. elections. I think simply DOD, working with Congress, has got to demand a whole-of-government strategy to fight against this enduring disinformation and influence operation. We do not have a national strategy. Unfortunately, modernizing our nuclear forces will not stop a Russian influence operation. That is where we are missing a grave threat that exists in the American people's palm of their hand and on their computer screens. It is vital that we start talking publicly about this threat and educating the American people on a bipartisan basis.

Tragically the Russian campaign has already deeply polarized our country, which only serves the Kremlin's interests. As one of the most trusted institutions in the United States, the Department

[12] Defense Science Board. (2017, February). Task Force on Cyber Deterrence. *https://www.acq.osd.mil/dsb/reports/2010s/DSB–CyberDeterrenceReport_02-28-17_Final.pdf.*

of Defense must leverage that trust with the American people to mitigate Russian influence. Simply put, the Department of Defense has to model the bipartisan and fact-based action, behavior, and awareness that will help reduce societal division. This is about leadership. It is about protecting the United States, and as far as I can see, that is in the Department of Defense's job description.

So a good place to begin is using DOD's extensive employee and military networks to provide timely policy guidance and statements about the threat the Russian influence operation poses to election security. Secretary Mattis and General Dunford should provide extensive public outreach to the defense community about the threat and how to counter it. Perhaps they should think about forming public service announcements. European governments have been very effective in warning their publics about the danger of Russian disinformation. France and Germany were very strong on that, but you have to put the message out and we have not.

I offered one suggestion in my written testimony to look at how we could leverage the National Guard Bureau, working closely with State and local leaders in cooperation with the Department of Homeland Security, to enhance cybersecurity awareness and be able to detect patterns of influence, for example, if packed emails surface online in conjunction with the false rumors about potential electoral candidates. We need to start talking about this.

Another instrument is the State Partnership Program. The National Guard has partnered with the Lithuanian military, the Estonian military. They can bring back to their States information about how Russian influence works.

We are speaking today about protecting the homeland from continuous disinformation attacks, which alter how the average American thinks about their system of governance and their government. What the American people may end up thinking is that everyone is lying, everything is fake, and there is nothing that can be trusted. Then even the most trusted of American institutions, the Defense Department, the Justice Department, the FBI [Federal Bureau of Investigation], the Department of Homeland Security, the Office of the President, will mean very little to the American people. This is exactly how you break the internal coherence of the enemy's system according to Russian military doctrine. Unfortunately today we are doing most of this to ourselves without assistance from the Kremlin.

This is a matter of urgency. We have 9 months. We need to educate the American people in addition to enhancing, of course, our cybersecurity protections. But as the French disinformation attacks showed, what many of the organizations that looked like that disinformation was coming from—it was coming from American organizations. This is designed to be hidden. It adapts. We have to educate the American people about what they are going to confront on the November elections.

Thank you.

[The prepared statement of Ms. Conley follows:]

PREPARED STATEMENT BY HEATHER A. CONLEY

Mr. Chairman, Ranking Member Nelson and distinguished members of the Cybersecurity Subcommittee of the Senate Armed Services Committee, thank you for the

invitation to speak before this important subcommittee on a topic that is of utmost importance to the future of the United States and its national security: The essential need to ensure that the American people have complete trust and confidence in the fairness and accuracy of U.S. elections, be they at the local, state or federal level.

I am a professional outlier on this panel for I am not a cyber security expert, but I have spent the last several years at CSIS studying and understanding how malign Russian influence works in Europe, which we have described in detail in our seminal report, The Kremlin Playbook.[1] We have studied in detail how Russian economic influence has worked in five European countries (Latvia, Hungary, Slovakia, Bulgaria and Serbia) over a ten-year period to understand how Russia infiltrates a democracy and erodes confidence and credibility in how that democracy works. We have extended our research to include six more European countries (Italy, Austria, the Netherlands, Romania, the Czech Republic and Montenegro) which will culminate in a new report, The Kremlin Playbook 2, in early 2019. The Central and Eastern European region has constituted an extensive Russian laboratory for a variety of influence operations for nearly two decades. European Governments and citizens have been exposed to a full spectrum of Russian influence tactics that have collapsed weakened governments as well as systemically important financial institutions. Russian influence has fomented societal unrest and altered Western-oriented government policies.

Having said this, I believe Russian influence is less about physical cyber security (although cyberattacks are a useful tool) and more about (dis)information and influence superiority, which is how the Kremlin believes it will maintain its global preeminence as it addresses slow and long-term decline. According to the Czech Security Information Service, it is the Kremlin's goal to convince the average citizen that "everyone is lying," which in turn will "weaken society's will to resist" Russian interests.[2]

Therefore, *one of our first lines of defense is to develop a much deeper understanding of and a body of research into how Russia practices its influence operations as well as to study how European countries defend themselves against these ongoing operations.* Europe has been at this longer than we have. Our knowledge has atrophied. Our defense and intelligence officials must have the closest possible relationship with our European partners to develop effective and sustainable countermeasures against Russian influence.

Secondly, *it needs to be understood that Russian influence does not simply occur in and around a national election; it is a continuous and holistic series of operations that are designed to break the "internal coherence of the enemy system."*[3] It is true that elections are the most visible opportunity to harm a democracy when it is at its most vulnerable. We can observe that Russian influence operations and cyber infiltration may accelerate approximately two years prior to an election but this does not mean that Russian operations cease after an election. If anything, they simply adapt their methods to the outcome and alter their strategies to continue to degrade confidence in democratic institutions. Sustained Russian influence operations focus on those issues that are deeply divisive within a society, such as issues related to migration or questions of history or national, racial or religious identity. Today's Russian influence operations, just as their predecessor, Soviet active measures, exploit the weaknesses that are present within a society but they benefit from increasingly sophisticated means amid increasingly confused Western societies that are overwhelmed daily by a growing amount of information.

My contribution to this important discussion is to offer you what I believe European countries have done successfully to combat malign Russian influence and disinformation as well as increase cyber-protection. But before doing this, I will address the questions posed to all the witnesses today.

I do not believe the Department of Defense has a leading role to play in the cyber protection of U.S. elections. This is the purview of the Department of Homeland Security, which has struggled to develop effective policies to protect critical election infrastructure as distrust between the Federal Government and state as well as local election officials has grown. However, I believe the Department of Defense can

---

[1] Heather A. Conley and Ruslan Stefanov, *The Kremlin Playbook,* Center for Strategic and International Studies, October 2016, *https://www.csis.org/analysis/kremlin-playbook.*

[2] Jakub Janda, "How Czech President Miloš Zeman Became Putin's Man," *Observer,* January 26, 2018, *http://observer.com/2018/01/how-czech-president-milos-zeman-became-vladimir-putins-man/.*

[3] Dimitry Adamsky, "Cross-Domain Coercion: The Current Russian Art of Strategy," Proliferation Paper no. 54, Institut Français des Relations Internationales, November 30, 2015, *https://www.ifri.org/en/publications/enotes/proliferation-papers/cross-domain-coercion-current-russian-art-strategy.*

play a role that is highly complementary to the work of the Department of Homeland Security by rebuilding trust between state and federal officials, and building knowledge and awareness of the ever-present threat. This will not be easy. State and local election officials are unable to receive classified intelligence briefings. Candidates for office may not have received cybersecurity training or know whom to contact should they become the victim of illicit hacking or an influence operation.

We can learn from the French Government about how to combine military and civilian efforts to prevent cyber-destabilization. This month the French Ministry of Defense released its Military Planning Law, which prioritizes cyber risks and seeks to increase cooperation with telecommunication companies to enable them to scan networks for technical clues of ongoing or future cyberattacks. The civilian French Network and Information Security Agency (ANSSI) will provide a list of risk indicators to the Defense Ministry. These risk indicators only focus on technical aspects of security breaches and not on content (which is important to ensure First Amendment protections in the United States). The goal is to enhance early detection. A French white paper was released in conjunction with the planning law which outlined and defined the possible cyberattacks that France could suffer and identifies cyber-protection as a strategic priority.[4] The strategic review of France's cyber defense sets out six main goals: prevention, anticipation, protection, detection, attribution, and reaction.[5] The ANSSI provides cybersecurity awareness-raising seminars to politicians and parties. Could DOD produce something similar in cooperation with DHS?

While there is a role for the Defense Department to play in deploying offensive cyber capabilities should there be an attributable Russian attack on the United States election process, it would have to be part of a whole-of-government policy and strategy toward Russian influence operations, which at present the United States Government does not have—but urgently needs. Perhaps a more credible policy of deterrence would be for the United States Government to notify the Kremlin that future attributable attacks against United States elections would force the United States to seek to block Russia's access to the Society for Worldwide Interbank Financial Telecommunications (SWIFT). Although the Russian Government has developed an alternative system that may mitigate financial disruption internally, it could certainly hamper access to international bank accounts from the Kremlin's very wealthy inner circle—which may have more immediate impact.

There are two additional areas that the Defense Department could explore to enhance disinformation awareness and cyber-protection prior to the 2018 mid-term and 2020 presidential elections. First, it could use its extensive employee and military network to provide timely policy guidance and statements about the threat that Russian influence operations pose to election security. Secretary Mattis and General Dunford should provide extensive public outreach to the defense community about the nature of the threat and how best to counter it to sensitize the DOD community to the threat of Russian influence and misinformation operations in a public service announcement format. Another idea would be to consider engaging the National Guard Bureau to help develop and facilitate training of state and local election officials to enhance cybersecurity awareness and to be able to detect patterns of influence (for example, hacked e-mails surfacing online in conjunction with the spread of false rumors about candidates) in partnership with the Department of Homeland Security. Those National Guard units that have participated in the State Partnership Program (SPP) have served and developed relationships with European partners, and could also be particularly helpful in sharing information about Russian influence operations (United States forces serving in these countries have been the recipients of Russian misinformation campaigns) through the State Adjutant Generals who are very well regarded among state and local officials. State Partnership Programs particularly well placed for this would be the Pennsylvania National Guard (Lithuania), the Maryland National Guard (Estonia), the Texas National Guard (the Czech Republic) and the Michigan National Guard (Latvia).[6]

Simply put, the Defense Department must model the bipartisan and fact-based actions, behavior and awareness that will reduce societal division and help bridge the

---

[4] Martin Untersinger, "Cybersécurité: le gouvernement veut mettre les télécoms à la contribution pour détecter les attaques," *Le Monde,* February 8, 2018, *http://www.lemonde.fr/pixels/article/2018/02/08/cybersecurite-le-gouvernement-veut-mettre-les-telecoms-a-contribution-pour-detecter-les-attaques_5253808_4408996.html.*

[5] Olivier Berger, "Revue stratégique de cyberdéfense : l'Etat et les opérateurs pourront collaborer pour traquer les attaques informatiques," *La Voix du Nord,* February 8, 2018, *http://defense.blogs.lavoixdunord.fr/archive/2018/02/08/l-etat-et-les-operateurs-pourront-collaborer-pour-traquer-le-15570.html*

[6] See more at "State Partnership Program," National Guard, *http://www.nationalguard.mil/Leadership/Joint-Staff/J–5/International-Affairs-Division/State-Partnership-Program/.*

state and federal divide. As one of the most trusted institutions in the United States, the Defense Department must leverage that trust to mitigate malign Russian influence.

Turning now to the European laboratory of Russian cyber-destabilization, there are several important lessons that the 2017 European election cycle has taught us (and that Europeans have learned):

- The necessity of having a paper ballot either as the ballot of record or as a back-up to an electronic ballot. The Dutch and German national elections use paper ballots. The German Government has also focused on protecting the software that tallies the election results to ensure that these systems are not vulnerable to cyberattack.
- A unified and all-political party message on what is at stake as well as how to detect and understand Russian influence. The French and German Governments were particularly effective at early notification regarding the likelihood of Russian influence and announcing when data breaches occurred. There was sufficient trust in the institutions and their leaders to ensure that a majority of the public took heed of the warning, which reduced the impact of the Russian misinformation campaign.
- French and German media organizations set up fact-checking teams and social media platforms that cooperated with authorities to protect sensitive accounts. The French polling commission went so far as to warn against illegitimate polls coming from Kremlin-affiliated outlets that did not fit legal criteria for accurate polling. [7]
- In Sweden, ahead of the September 2018 elections, the Government plans to create a new agency to enhance the public's "psychological defense" against influence by identifying, analyzing and reacting to Russian influence attempts; this would also take place through increased funding for the Swedish intelligence services, and cyber-defense. [8] In January 2018, the Swedish head of security services (Sapo) warned against increased foreign influence operations ahead of the election, citing as examples forged letters of arms deals with Ukraine or fake reports that Muslims had vandalized a church. [9]
- Swedish Prime Minister Lǫfven plans to convene political parties to share protection and resilience strategies throughout the election process. The media would also take part in some of these meetings to bolster awareness of foreign influence.
- The chief of Sapo has increased information-sharing with European partners, and with other security services to better protect the election process; he argued that despite being a security service, openness was important to inform the public on the threat. [10]
- The Swedish Government is also discussing the inclusion of critical thinking skills in primary school curricula, teaching children how to spot fake news. Swedish Government authorities have initiated a series of public news literacy activities to help the Swedish public discern how truthful and fact-based information that receive. [11]

The U.S. Government has taken none of these positive, proactive steps—to my knowledge. The most proactive work being done in this space is taking place in U.S. think-tanks and universities through independent funding.

If we understood 2016 and 2017 to be exceptional years for all-encompassing Russian influence operations, we must reckon with the fact that 2018 has already witnessed significant Russian influence activities, particularly around the Czech presidential elections. There, in a close second-round election, the opponent (a former president of the Czech Academy of Sciences) of the preferred Russian candidate (outgoing president Milos Zeman) received an onslaught of disinformation during the second and final round of the campaign, from being called a pedophile to a Com-

---

[7] Laura Daniels, "How Russia hacked the French election," *Politico,* April 23, 2017, *https://www.politico.eu/article/france-election-2017-russia-hacked-cyberattacks/*.

[8] Andrew Rettman and Lisbeth Kirk, "Sweden raises alarm on election meddling," January 15, 2018, *https://euobserver.com/foreign/140542.*

[9] Gordon Corera, "Swedish security chief warning on fake news," January 4, 2018, *http://www.bbc.com/news/world-europe0-42285332.*

[10] 10 *Ibid.*

[11] "A practical approach on how to cope with disinformation," Government of Sweden, October 6, 2017, *http://www.government.se/articles/2017/10/a-practical-approach-on-how-to-cope-with-disinformation/*.

munist secret police agent who stole intellectual property. Milos Zeman won 51.4 percent to 48.6 percent. [12]

We watch with particular concern the upcoming Italian parliamentarian elections (March 4), Montenegro's presidential elections (April 15), Latvian parliamentary elections (September/October), Swedish parliamentary elections (September 8), and Moldovan elections (to be held before April 2019), where Russia has long-standing investments and would potentially seek to influence the outcome of elections in support of the Kremlin's interests. The very same methods that are being deployed to undermine the credibility of these elections are being actively pursued in the United States. This has been recently acknowledged by CIA Director Mike Pompeo. [13] So perhaps the most immediate and important step the Department of Defense could take—in concert with Congress—is to demand a whole-of-government approach to minimize the impact of Russian influence operations in the United States. A disjointed approach by the United States Government and the daily undermining of the legitimacy of United States intelligence and law enforcement agencies does the Kremlin's work far better (and cheaper) than any Russian influence operation could.

Senator ROUNDS. Thank you, Ms. Conley.

Dr. Harknett?

STATEMENT OF DR. RICHARD J. HARKNETT, PROFESSOR OF POLITICAL SCIENCE AND HEAD OF POLITICAL SCIENCE DEPARTMENT, UNIVERSITY OF CINCINNATI

Dr. HARKNETT. Chairman Rounds, Ranking Member Nelson, distinguished members, thank you for this opportunity to speak to you about this critical issue today.

We have a big picture problem. Throughout international political history, states have at times misaligned their security approaches to the strategic realities in which they tried to secure themselves.

In 1914, every general staff in Europe thought that security rested on the offense, and they found out devastatingly in World War I that they were tragically wrong.

France in the 1930s said, okay, we learned from the last war. It is a defense-dominant environment. We are going to rest our security on the most technologically advanced defensive works in history. But again, the fundamentals had changed and the Germans simply went around the Maginot Line.

Senators, with all due respect, I do not want to be France in the 1930s, but I think we are coming dangerously close to that myopia and the misalignment of strategy that follows from it. Our adversaries are working through a new seam in international politics. Cyberspace is that seam. Its unique characteristics have created a strategic environment in which our national sources of power can be exposed without having to violate traditional territorial integrity through war.

What we have been witnessing are not hacks. They are not thefts. It is not even simple espionage. What we must accept is the fact that we are facing comprehensive strategic campaigns that undermine our national sources of power, be they economic, social, political, or military. Therefore, I agree we must develop a counter strategic campaign to protect those sources that has as its overall

[12] Marc Santora, "Czech Republic Re-elects Milos Zeman, Populist Leader and Foe of Migrants," *The New York Times,* January 27, 2018, *https://www.nytimes.com/2018/01/27/world/europe/czech-election-milos-zeman.html.*

[13] Scott Neuman, "CIA Director Has 'Every Expectation' Russia Will Try To Influence Midterm Elections," NPR, January 30, 2018, *https://www.npr.org/sections/thetwo-way/2018/01/30/581767028/cia-director-has-every-expectation-russia-will-try-to-influence-mid-term-electio.*

objective a more secure, stable, interoperable, and global cyberspace.

With regard to the integrity of our elections, we have effectively left civilians, whose main focus is not security, on the front lines. That is not a recipe for success.

Specific to the Department of Defense's role in producing greater security in, through, and from cyberspace, we must adopt a seamless strategy of what I call cyber persistence, in which our objective is to seize and maintain the initiative. We must defend forward as close to adversary capacity and planning as possible so that we can watch and inform ourselves, disrupt and disable if necessary.

Our immediate objective must be to, first, erode the confidence adversaries now have in their ability to achieve and enable objectives. They are very confident.

Second, we have to erode their confidence in their own capabilities.

Third, we must erode those capabilities themselves.

We are well past the post on this. We need a comprehensive, seamless, integrated strategy that pulls to get a greater resiliency, forward defense, and when necessary, countering and testing cyber activity to reverse current behavior. We are not at step one. We are well past that. We actually have to reverse behavior.

Our security will rest on our ability to simultaneously anticipate how adversaries will exploit our vulnerabilities and how we can exploit theirs.

Cyberspace is an interconnected domain of constant contact that creates a strategic imperative for us to persist. This is a wrestling match in which we have to grapple with who actually has the initiative, being one step ahead in both knowledge and in action. If we do not adjust to this reality, our national sources of power will remain exposed and more of those who wish to contest our power will pour into this seam.

I, therefore, argue that we must make three critical adjustments.

The first is we have to adjust our overall strategic perspective. War and territorial aggression, which can effectively be deterred, are not the only pathways for undermining our national sources of power. In fact, because we have this effective strategic deterrent, we should expect our adversaries to move into this new seam of strategic behavior below the threshold of war.

Second, we must move our cyber capabilities out of their garrisons and adopt a security strategy that matches the operational environment of cyberspace. We must meet the challenge of an interconnected domain with a distinct strategy that continuously seeks tactical, operational, and strategic initiative.

Third, we must make the fundamental alterations to capabilities development, operational tempo, decision-making processes, and most importantly, as Bob referred to, overall authorities that will enable our forces to be successful. We cannot succeed using authorities that assume territoriality and segmentation in an environment of interconnectedness, constant contact, and initiative persistence. We cannot secure an environment of constant action through inaction. Strategic effect in cyberspace comes from the use of capabilities and having the initiative over one's adversaries. It is time for us to seize that initiative.

I look forward to explaining in more detail how we can pursue security through persistence during our Q and A. Thank you, Mr. Chairman.

[The prepared statement of Dr. Harknett follows:]

PREPARED STATEMENT BY PROFESSOR RICHARD J. HARKNETT

"DEPARTMENT OF DEFENSE'S ROLE IN PROTECTING DEMOCRATIC ELECTIONS"

The Subcommittee is concerned that, in the lead-up to the 2018 and 2020 elections, the Department and Government as a whole have not sufficiently deterred future interference, leaving our democratic institutions at risk to foreign intrusion.

The Subcommittee is correct in its concern. The likelihood of foreign intrusion (not just Russia, but other revisionist actors as well) is high due to the nature of this domain. Cyberspace is an interconnected domain and yet all our approaches rest on a principle of segmentation, instead of seeking synergies of expertise. Our adversaries have figured this out. Cyberspace is a new Seam in international power competition in which strategic effect can be produced below the threshold of war and the reach of traditional deterrence strategies. We should assume as a starting point that adversaries will engage in cyber operations against our national sources of power, including economic wealth and social-political cohesion. If we do not actively engage these strategic cyber campaigns, we will suffer. We need a new strategy that rests on a seamless operational environment of 1) integrated resiliency, 2) forward defense, 3) contesting adversaries' capabilities and 4) countering their campaigns. Through this new strategy, we can actively erode the confidence that our adversaries have in achieving their objectives and in their capabilities. Over time this may produce a deterrent effect, but that can only be achieved through persistent efforts to seize the cyber initiative away from our adversaries. [1]

In traditional great power politics, national sources of power were vulnerable only through direct violation of the territory upon which they centered. Thus, we came to equate strategic effects with war, and to narrow the central role of the state to promoting territoriality (its sovereign territorial integrity). The interconnected nature of cyberspace, however, means that now our national sources of power are vulnerable to manipulation without direct assault across territory. Strategic effects can occur without war through this new seam—and we should expect adversaries to explore it. We must contest this effort and seize back the initiative. In order for this to occur and positively affect the electoral cycle, we must position the Department to contribute to the defense of electoral integrity, protecting the vote and the voter. *Electoral integrity cannot be protected by leaving civilians alone on the front lines.*

Are the roles and expectations of the Department clearly defined with respect to protecting U.S. elections process from foreign influence in the cyber domain?

They currently are not sufficiently defined nor enabled. Most importantly, we must move away from 1) our "doctrine of restraint" [2] that forces us to defend in our own space after the first breach is detected, and 2) away from the tendency o view every intrusion as a law enforcement problem first. Cyberspace is an interconnected domain of constant contact, which creates a structural imperative to persist. Persistence in resiliency, forward defense and countering is necessary because the analytical categories of offense and defense do not actually hold in this space—it is too fluid and dynamic. As former Deputy Director of the National Security Agency Chris Inglis put it: "It's almost impossible to achieve a static advantage in cyberspace—whether that's a competitive [offensive] advantage or a security [defensive] advantage—when things change every minute of every hour of every day. And it's not just the technology that changes; it's the employment of that technology; the operations and practices." [3]

Our protection posture must be moved as close to the sources of adversarial action and capability as possible so that we can watch, react, disable, and disrupt at a speed of relevance (defined as one step ahead of the adversary). We forward deploy in terrestrial space, where actual time and distance still matter for defense, so why do we hesitate to do so in the one domain where time and distance are crushed and

[1] For more on persistence, see M. Fischerkeller and R. Harknett, "Deterrence is Not a Credible Strategy for Cyberspace," Orbis 63 1 (Summer 2017): 381–393.

[2] Department of Defence, DOD Cyber Strategy (2015).

[3] Chris Inglis as quoted in Amber Corrin, "Is Government on the wrong road with cybersecurity?, FCW: The Business of Federal Technology (May 21, 2013), *https://fcw.com/articles/2013/05/21/csis-cybersecurity.aspx.*

cannot be leveraged for defense? Garrisoning our cyber forces has created a great disadvantage for us and invites opportunity for our adversaries. *DOD is not on the front lines, which because of interconnectedness, are everywhere.* We need to secure through a persistent pursuit of the initiative if we are to manage this new seam in international power competition.

How can the Department use its national mission teams' offensive capabilities to improve deterrence?

National Mission Teams (NMTs) can eventually produce a deterrence effect, but not by relying on deterrence strategy. Cyber strategic effects do not come from mere possession and the threat of employment, but from actual use. It is critical to differentiate between deterrence strategy and deterrence effects in answering this question because they get conflated too often. We can achieve a deterrent effect through other means than a deterrence strategy. Deterrence strategy rests on the prospective threat of punishment or denial to convince someone not to take an action. This dynamic cannot work in a strategic environment of constant action. Cyberspace is a strategic environment of initiative persistence (one can always find the willingness and capacity to get one step ahead). Our NMTs must be charged with eroding adversary confidence and deployed capability, not sit idle as prospective threats to impose costs in the face of cyber operations below the level of war. Cyberspace operations should be treated as a necessary national security activity and as a traditional military activity. Persistent erosion of confidence and capability will shape adversaries' behavior, over time, toward more stable norms. If we make the strategic effects sought by adversaries inconsequential, their penchant for attack may diminish—then we may get a deterrent effect (i.e., adversaries may determine it is not worth it to confront us). But we will not get there without allowing our NMTs to hunt, disrupt, disable cyber activities, and thereby seize the initiative back from our adversaries. We must understand this cyber persistent space not as an unstable escalatory environment, but rather as a fluid environment in which the initiative is always in play and we must seek initiative control.

Is the Department's conception and implementation of deterrence sufficient?

The Department's Cold War conception of deterrence does not map to the realities of this new strategic environment. Deterrence is *an* approach to security, not *the* approach. We cannot rely on a strategy in which the measure of effectiveness is the absence of action if we hope to manage an environment of constant action. The cost-benefit calculus an adversary may hold within cyberspace is never stable enough for us to be certain that our static deterrent threats are credibly influencing adversaries. There are always new and cost-effective opportunities for them to explore. They can constantly manipulate the data, networks, tools, and vulnerabilities that are coming on-line daily thanks to the efforts of malware developers and the innovations of the market. The cyber terrain to secure and the means to traverse that terrain are always changing. There is too much incentive and potential for adversaries to refrain from persisting in cyber activities below the level of war.

In short, deterrence is a strategy reinforced by segmentation (borders/thresholds), sovereignty, relative certainty, and territoriality. Cyberspace by contrast is defined by none of those conditions; it is defined instead by its interconnectedness, constant contact, relative anonymity, and a lack of territoriality. Just as nuclear weapons precluded defense and necessitated deterrence, cyberspace below the threshold of war precludes deterrence and necessitates persistence. We must understand this space as a wrestling match in which we are in constant contact with the adversary and we are grappling to sustain the initiative through both our knowledge of what the adversary is likely to do and through our action anticipating what they wish to do.

How should our posture be improved to combat the threat of future Russian interference?

First, we need to build a posture focused not just on Russia, but on revisionist actors across the globe. We need to focus on the effects on our national sources of power we wish to prevent. To achieve this outcome, we need an alignment of forces, capabilities development, operational tempo, and, critically new authorities and decision-making processes that allow the Department to gain tactical, operational, and strategic initiative, continuously. We must operate in cyberspace globally and continuously, seamlessly shifting between defensive and offensive tactics to create an operational advantage—i.e., cyber initiative. By understanding our own vulnerability surface better than our enemies do, we can through resiliency and defending forward render much of their activity inconsequential. This can in turn help free our forces to focus on the truly consequential potential of strategic action below war,

to disrupt and disable their cyber activities, creating enough tactical friction in our adversary's operations to shift their focus toward their own vulnerabilities and defending their own networks. This can produce a strategic effect for us.

This will also require a new alignment with the private sector that makes a clear demarcation around protecting *human* speech. Bots cannot be afforded First Amendment rights. Trending on social media must reflect *human* majoritarian aggregation, and automated manipulation of that speech needs to be examined in our public policy. The Department should be enabled to disrupt foreign attempts at technical manipulation. 2016 was the Stone Age relative to the sophistication of cyber activities we are likely to see. Before the next presidential election, for instance, we will lose the capacity for audio-visual authentication due to Artificial Intelligence manipulation. We need policy changes to make the Department's capabilities more relevant to the private sector's defense.

What can the Department do to close the gaps—across the Federal Government and between state and local governments—that inhibit the protection of election infrastructure?

First, it is critical to recognize that there are gaps and that our adversaries are likely to engage in operations that exacerbate them. These gaps exist in the authorities, roles and responsibilities that we have put in place for protecting the voting infrastructure, and exist in the absence of a plan for protecting the information space so that the competition of election campaigns can be conducted fairly by Americans. Based on open source reporting, most State election boards have not prioritized security based on open source reporting and we have not aligned with the private sector social media platforms to produce a coherent plan of how Department resources could contribute to the nation's defense. Our current policy framework essentially rests on a reactive context. The Defense Support to Civil Authorities has not been construed in a proactive and on-going context of defense, which is what is needed to map to the realities of cyberspace. We cannot succeed with an emergency management/disaster relief/crisis framework that places us on the back foot and relegates action to 'cleaning up on aisle nine.' We need to consider authorities that allow DOD, DHS, and our intelligence community to employ a coordinated strategy of cyber persistence as described above. If one considers the approaches emerging among all of our allies, particularly the British, Germans, Australians and Israelis, they are all moving toward increased policy and organizational coordination and synergy. They understand that the answer to the challenge of interconnectedness is not segmentation of roles, responsibilities, and authorities but synergies across pockets of expertise. *The policy framing question you should ask yourselves in every discussion you have is whether the policy under question advances synergy or segmentation.* If it is the latter it should be rejected; if it is the former it should be explored. Right now our approach to defending our electoral integrity rests on the principle of high segmentation. That will expose us to clever adversaries moving forward.

Senator ROUNDS. Thank you, Dr. Harknett.

Dr. Sulmeyer?

STATEMENT OF DR. MICHAEL L. SULMEYER, DIRECTOR, CYBER SECURITY PROJECT, BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS, HARVARD UNIVERSITY

Dr. SULMEYER. Thank you, Chairman Rounds, Ranking Member Nelson, and distinguished members of the subcommittee. It is an honor to be with you today.

Before I get to the military's role, however, I would like to note that I am part of a team at the Kennedy School's Belfer Center that released a report a couple hours ago. It is a playbook for State and local election administrators, and it has got steps they can take to improve the cybersecurity of systems that they administer. It is based on field research by a wonderful research team. Many, many students contributed. I am very lucky to have one of the wonderful students here with us today. Corina Faist has flown down to join us.

So regardless of the role of the Department of Defense, these defensive improvements are essential. I want to make sure I hit that

right up front. Those recommendations that we put out today complement our last playbook for political campaigns to also improve their cybersecurity. It is essential that we make our elections harder to hack and that we improve resiliency in case critical systems are compromised. But we should also consider how best to counter threats abroad before they hit us at home.

So let me transition to how I see some potential roles for the military outside of the United States to protect our elections. There are two necessary conditions of posture that I see as critical: reconnaissance posture and force posture.

First, reconnaissance posture. Our cyber mission forces should constantly conduct reconnaissance missions abroad to discover election-related threats to the United States and provide indicators and warnings to our forces and decision-makers. There will never be sufficient resources to address all threats equally, so prioritizing threats to our democratic processes is critical. Otherwise, we cannot hope to disrupt these threats.

On force posture, our forces must be sufficiently ready to strike, strike against targets abroad that threaten our elections. Readiness is a critical issue for our armed forces today, and I would encourage Senators on this subcommittee to ensure they are asking tough questions about the readiness of our cyber forces just as they would about any other part of our military.

If the military's reconnaissance and forces are postured to focus on threats to our elections from abroad, there are four objectives that I think our forces should be prepared to pursue. It should go without saying that undertaking these actions should be consistent with international law and other relevant U.S. commitments.

Those objectives are: first, preventing attacks from materializing; second, preempting imminent attacks; third, halting attacks in progress; and fourth, retaliating, if necessary, after an attack.

On the fourth, let me just note I would emphasize that this retaliation needs to be timely. It has got to be timely since the more time that elapses after an adversary's initial attack, the harder it will be to message and communicate that our action is a direct response.

Across those objectives, proper training, thorough rehearsals, and coordination with other parts of our government are essential. Bringing military capabilities to bear inside or outside of cyberspace is always a serious matter, so it is critical to ensure that rules of engagement and questions about authorities are settled well in advance of any order to strike. Here, I would note that some of our closest allies like the United Kingdom and Israel have undertaken some national-level organizational reforms to streamline responsibilities for cyber issues. We may at some point want to consider something similar here.

One of the best cyber-related investments the Nation has made is in the national mission force, an elite group of network operators at Cyber Command. They defend the nation from an attack of significant consequence in cyberspace. I think it is very much worth considering what role the NMF [National Mission Force] can play to accomplish the objectives I described just now.

I might note for Senators that I have not discussed deterrence much so far. I very much support calls to deter our adversaries

from meddling in elections. Do not get me wrong. However, I would not want to bet the cybersecurity of U.S. elections on a policy of deterrence if I did not have to. Sometimes, like the prospect of defending against thousands of nuclear-tipped missiles, deterrence is the least bad option. That is not the case in cybersecurity. We have other options, like the ones I described just now, and we should employ them alongside strong policies of deterrence.

Finally, I would just note that information derived abroad from reconnaissance should be shared with relevant parties at the State and local level. I want to commend the Department of Homeland Security for working hard to promote information sharing over the last few years.

I would also like to encourage more thinking, especially among my colleagues in academia, to help Congress protect itself since Congress is so critical as a part of our democratic process, not just work accounts but also campaign accounts, personal accounts. These cannot be left vulnerable.

That concludes my prepared testimony. I look forward to taking your questions.

[The prepared statement of Dr. Sulmeyer follows:]

PREPARED STATEMENT BY MICHAEL SULMEYER

Chairman Rounds, Ranking Member Nelson, and distinguished members of the committee, it is an honor to be with you today. The need to protect the foundations of our democratic system is of vital importance, and there are several potential roles the military can play.

I am proud to be part of a team at the Belfer Center that is releasing a new report in the coming days: a playbook for state and local election administrators with steps they can take to improve the cybersecurity of the systems they administer. Regardless of what roles the Department of Defense assumes, these defensive improvements we recommend are essential. These 10 recommendations reflect months of fieldwork by the research team, including several exceptionally talented students. They are:

- Create a proactive security culture,
- Treat elections as an interconnected system,
- Have a paper vote record,
- Use audits to show transparency and maintain trust in the elections process,
- Implement strong passwords and two-factor authentication,
- Control and actively manage access,
- Prioritize and isolate sensitive data and systems,
- Monitor, log, and backup data,
- Require vendors to make security a priority, and
- Build public trust and prepare for information operations.

These recommendations complement our last playbook, which contained recommendations for political campaigns to improve their cybersecurity. Both reports can be downloaded from our website, belfercenter.org. It is essential that we make our elections harder to hack and to improve resiliency in case critical systems are compromised. Bolstering federal capacity to provide the kinds of support that state and local administrators request should be a priority.

In addition to improving defenses and becoming more resilient, we should also consider how best to counter threats abroad before they hit us at home. To that end, let me transition to how I see some potential roles for the military in protecting our elections. I will focus my remarks on roles that the military could play outside of the United States.

There are two necessary conditions of posture that I see as critical:

1. *Reconnaissance Posture:* Our cyber mission forces should be constantly conducting reconnaissance missions abroad to discover election-related threats to the United States and provide indicators and warnings to our forces and decision-makers. There will never be sufficient resources to prioritize all threats equally, so prioritizing threats to our elections and our democratic processes is crucial. If we do not prioritize collecting information abroad about election-related threats, than we cannot hope to disrupt them.

2. *Force Posture:* Our cyber mission forces must be sufficiently ready to strike against targets abroad identified by reconnaissance as threats to our election. Readiness is a critical issue for our armed forces today, and I would encourage the Senators on this committee to ensure they are asking tough questions about the readiness of our cyber mission forces just as they would about any other area of our military. Our forces must be ready to create different effects against a range of targets. Sometimes, they will not have much notice, so developing tactics that can be employed on the fly is important.

If the military's reconnaissance and forces are postured to focus on threats to our elections from abroad, there are four objectives that our forces should be prepared to pursue. It should go without saying that undertaking these actions would need to be consistent with international law and other relevant U.S. commitments.

1. *Preventing Attacks from Materializing:* Based on election-focused reconnaissance, U.S. cyber mission forces should develop options to disrupt the activities of those planning to meddle in our elections, and those who are in the early steps of doing so. Because these would be actions conducted by U.S. forces with a relatively long lead time, scenario-based plans should be developed and socialized with decision-makers so they are aware of the viability, risks, and benefits of different options.
2. *Preempting Imminent Attacks:* Reconnaissance abroad may provide indicators and warnings of an imminent cyber attack against election-related infrastructure, campaigns, and media and social media platforms. Our forces can prepare to neuter those attacks before they commence. Such actions would need to be undertaken rapidly as opportunities to strike may be fleeting, so developing options in advance to deliver effects promptly when so ordered is essential.
3. *Halting Attacks in Progress:* There may be situations when an adversary has already established access to a system, is in the process of denying access to data by legitimate users in the United States, or is already conducting operations to inject misinformation or steal information. In these cases, our cyber forces should provide options to decision-makers to disable these attacks by taking actions outside of the United States at the source of an attack.
4. *Retaliating after Attacks:* If the United States suffers an attack on its election infrastructure and democratic processes, policymakers may request options to respond in a timely manner. I would place emphasis on timely retaliation, since the more time that elapses after the adversary's initial attack, the harder it will be to communicate that our action is a direct response to that attack.

Across all of these objectives, proper training, thorough rehearsals, and coordination with other parts of our government are essential. Bringing military capabilities to bear, inside or outside of cyberspace, is always a serious matter, so making sure that rules of engagement and questions about authorities are settled in advance of any order to strike is critical. Here, I would note that some of our closest allies like the United Kingdom and Israel have undertaken some national-level organizational reforms to streamline responsibilities for cyber issues. We may at some point want to consider something similar.

I always appreciated how the Armed Services Committee has been a champion of supporting the Department of Defense's cyber mission force. Through the last several National Defense Authorization Acts, this committee, and its counterpart in the House of Representatives, has empowered Cyber Command with unique authorities and has engaged in necessary civilian oversight. One of the best cyber-related investments the nation has made is in the National Mission Force, an elite group of network operators under the command of the Commander of U.S. Cyber Command. According to the 2015 DOD Cyber Strategy, their mission is to defend the nation from a cyber attack of significant consequence. I think it is very much worth considering what role the National Mission Force could play to accomplish the objectives I described.

Senators might note that I have not discussed deterrence in this testimony. I very much support calls to deter adversaries from meddling in our elections. However, I would not want to bet the cybersecurity of U.S. elections on a policy of deterrence if I did not have to. Sometimes, like the prospect of defending against thousands of nuclear-tipped missiles, deterrence is the least bad option. That is not the case in cybersecurity. We have other options, like the ones I described previously, and we should employ them alongside deterrence.

Let me conclude with one final proposal for the military: when possible, relevant information derived from the reconnaissance it conducts should be shared with relevant parties at home. At times, some of this information may be useful to officials at the state and local level. I want to commend the Department of Homeland Security for working hard to promote information sharing over the last several years,

and more recently to provide clearances to state officials so they have greater access to important information.

That concludes my prepared testimony. I look forward to taking your questions.

Senator ROUNDS. Thank you, Dr. Sulmeyer.

First of all, let me thank all of you for some great insight, and I look forward to your thoughts in terms of the questions that we ask.

What I would like to do is to do what we call 5-minute rounds here. We will alternate back and forth. Then after we have done that once through, if we have time, I would go back through and do a second round depending upon the amount of time that we have and whether or not other members come.

Let me begin with mine. I am going to start with Dr. Harknett. You have written that restraint and reactive postures are not sustainable, that the United States needs a strategy that capitalizes on the unique attributes of the cyber domain. You have called for a strategy of cyber persistence where we are constantly engaged with our adversaries seeking to frustrate, confuse, and challenge.

How would your strategy calling for persistent engagement apply in the Russian meddling with our election as an example? Should this involve us contesting the malicious behavior at its source? What do you believe are the consequences of our failure to respond in cyberspace to the Russian election interference? Because, number one, we have got to be able to provide attribution to where it is coming from, and hopefully we have got that completed. But give me your thoughts on it. What would you say would be an example of persistent engagement with regard to what they have done already and what we expect them to do?

Dr. HARKNETT. Thank you, Senator.

So let us think about the Internet Research Agency. Right? I mean, we know about this center in St. Petersburg. We know that it controls a series of automated bots that are driving particularly well conceived information operations that are meant to be divisive. I do not know why we are according or why we should accord First Amendment rights to bots. It is not a free speech issue. If we have evidence of foreign manipulation, technical manipulation, of the social media space, that is not what the American people, from an educated standpoint, actually understand is coming at them. They think that this is a majoritarian aggregator trending. It is telling me, hey, this is where everybody is going. But if that trend is being driven by automated foreign intrusion, that is not an issue over free speech. That is an issue of direct foreign manipulation.

I agree with Dr. Sulmeyer. We need to have the reconnaissance, to your point about attribution. That is what persistence enables you to do, to start to get better at attribution. But we need to be able to move at the speed of relevance. So if in fact those bots are hitting us in a particular trend that is meant to be divisive, we should be able to have the capacity to at least disrupt if not disable that capacity.

So we do know where some of these capacities lie. By being persistent in our reconnaissance, we will get a better understanding of what our vulnerability surface is. We have to think about it that way. We tend to think about an attack surface. That is from their perspective. We have to get a better handle on what our vulner-

ability surface is. By being able to understand where our vulnerabilities are and anticipate where their capabilities map to that, again, a product of being persistent in this space, we can start to take those capabilities away.

Senator ROUNDS. Dr. Sulmeyer, do you agree with that?

Dr. SULMEYER. I do. I agree with the vast majority of what my colleague, Dr. Harknett, just said.

For me, even just to get a little more specific, the kinds of options that I would want to be seeing presented need to allow decision-makers some flexibility from lower-level actions like denying troll farm access to compromised infrastructure, to deleting some accounts, to erasing some systems if it comes to it. It is too important to take options off the table ahead of time. So as long as the option space is kept open, we can do it persistently or less persistently, but a wide range of options.

Senator ROUNDS. Mr. Butler, your thoughts?

Mr. BUTLER. I agree with both Michael and Richard on this. I would say that we need to be asymmetrical in our response. So I am a big believer in botnet disruptions and taking down bot infrastructure, as we just saw with Levashov, but we need to do that in a continuous way and that is a symmetrical response.

I think if you look at the Internet Research Agency in St. Petersburg, they are coupled to the Kremlin. You need to have an information operations counter-influence campaign where you begin to cut the funding and cut the support enablers behind that infrastructure. So we need to think about things differently. It should not be cyber on cyber, social media on social media. It has got to be a broader campaign.

Senator ROUNDS. Ms. Conley?

Ms. CONLEY. Yes. I will agree with absolutely the asymmetrical response. While trying to bring down the infrastructure of those bots, what they are doing, though, Russia exploits the weaknesses that it finds. So it is amplifying the weaknesses and divisions that are already appearing on social media. So how do we try to reduce the weaknesses?

This, again, gets back to the critical importance of exactly what this committee represents, the bipartisanship, fact-based, and getting to communities through a variety of methods to help inform the American people so when they see a trending site, let us look at that. What is underneath that? The only way we can really stop this from changing hearts and minds among the American people is helping them discern what is coming. We can do everything we can technologically to eliminate it. But the other part is just missing. We are not educating.

On the asymmetrical sanctions, my frustration—and I am sure many on this committee as well——

Senator ROUNDS. I am going to ask you to shorten it up because my time has expired.

Ms. CONLEY. Absolutely, sorry about that. Is to think about ways that we can focus on the Kremlin, on financial sanctions, on sanctioning the inner circle as ones attributable back to that, so not just in the cyber domain, focusing on financial sanctions and individual sanctions. That could be very powerful as well.

Senator ROUNDS. Thank you.

Senator Nelson?

Senator NELSON. So all of you sound like that you just do not think enough has been done and that we are not ready. Dr. Harknett, you have said that 2016 was the Stone Age compared to what is going to happen. So do you want to trace what you think will happen?

Dr. HARKNETT. Well, one of the things, back to the chairman's question about whether the lingering effects, is again we have got adversaries who are confident. There are other actors aside from Russia out there as well that are going to look at this space and say, hey, this is a space that I can play in and I can work in. Until we start to reverse that confidence, we are going to see greater experimentation.

Technologically, I will give you one example, Senator. My concern with regard to leveraging artificial intelligence and machine learning. I mean, this will be a step function, thus my Stone Age allusion, from where we are. We are going to—within the next 16 months, I am going to be able to take you and put you in a video in which you are saying something that you never said in a place that you have never been, and you are not going to be able to authenticate that you were not doing—that you had not done that and not been there. Just think about that as a tool for an adversary who wants to engage in disruptive social cohesion types of information campaigns.

Senator NELSON. Right.

Dr. HARKNETT. That is around the corner.

Senator NELSON. So, Ms. Conley, given that, you have already said that you do not think we have taken any positive proactive steps. Why do you think that is the case?

Ms. CONLEY. I think the executive branch refuses to recognize the threat. It refuses to put forward a national whole-of-government, whole-of-society strategy and bring all the agencies and tools of influence to bear on this. We have to think of this as a direct threat to the national security of this country. It has to receive the priority.

Also, to focus on what Dr. Harknett said, this is adaptation. If we are preparing for what Russia did in 2016, it will be very different in November. It will be very different in 2020. It will look more American. It will look less Russian. This is adaptation. We are already fighting the last war. We are not ahead of the new one, which is why I think education is so critical, that absent a U.S. Government approach, we are all going to have to do our part in our communities to inform the American people about the threat. It is unfortunate we cannot pull together and do this in a unified way.

Senator NELSON. So if we cannot get the Government to move, are there any private initiatives that would help?

Ms. CONLEY. What I am seeing is some very effective news literacy campaigns. I think, again, news sources, social media are doing fact checking. The pressure that Congress has brought to bear on the social media companies is changing their perspective. But, again, we are so late to need. This has been ongoing. This campaign is only intensifying, and we are just getting our arms wrapped around this. So this is where every Member of Congress

has to return to their home district and talk about this in very clear ways.

Senator NELSON. Amen to that.

Dr. Harknett, on the example that you gave of the next level of technology, of which something can be created that looks real, acts real, feels real, et cetera, if Cyber Command were to adopt your thinking, knowing what the threat is even greater in the future, what would you suggest that they change the way that they are doing their operations?

Dr. HARKNETT. I think it is very important to expand this notion of defending forward, this notion that we need to be as close to the source of adversarial capability and decision-making as possible. This is not a space in which time and geography is leveragable for defense. So when we think about the notion of front lines, the front lines are everywhere. Right now, our general approach has been to defend at our borders, at our network, which actually means that we start defending after the first breach, and we are already playing catch-up.

So I concur with the notion of adaptability here. It is all about anticipation. So when Bob Butler talks about asymmetric, that is what I would talk about in terms of being able to be one step ahead. We have to be able to anticipate the exploitation of our vulnerabilities. You need to be able to be defending as far forward as possible. In terrestrial space, we defend forward. We are not defending forward in cyberspace right now.

Senator NELSON. Thank you.

Senator ROUNDS. Senator Gillibrand?

Senator GILLIBRAND. Thank you, Mr. Chairman and Mr. Ranking Member, for having this hearing.

Thanks to all of you for your testimony. I agreed with a lot of it.

So to Professor Harknett, I appreciate your effort to redefine cyberspace and the challenges we face in operating within it. Were Russia to have bombed one of our States rather than attacked our election infrastructure, we would treat it just like an attack, as you said. But because of the way in which we set up our cyber capabilities, which we have done for good reasons, including privacy and States rights, it seems to me that the DOD is hamstrung in trying to properly respond to an attack on our democracy.

I have asked this in many settings, and every single time they said it is not our job.

So you argue that we need to consider authorities that allow DOD, DHS, and our intelligence community to employ a coordinated strategy of cyber persistence and recommend looking at approaches emerging among all of our allies. Can you expand on what kind of authorities we should be considering and what we might learn from our allies?

I ask this because I have put this question to the Department of Defense in every setting we have had, any conversation about cyber, and every response is we do not have the authorities and the States rights issue. It is not our job. I cannot, for the life of me, understand why they do not see it as their job because if another country bombed any one of our States, then that is a declaration of war and we would have responded from the military. We are not

doing that in this regard, and it seems really off-putting to me. Their response is often, that is Homeland Security's job. They can call us if they need us, but they have not. I understand why that is probably not the case because a lot of secretaries of state in a lot of States think it is their job, not anyone else's job, and they do not want to relinquish that control.

So I would like your suggestions on how to write the authorities that you think are necessary, but also I have really tried to push National Guard as a possible place where this can be done because the National Guard already serves the States. They are already under control of the governors. So why not amplify what we are already doing with our National Guard and Reserve to give them the expertise in cyber but actually delegate this mission specifically to them in conjunction with all the other assets in the military?

So to all of you, you can answer this question. You start, Dr. Harknett, since you addressed it a little bit in your opening remarks about what authorities can we give. How can the National Guard be useful, and how do we get this done? Because it is frustrating to me that we are not doing it.

Then just a third thing to add to your answer. I do have a bill with Lindsey Graham to do a 9/11 deep dive style analysis of the cyber threat to our electoral infrastructure. It is a bipartisan bill. You know, whether we ever get a vote on it, I will never know, but that would be a great first step in my mind to at least just get a report and say these are the 10 things you need to do to harden our infrastructure. So maybe comment on those three ideas.

Dr. HARKNETT. Thank you, Senator.

You mentioned our allies, and I think Michael had some work that he has been doing as well analyzing them. I think if you look at the UK [United Kingdom], for example, you look at the Israelis, you look at the Australians, their first default in cyberspace is to ask how do we find synergy, not segmentation. Our entire approach to this space has been starting with who has divided roles and responsibilities. So I think we can learn something from our allies right now in terms of their orientation to trying to find synergy rather than segmentation. That should be our first policy framework question.

But in terms of authorities, I think there is a false debate, say, for example, between 10 and 50. So when I argue for a seamless notion, I am suggesting that we understand title 10 and title 50 as actually mutually reinforcing, not defined as, again, segmentating. They segment in Congress in terms of oversight, and I get that, but they do not segment in operational space. We should actually understand and reinterpret, I would argue, those authorities to emphasize where a synergy and where there is seamless reinforcement rather than looking at those authorities as something that divides and puts us into different lanes.

In terms of the National Guard, I think the cyber protection teams and force type of an approach would be appropriate. We need to get at this, Senator. So if that is the best mechanism, there is expertise at that level.

Ms. Butler has talked about leveraging our private sector. Through National Guard, as well as Reserve, we have a capacity. If you look at the Brits, they are looking at cyber civilian reserve

force. I think that is another interesting way of thinking about this.

So ultimately if we need to do a deep dive, I think we do. Right? I think we have authorities that are structured for a terrestrial space that do not map to the realities of this human-made interconnected space. Authorities are what we should do last. We should figure out what our mission is. We should develop the organizations to pursue those missions, and then we should authorize them to do it.

I would submit to you that one of the major problems that we have faced is we have been continually trying to shoehorn our cyber forces into existing authorities and working backwards from the way we should be working.

Senator GILLIBRAND. Ms. Conley?

Ms. CONLEY. Senator, I think the National Guard is an area that we absolutely should explore, and I mentioned it in my written as well as far as education, bringing together DHS, DOD, working with community leaders at the State and local level.

On the 9/11 Commission style, cyber is critical pillar of this, but it transcends it as well. We need to look at Russian economic influence. We have to look at a whole range not just of Russia as the adversary but other adversaries that will use cyber disinformation and economic. So please broaden that out. They will find any seam, State, federal, First Amendment, privacy. That is where they will be, and that is why we cannot get locked into those seams.

Mr. BUTLER. Senator, I take it from two different angles. One is clean-sheet everything. What do you want to do? Let us refocus the authorities. Catherine Lotrionte's work here in looking at countermeasures is a great example of that. Her legal interpretation of the Tallinn Manual is very different than what most people are saying these days.

The other thing is I am involved in exercises where I am blending physical and cyber together and looking at what we can do with physical authorities in cyberspace. So I am working with the Army Cyber Institute on an activity where we have a natural hazard and a nation state actor is manipulating inside of it. How do you get a rolling start? You can use our authorities. The military has the ability to use an immediate response authority to create a rolling start. We need to leverage. We need to reinterpret and leverage these kinds of things as we go forward.

A part of that is the National Guard Bureau. We have unevenness within the stand-up of our National Guard activities both in the air and now with the Army. We have both cyber and information operations. I think we could create pockets of talent. I mean, Washington State has a phenomenal industrial control system security unit. Maryland has a fantastic unit where they leverage a lot of NSA [National Security Administration] expertise. We have got units spread around the country. We need to create a construct of cyber mutual assistance across boundaries, across State borders. Again, I think we can do that. We have just got to sit down and plan together a campaign in that regard.

Senator ROUNDS. While the Senator's time has expired, if you could expedite your answer, we will let you finish up as well, sir.

Dr. SULMEYER. I will go real quick. I support all the goodness just said.

Abroad, I do not believe the kinds of activities I described earlier need new authorities.

On the deep dive, I would say great. The Belfer Center's work over the last year has tried to get a start on that. So we hope we can be of support.

On coms and education, there is a part of me that wonders if that by saying "cyber," the response is help desk. By not describing it in a way about warfare and propaganda and foreign influence, we do a disservice to the real problem.

Thank you.

Senator ROUNDS. Senator Blumenthal?

Senator BLUMENTHAL. Thank you, Mr. Chairman.

I want to thank all of you for being here. I am very familiar with the work done by the Belfer Center in particular, and thank you all for the work that is done by each of your organizations.

I want to first tell you—you probably already know—that the immediacy and urgency of this task was reinforced this morning before the Senate Intelligence Committee where Dan Coats, the Director of National Intelligence, said, "There should be no doubt that Russia perceives its past efforts as successful and views the 2018 midterm elections as a potential target for Russian influence operations." That statement would be beyond conventional wisdom. It would be unnecessary to state because it is the consensus of our intelligence community. It has been broadly accepted by everyone except the President of the United States. In my view that is the elephant in this room, that the President refuses to acknowledge this threat to our national security.

So I put that on the record simply because we can propose all the great ideas in the world. Some very good ideas, as a matter of fact, came from a report done by the Senate Foreign Relations Committee. It is a minority report by my colleague, then-Ranking Member Senator Cardin, called, "Putin's Asymmetric Assault on Democracy and Russia and Europe Implications for United States National Security." It makes some very good proposals.

I would be interested to see the Belfer Center's release today, and in fact, without even having seen it, Mr. Chairman, I ask that it be made part of our record.

Senator ROUNDS. Without objection.

[The information referred to in Appendix A.]

Senator BLUMENTHAL. But I think we need to make progress on gaining acceptance at the highest levels of the United States Government—let me put it as diplomatically as possible—for the proposition that Russia attacked our democracy. In my view it committed an act of war. They are going to do it again unless they are made to pay a price for it, and that includes enforcing sanctions passed overwhelmingly by this body 98 to 2, still unenforced. So the talk about retaliatory measures in real time, Dr. Sulmeyer, I think is very well taken. But why should the Russians take us seriously when the President denies the plain reality of their attacking our country and the sanctions that would make them pay a price are still unenforced?

All of that said, I want to raise another topic, which I think so far has been untouched, the social media sites, Facebook, Google. Let me ask each of you if you could comment on what their responsibilities are and how they are meeting them in this disinformation, propaganda campaign using bots and fake accounts which have been appearing on those sites. Mr. Butler?

Mr. BUTLER. I think, Senator, the response—and I have talked with a couple of the web-scale companies about this—is aligning with what we have already seen in the counterterrorism fight. In that space what you see is them actively, proactively looking for disinformation, in the case of terrorism, of course, looking for recruitment. I think the challenge is guidance with regard to counternarratives or alternative narratives in that space. That needs to be done with others. But I think that is where we need to head. They have the ability based on their reach and their fusion engines to really help us move much more quickly into active defense in this space and not just to do it from a cyber perspective but from a counter-influence perspective which I think is so critical.

Senator BLUMENTHAL. Thank you.

Ms. Conley?

Ms. CONLEY. Thank you, Senator.

I would just note that building the awareness of what Congress has already done to force the social media companies to really take a very deep look at this has been very helpful.

I would suggest to you that I think Russia will adapt their tools, that this will look more and more American, which will get more and more into First Amendment issues because that is a weakness to exploit here.

So what I would commend, in the interest of being ahead of the curve and not behind it, is we start looking at how social media engines can start detecting what looks like it is American origin but it in fact is not. So that would be the next step I would recommend.

Senator BLUMENTHAL. Thank you.

Dr. HARKNETT. I think we have to move away from a partnership model, to be perfectly honest with you. We have been talking about a public-private partnership for 25 years. I published about this 25 years ago. The problem is that partnerships require shared interest in the beginning of the morning. The private sector has a very specific interest: profit making. The state has a very specific interest: security providing. We should recognize and grant that they have a different interest.

We need to move us to an alignment model. How do we structure incentives within the marketplace for them to achieve their primary objective, which is profit making, while producing an effect that the state requires, which is enhanced security?

Until we actually start to think about how can we shape and incentivize that behavior and recognize that we actually have very different interests in this space—I mean, that is Strava fitness band company a few weeks ago produced a heat map that exposes all of our forward-deployed troops. I would submit to you that nobody at their board meeting, when they came up with this really great idea of releasing that heat map—and they said, look, our stuff is in the real dark places, and they thought that was really cool. Ten years ago, the intelligence capacity that a state would

have had to have found all of our forward-deployed troops—think about that. This was produced by a fitness company.

There are non-security seeking, security relevant actors in this space. That is the way we have got to think about them. Let us meet them on their grounds and start to get them to align towards the security needs that we have.

Senator BLUMENTHAL. Thank you.

Dr. SULMEYER. Briefly I would just note the interests are not aligned, and that is really the most essential part and to not treat them all the same. Not all the companies have gone through the same amount of self-reflection. Some have not; some have. We should be honest about that.

Finally I do not think we should limit this to social media companies. There is a lot of companies up and down the stack, a lot of different types of people on the Internet who have an interest in this type of work.

Senator BLUMENTHAL. Thank you all.

I apologize, Mr. Chairman. I have gone over my time.

Senator ROUNDS. What I would like to do is another round. Okay? Let us do it this way. Let us do one more round so that everyone has an opportunity. We will make it 5 minutes. I would simply say that for those of us up on this end—and I went over as well—let us phrase it so that when we hit the 5 minutes, whoever is final speaking on it will have their—that will be the last one and we will move from there.

So with that, let me just begin with this very quickly. Right now, we are looking at changing our hats, our dual hats. Right now, within the cyber community, we have a dual-hatted individual for both title 10 and title 50 operations and so forth. We are looking at separating those into separate items: title 10 one side, title 50 on the other. The cybersecurity side would be separated out from the NSA side and so forth. We had a lot of discussions over it. We were concerned at first that they were going to go very, very rapidly. Now there is the discussion about whether or not moving in this particular way is quick enough.

I just want to know your thoughts about whether or not we are actually approaching the challenges that are facing us in the right way with regard to the organization of government as a whole. Can I just very quickly go across and just ask each of your thoughts about whether or not we are moving in the right direction as to how we are arranging so that we can respond to these types of threats? I will begin with Mr. Butler.

Mr. BUTLER. Thank you, Senator.

Let me start with the CYBERCOM/NSA issue. My sense is we are at a point where we have got enough of the infrastructure developed to really work within Cyber Command, that we are not as dependent as we once were on the National Security Agency.

I think the other part of this is as we move forward with the kinds of influence strategies that we are talking about, we need to have a way of checking and understanding whether it is working. We need an activity that understands this space that can help Cyber Command make adjustments along the way.

So I support the split and support where we are trying to go as we move forward. As we take a look at those two elements and we

put it into a larger DOD IC [Intelligence Community] and whole-of-government, whole-of-America construct, I go back to what I put in my written statement. I think from my perspective, having been through this both in uniform and doing information operations campaign planning and where we are today, we need to get the best of America into this space. There is a role for DHS. The FBI is very engaged. There is a role for the Department of Defense that goes beyond the National Guard Bureau that ties in with the intelligence community. There is a role for trusted private sector partners in this space. As a matter of fact, you cannot scale without it. So I think we have to align.

Senator ROUNDS. Thank you.

Ms. Conley?

Ms. CONLEY. The organizational structure gets to the reason why we needed a comprehensive 9/11-type commission because we are horribly structured for this particular challenge. It falls within the streams of law enforcement, intelligence, defense, education, awareness, and that is why we need a deeper dive to get to a reconfiguration. Just as we did after 9/11 with the DNI and DHS, we restructured ourselves. We need to do that again.

Senator ROUNDS. Thank you.

Dr. Harknett?

Dr. HARKNETT. I fully concur that we should do that deep dive, and I would urge us to reconsider the split of the dual hat. I know that that is not the current view. This notion of my litmus test. Are you producing more synergy or are you producing more segmentation? There is not one of our allies that is moving in that direction.

Senator ROUNDS. Let me just ask one question on that very quickly because one of the items was is that we know that on the title 50 side, on the NSA side, they love to be deeply embedded and they do not want to be seen. There is a real concern out there that if they actually actively and more persistent that they are constantly being seen, that that interrupts their capabilities to be the intelligence gatherers that they are. How do we then allow for that constant and persistent activity if they have the same concern about they would really rather not been seen? They just simply want to be the deep ears for us.

Dr. HARKNETT. So I think having the dual hat enables that kind of determination to be made. The sensitivity of both when and where we are going to make certain tradeoffs and where that seamless between intelligence and——

Senator ROUNDS. But it is not working today. Is it?

Dr. HARKNETT. No. I think it can. I think it can, sir.

Senator ROUNDS. But we do not have evidence.

Dr. HARKNETT. But if you look at our adversaries, why are they not worried about burning capabilities? Why are they not worried about—we have had a high-end right kind of focus to all of this both in the recon phase and in the force phase that I think has actually been distorting of this space.

Senator ROUNDS. I am going to move over very quickly because Dr. Sulmeyer has been shorted each time around here.

Dr. SULMEYER. You always pick on the Harvard guy.

[Laughter.]

Dr. SULMEYER. I think we are back to different interests. The two different institutions have matured and now they have different missions, different jobs to do. The current structure, what you can say for it, is very efficient decision-making because it is one person who makes the decision. I think it is time, though, for two different and for an adjudication to be made for which priorities are going to take precedence each time.

Senator ROUNDS. Thank you.

Senator Nelson?

Senator NELSON. But until we evolve into that new structure, we are stuck with what we have. We set up these Cyber Command national mission teams to disrupt the Russian troll farms, the botnets, the hackers, all engaged in attacks on our democracy, re the elections. We can identify them, the infrastructure they use. We can identify their plans, their operations. We can do everything that we can to stop these activities, but if you do not do anything, it is not going to happen. Until the existing structure that we have—the Secretary of Defense walks into the room and says, boss, and his boss is the commander-in-chief—until he says, boss, we have got to act, nothing is going to get done.

So are we describing a situation that we are defenseless in this 2018 election?

Mr. BUTLER. My sense, sir, is no. My recommendation is, in the homeland defense mission of the Department of Defense, we should stand up a JIATF [Joint Interagency Task Force] and move forward as we begin to move to another level, which would be a national security task force. But in the interim, this committee has jurisdiction. The Secretary has prerogatives to set up a JIATF in support of homeland defense. This is a homeland defense issue.

Dr. HARKNETT. I would just add one. I think it is a defend the nation issue.

Senator NELSON. I think you are right. I think this is as clear an attack on the country as if you lobbed a missile or if you lobbed an artillery shell.

Senator Blumenthal wanted to ask the question. One of you had stated that it is going to morph into where the attacks are going to look more American. Would you expand on that, please?

Ms. CONLEY. Senator, that was me.

It is in part from some of the lessons we learned from the French presidential election. The last cyber attack, which happened within the last 24 hours of the campaign—it was a combination of both hacked emails from Macron's campaign, as well as made-up messages, and it was all mixed in between. What we understand—and I do not have access to classified briefings from our French colleagues—where the source came from looked like it was coming from the United States, from United States organizations. Some of this is tied into adaptation where they do not want it to look like a Russian bot. They do not want it to look Russian. They wanted to originate from other sources to confuse and make attribution questionable in those last few moments.

So my intuition tells me that more and more of these attacks will look like they are coming from America. It will obscure attribution, and then people will say this is their First Amendment right to say these things and put forward these—that is the problem.

Senator NELSON. How did the French counter that?

Ms. CONLEY. Well, very gratefully, the French have a very unique—they have a blackout period 24 hours before an election. It is a reflection period. Because the French Government and intelligence agencies had made very clear repeatedly and publicly that this was likely to happen, French media were very responsible. They could not fact check the material in time. The reflection period would not move forward. In fact, that last major attack was really thwarted because both of a law but also a lot of French proactive steps to inform their public that this could happen.

Senator NELSON. That was in the last 24 hours before the French election.

Ms. CONLEY. So what had happened, it was the presidential election debate between Marine Le Pen and Emmanuel Macron. It was the Wednesday before the election on Sunday. In that debate, she began to hint that there may be some information about potentially Mr. Macron's overseas bank accounts and sort of hinted at this. Then about 24 hours later, the document release happened. So one could speculate that there was some coordination. But because it hit so late, it really did not have the impact. But, again, responsible media, Government warnings, and the reflection period all prevented something that, if it would have happened 72 hours before, may have had a different impact on that election.

Senator ROUNDS. Senator Gillibrand?

Senator GILLIBRAND. Thank you.

Just following up on a couple things. You said the Belfer Center already has done a deep dive on how we were hacked and ways to prevent it. Is that true?

Dr. SULMEYER. Senator, the two reports are about the practices that campaigns and State and local officials can take based on field research about what they found as vulnerable and techniques that were effective in the past, so ways to shore up those defenses. It is not going to be that kind of a deep dive like you are——

Senator GILLIBRAND. Have you distributed that to the 50 States?

Dr. SULMEYER. I believe so, yes.

Senator GILLIBRAND. Have you gotten comments or any response back?

Dr. SULMEYER. It went live today.

Senator GILLIBRAND. So I would like to request that you brief this committee on what the responses are to each of those efforts to outreach the different States and a copy of the report for all committee members so that we have our own first draft of what our 9/11 deep dive might ultimately look like because this has to be done. It is striking to me that there is no sense of urgency by this administration. It is absolutely crazy as far as I am concerned. I want to work towards elevating this issue, and your work will help us do that.

Dr. Harknett, you mentioned in your comments that bots do not have free speech rights. I could not agree with you more. So what kind of legislation do you think we could write or could be written to say we expect these platforms, whether it is Facebook or Twitter or Instagram or any other online community, to not sell its technology to fake entities who are posing as real people? The reason I say that is it is simple fraud, as far as I am concerned, because

you are doing it for the purpose of changing someone's mind, distracting them, giving them false information. I believe it should be illegal under the same analysis that we have for fraud statutes. How would you go about trying to take away those free speech rights that are given to non-entities today?

Dr. HARKNETT. Thank you, Senator.

So I am not a lawyer, but I would build on what you just said. I think the notion of our default to fraud—so if in fact what you are trying to sell is trend, if that is the actual operative thing that you are trying to—then that actually should be capturing human behavior. We really have to think through—I mean, this is very tricky. But legislatively we have to separate out human behavior from automated behavior, and automated behavior can be classified as falsification of trending, if you wanted to capsulize it in that fashion. So I think the notion of understanding technical manipulation of the space is not smart marketing. It is manipulation and therefore should be out of bounds.

Can I make one quick comment on your deep dive?

Senator GILLIBRAND. Yes.

Dr. HARKNETT. I would look as another example, Eisenhower's Solarium exercises back in the 1950s. President Eisenhower said, okay, what is going to be our macro level grand strategy? Set up three competing teams to come up with what those strategies should look like, and that is where containment and deterrence came from. It is an interesting alternative approach, but we get at the same sort of things that you are looking at.

Senator GILLIBRAND. Like a national competition?

Dr. HARKNETT. Well, he brought together three very specific groups of experts. They were given access to classified information, but they worked as independent teams. Then they were brought together to knock heads over what the best route to a grand strategy looks like.

We do not have a cyber grand strategy, and we do not have a grand strategy for cyberspace. I can tell you the Chinese do. They have announced it. They are going to be the number one AI [Artificial Intelligence] country by 2030. We need to start to think in those kinds of grand strategic terms.

Senator GILLIBRAND. Other thoughts?

Mr. BUTLER. Yes. Senator, I would build on the Honest Ads Act. You have got elements in this particular legislation which gets to what we want online platforms to do. They can identify botnet infrastructure and are beginning to identify infrastructure that has origin in elements that are nefarious. I think I would add to that as one way of kind of tackling this issue.

The second point. I do not want to disagree too strongly with my colleagues here, but I have worked in the private sector and I have worked on the public sector side. I know that there are models that can work to align incentives. The enduring security framework is a good example of that. We have had it work before. When you show private sector and national security government elements working together a threat of this magnitude and you provide some type of limited liability protection, you can get there. It took us a long time with Facebook, Twitter, and Microsoft to get to pulling terrorists' data offline, but they are doing it now. My sense is the

sooner we get into this process with creating an alignment of not only incentives but understanding of the problem—and again, it is not with everyone. It is with folks who can do things on scale and really help us as a nation.

Senator GILLIBRAND. Thank you.

Thank you, Mr. Chairman.

Senator ROUNDS. Thank you, Senator Gillibrand.

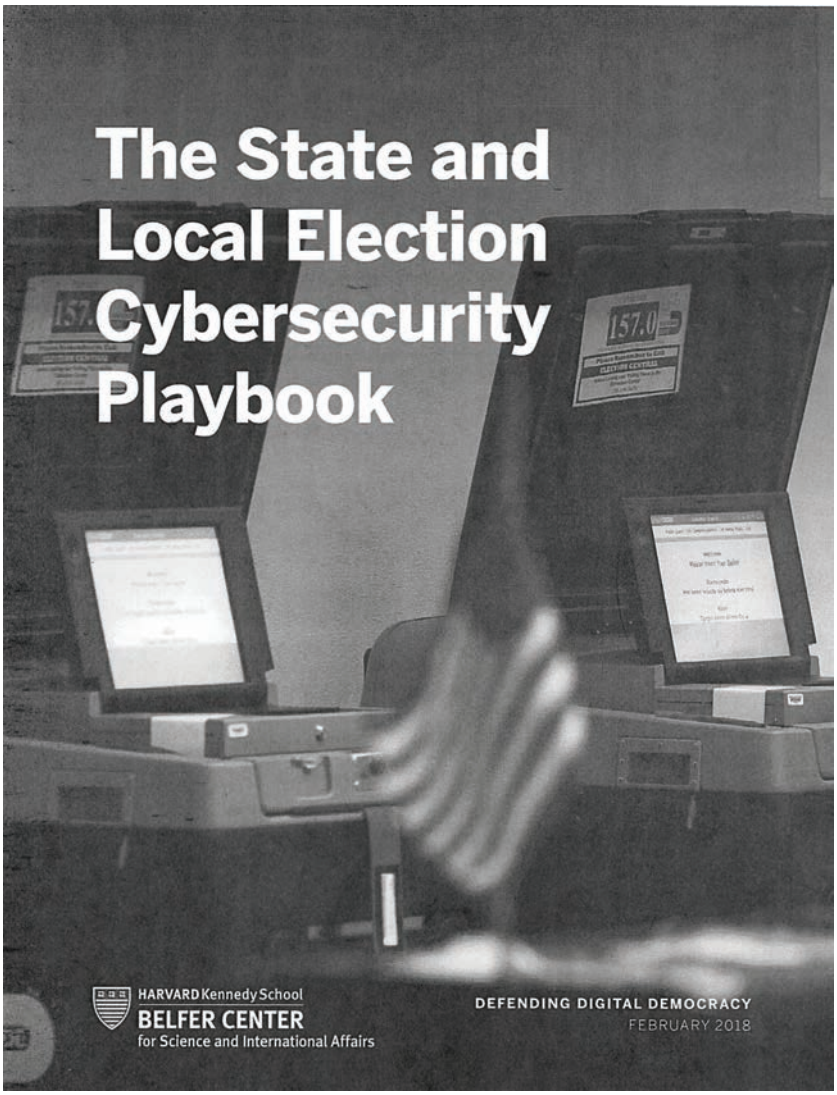
First of all, let me just take this time to say thank you very much to all of our witnesses for your time. You spent an hour and a half with us today. It has been greatly appreciated. I would suspect that we will be speaking again in the future as we continue to learn more about the challenges and the threats that face our country. It is not going to get better. It is going to get worse. We all recognize that. Our challenge is to make sure that we have the right long-term strategies and that they are being properly implemented. As such, I think we have got a lot of work to do.

With that, once again, thank you. Thank you for the participation of our members here today.

At this time, this Subcommittee meeting is adjourned.

[Whereupon, at 3:53 p.m., the Subcommittee adjourned.]

APPENDIX A


The State and Local Election Cybersecurity Playbook
HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs
DEFENDING DIGITAL DEMOCRACY
FEBRUARY 2018

Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/D3P

Design & Layout by Andrew Facini

Figure Illustrations by Jordan D'Amato

Cover photo: Voting machines in Miami Shores, Fla., Nov. 8, 2016, (AP Photo/Lynne Sladky)

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DEFENDING DIGITAL DEMOCRACY
FEBRUARY 2018

The State and Local Election Cybersecurity Playbook

Contents

Defending Digital Democracy Project: About Us

We established the Defending Digital Democracy Project (D3P) in July 2017 with one goal: to help defend democratic elections from cyber attacks and information operations.

There are two groups on the frontlines of defending democracy: (1) political campaigns, which enable citizens to pursue elected office; and (2) election officials, who ensure the election process is free and fair. Last year, we set out to provide campaign and election professionals with practical guides to the most applicable cybersecurity best practices in advance of the 2018 midterm elections. In November 2017, we released "The Campaign Cybersecurity Playbook" for campaign professionals. Now, in February 2018, we are releasing a set of three guides designed to be used together by election administrators: **"The State and Local Election Cybersecurity Playbook," "The Election Cyber Incident Communications Coordination Guide,"** and **"The Election Incident Communications Plan Template."** What follows is The State and Local Election Cybersecurity Playbook.

D3P is a bipartisan team of cybersecurity, political, and policy experts from the public and private sectors. To better understand both the cybersecurity and other challenges that elections face, our team of nearly three dozen professionals spent six months researching state and local election processes. We visited with 34 state and local election offices, observed the November 2017 elections in three states, and interviewed leading academic experts, election equipment manufacturers, and representatives of federal government agencies. We conducted a nationwide security survey with 37 participating states and territories, which identified detailed nuances in election processes and their corresponding risk considerations. We hosted two state election cybersecurity conferences where we engaged state and local election officials in "tabletop exercise" election simulations to increase awareness of the cybersecurity threats they face and improve their ability to mitigate those threats.

This research taught us many things. Most importantly, we learned how difficult it is to defend the multifaceted nature of the elections process. In the United States, elections are among the most complex and decentralized operations in either the public or private sectors. Every state and locality is unique. We were humbled by the intricacies of election operations in each state we visited, and inspired by election officials' incredible level of commitment to the democratic process. We also learned that the leadership of election officials is critical in creating a more secure system. Secretaries of state, election board members, state election directors, and local election administrators set the tone—it's ultimately their job to create a culture in which all staff make security a top priority.

This Playbook is intended for leaders at every level who play a role in running elections. While the future threats elections face are multifaceted, one principle stands clear: defending democracy depends on proactive leadership. This Playbook focuses on the U.S. experience, but it is also relevant to election officials around the world facing similar threats. We have designed it to identify risks and offer actionable solutions that will empower state and local election officials to protect democracy from those who seek to do it harm.

Finally, we would like to thank the election officials around the country for whom we wrote this guide. You are the frontline defenders of democracy. We hope this effort helps make that tremendous responsibility a little easier.

Good luck,
The D3P Team

Authors and Contributors

AUTHORS

Meredith Berger, D3P, Harvard Kennedy School

Charles Chretien, Software Engineer, Jigsaw (Alphabet)

Caitlin Conley, Executive Director, D3P

Jordan D'Amato, D3P, Harvard Kennedy School

Meredith Davis Tavera, D3P, Harvard Kennedy School

Corinna Fehst, D3P, Harvard Kennedy School

Josh Feinblum, Chief Security Officer, DigitalOcean

Kunal Kothari, D3P, Harvard Kennedy School

Alexander Krey, D3P, Harvard Kennedy School

Richard Kuzma, D3P, Harvard Kennedy School

Ryan Macias, Election Assistance Commission

Katherine Mansted, D3P, Harvard Kennedy School

Henry Miller, D3P, Brown University

Jennifer Nam, D3P, Harvard Kennedy School

Zara Perumal, D3P, Massachusetts Institute of Technology

Jonathan Pevarnek, Software Engineer, Jigsaw (Alphabet)

Anu Saha, D3P, Massachusetts Institute of Technology

Mike Specter, D3P, Massachusetts Institute of Technology

Sarah Starr, D3P, Harvard Kennedy School

SENIOR ADVISORY GROUP

Eric Rosenbach, Co-Director, Belfer Center;
Director, Defending Digital Democracy Project

Robby Mook, Co-Director, D3P

Matt Rhoades, Co-Director, D3P

Heather Adkins, Dir. of Information Security and Privacy, Google

Dmitri Alperovitch, Co-Founder and CTO, CrowdStrike

Siobhan Gorman, Director, Brunswick Group

Yasmin Green, Head of Research & Development, Jigsaw (Alphabet)

Stuart Holliday, CEO, Meridian International Center

Kent Lucken, Managing Director, Citibank

Debora Plunkett, former Director of Information Assurance,
National Security Agency

Colin Reed, Senior Vice President, Definers Public Affairs

Suzanne Spaulding, Senior Advisor for Homeland Security,
Center for Strategic and International Studies

Alex Stamos, Chief Security Officer, Facebook

CONTRIBUTORS

Dmitri Alperovitch, Co-Founder and CTO, CrowdStrike

Arjun Bisen, D3P, Harvard Kennedy School

Drew Bagley, Sr. Privacy Counsel & Director of Global Cyber Policy,
CrowdStrike

Daniel Bartlett, D3P, Harvard Kennedy School

Judd Choate, Colorado Election Director and President, National
Association of State Election Directors

Amy Cohen, Exec. Director, National Association of State Election Directors

Mari Dugas, Project Coordinator, D3P

Alan Farley, Administrator, Rutherford County, Tenn. Election Commission

David Forscey, Policy Analyst, National Governors Association

Robert Giles, Director, New Jersey Division of Elections

Mike Gillen, D3P, Harvard Kennedy School

Chad Hansen, Senior Software Engineer, Jigsaw (Alphabet)

Eben Kaplan, Principal Consultant, CrowdStrike

Matt Masterson, Commissioner, Election Assistance Commission

Sean McCloskey, Election Task Force, Department of Homeland Security

Amber McReynolds, Director of Elections, City and County of Denver, Colo.

Joel Mehler, Senior Consultant, CrowdStrike

Robby Mook, Co-Director, D3P

Rachel Neasham, D3P, LoLa

Daniel Perumal, D3P

Debora Plunkett, former Director of Information Assurance,
National Security Agency

Sean Quirk, D3P, Harvard Kennedy School

Matt Rhoades, Co-Director, D3P

Eric Rosenbach, Co-Director, Belfer Center;
Director, Defending Digital Democracy Project

John Sarapata, Head of Engineering, Jigsaw (Alphabet)

Johanna Shelton, Director, Public Policy, Google LLC

Reed Southard, D3P, Harvard Kennedy School

Suzanne Spaulding, Senior Advisor for Homeland Security,
Center for Strategic and International Studies

Charles Stewart III, Professor, MIT

Michelle K. Tassinari, Director/Legal Counsel, Elections Division, Office
of the Secretary of the Commonwealth of Massachusetts

Frank White, Independent Communications Consultant

BELFER CENTER WEB & DESIGN TEAM

Arielle Dworkin, Digital Communications Manager,
Belfer Center

Andrew Facini, Publications and Design Coordinator,
Belfer Center

Acknowledgments

The D3P team would like to especially thank Heather Adkins of **Google**, Yasmin Green of **Jigsaw**, the **Hewlett Foundation**, the **Democracy Fund**, and the **Belfer Family**; without whom this Playbook would not have been possible. Additionally, we would like to thank the following organizations and offices for sharing their time with us through conversations, simulation participation, or field visits. Your perspectives were critical in shaping our approach to this document.

Department of Homeland Security (DHS)
National Association of State Election Directors (NASED)
National Association of Secretaries of State (NASS)
National Governors Association (NGA)
National Guard Bureau (NGB)

Election Officials from the Following States and Jurisdictions:

Atlantic County, New Jersey
Nevada County, California
Orange County, California
Santa Clara County, California
State of Colorado
Arapahoe County, Colorado
City and County of Denver, Colorado
State of Connecticut
Escambia County, Florida
Cook County, Illinois
State of Louisiana
State of Maryland
Caroline County, Maryland
Commonwealth of Massachusetts
State of Minnesota
State of Nevada
Clark County, Nevada
State of New Jersey
Mercer County, New Jersey
State of North Carolina
State of Ohio
State of Oregon
Multnomah County, Oregon
Commonwealth of Pennsylvania
State of Rhode Island
State of Tennessee
State of Vermont
Commonwealth of Virginia
State of West Virginia
Harrison County, West Virginia
State of Washington
State of Wisconsin

The Playbook Approach

Election officials are democracy's frontline defenders. Our election system faces an array of threats designed to undermine vote integrity and public trust in the election process. It is crucial that everyone involved in the election process—from top-level leaders, like Secretaries of State and Election Administrators, to day-to-day operators, like clerks and election site workers—understand their role in protecting the process and the threats that it faces. To this end, this Playbook has two goals: (1) to make the most likely and most serious cybersecurity and information operation threats understandable to everyone involved in the election process; and (2) to offer state and local election officials basic risk-mitigation strategies to counter these threats.

Our recommendations represent a baseline. It would be impossible for us to cover every vulnerability, as new malicious actors and attack vectors constantly emerge. For this reason, we have focused on the most likely and most serious cybersecurity and information operation risks that elections face. This is not intended to be a comprehensive technical reference for IT professionals, but implementation of some strategies will require their involvement. We also did not address every issue or policy challenge that impedes cybersecurity readiness. Instead, we focused on the vulnerabilities and threats that align to create risk to our election process.

Finally, we understand that election officials already face many challenges in delivering accessible, accurate and secure elections—not least of which are constraints on financial and staffing resources. This Playbook is written with those realities in mind.

We hope this guide will give election officials more confidence in deciding how to approach security strategies and a greater common understanding in working with the technical specialists needed to implement these strategies.

This Playbook consists of three parts:

Background: frames the elections operating environment.

Common Ground: provides 10 best practice principles applicable to every election jurisdiction and a list of research security insights by election system.

Technical Recommendations: offers basic risk-mitigation recommendations specific to five components of the election system: voter registration databases, vote casting, vote tallying, election night reporting, and internal and public communications.

Our appendices offer more specific recommendations on two complex topics: vendor selection and maintenance, and election auditing. Additionally, the D3P Team has put together two additional resources to help navigate the challenges of maintaining and preserving public trust: "The Election Cyber Incident Communications Coordination Guide" and "The Election Cyber Incident Communications Plan Template for State and Local Election Officials."

Introduction

Running elections is complicated. It requires year-round preparation and coordination. Election officials have a lot to manage to ensure that the process remains free, fair, and accessible. Historically, efforts to protect the election system have focused on physical security, but today's digital world requires that we also focus on cybersecurity and information operations to defend against malicious actors of varying motives and means.

Cyber Attack: an attack targeting a network for the purpose of disrupting, disabling, destroying, or maliciously controlling it; or an attempt to destroy the integrity of data or steal controlled information. Common attacks include: spear phishing (to gain unauthorized access to existing accounts), denial of service (DoS), and device takeover.

Information Operations: the dissemination of information, true or false, to manipulate public opinion and/or influence behavior. Digital technologies like social media have made it possible for nation-states to organize information operations at an unprecedented scale. Because the tools needed for information operations are incredibly cheap and widely accessible (all you need is access to the Internet), adversaries use information operations to gain an asymmetric advantage over the U.S. and compete for influence in the world. Common information operation tactics include: spreading fake or misleading information online, leaking stolen information online, and using social media to amplify opposing views and stir political conflict.

Cyber attack and information operations tactics are often used in coordination. For example, a malicious actor might hack an election official's email account, alter emails, and then use those stolen, altered emails to spread misinformation online. Alternatively, social media login credentials might be stolen, and an official account then used to create confusion.

Background

What's at Stake

A core tenet of democracy is that the government reflects the will of the people. Elections are the quintessential expression of this principle and citizens won't trust their government unless they trust the election process and the integrity of its outcome.

Perception is reality. An adversary can manipulate the outcome of an election through actual cyber operations, but they can get the same result (i.e., erode trust in the process) by using information operations to make the public *believe* that the election was manipulated, even if it wasn't in reality.

The U.S. intelligence community reported that cyber and information operations took place in the 2016 presidential election. While it didn't affect the outcome of the election, it did reveal significant vulnerabilities in our elections process. The 2016 case was not the first time malicious actors have meddled with U.S. elections, and it will not be the last. In January 2018, the Director of the Central Intelligence Agency, Mike Pompeo, stated he has "every expectation" Russia will continue meddling in U.S. elections, including the upcoming November 2018 midterm elections. While these foreign operations are traditionally a matter for the intelligence community and federal law enforcement, responsibility to secure elections ultimately falls on local and state officials.

Cybersecurity Threats to Elections

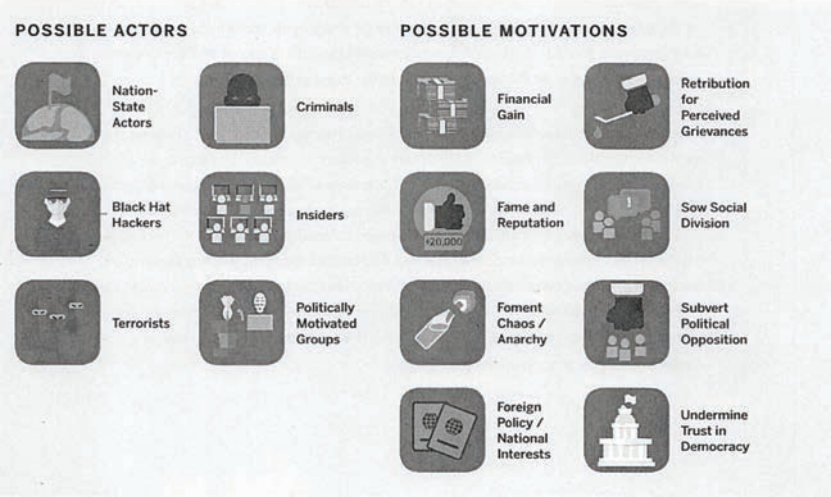
U.S. elections are decentralized. The federal government provides national-level guidance, but state and local governments administer elections. In almost every state, local officials at the county or municipal level have direct responsibility for the conduct of elections in jurisdictions ranging in size from a few dozen to nearly eight million eligible voters.

The distributed and decentralized nature of elections is both good and bad for cybersecurity. Fortunately, decentralization makes it hard, though not impossible, for a single cyber operation to compromise multiple jurisdictions. However, disparities in cybersecurity resources and

experience across jurisdictions creates vulnerabilities. Smaller jurisdictions with fewer resources may be seen as more vulnerable targets by adversaries. Our nationwide security survey of states and territories reinforced this, with the most frequent concern noted by election officials being insufficient resources to secure the process, especially in smaller counties.

The "Who" Behind Cyber Attacks & Information Operations Targeting Elections

A range of adversaries have both the capability and intent to inflict harm on the democratic process using cyber and information operations tools. They can do this from an ocean away or right down the street. The Russian intelligence services partially achieved President Putin's goal of undermining trust in American democracy by using a combination of cyber attacks and information operations to influence narratives of the 2016 presidential election. This partial success, and the U.S. government's failure to respond sufficiently to the Russians, likely means that future elections will face attack from a broader set of actors. Nation-states pose the most well-resourced and persistent threat. Lone "black hat" hackers and cybercriminals, who may be motivated by personal gain, notoriety, or the simple desire to see if they can succeed, are also a salient threat.



See the table on page 10 for an overview of known hostile actors.

KNOWN HOSTILE ACTORS THAT COULD TARGET U.S. ELECTIONS

Russia: The Department of Homeland Security, the U.S. intelligence community, CrowdStrike, and other private sector firms implicated Russian intelligence groups "Fancy Bear" and "Cozy Bear" in the 2016 U.S. presidential campaign hacks. Russian meddlers also probed information systems related to voter registration in 21 states, gaining access to at least two systems. Media sources also reported Russian hackers allegedly penetrated a U.S. election software vendor, hoping to gain information for a subsequent spear-phishing campaign against state and county election officials. In the run-up to (as well as since) the 2016 election, Russian-affiliated groups have conducted information operations using social media sites, exploiting existing fissures in American society. Similar coordinated efforts combining cyber attacks and information operations attempted to influence the 2014 Ukrainian and 2017 French elections.

China: In the 2008 and 2012 U.S. presidential elections, Chinese hackers are believed to have penetrated Democratic and Republican presidential campaigns. These breaches appear to have been focused on intelligence gathering as there is no evidence hackers released stolen materials, or attempted to interfere with state election systems.

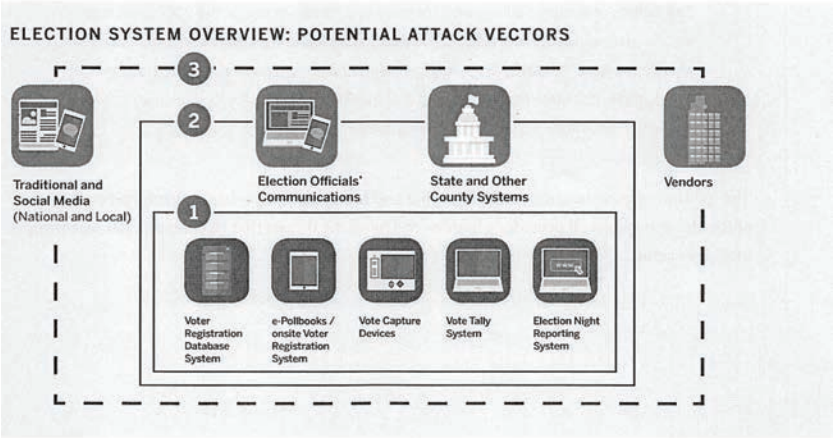
Iran: In 2016, the U.S. Justice Department identified Iran as the culprit in a 2013 cyber attack against a small piece of U.S. physical infrastructure, as well as a series of denial of service attacks on major U.S. financial institutions. Iran demonstrated strong cyber operational capabilities during its penetration of U.S. Navy unclassified networks in 2013. If geopolitical tensions with Iran rise, Iran's cyberspace capabilities could pose a future threat to U.S. elections.

North Korea: While there is no evidence to date of North Korean election-related hacking, the regime has targeted other industries. North Korean hackers infamously retaliated against Sony Pictures Entertainment for producing the film "The Interview" by stealing and releasing company emails and wiping out large parts of Sony's information systems. The U.S. government has attributed the "WannaCry" campaign, which damaged computers across the world, including the U.K. National Health Service, to North Korea. Additionally, government-linked hackers have conducted a series of cyber attacks on financial institutions, central banks, and the global SWIFT financial transaction system, with the aim of raising money for the regime. Heightening tensions between North Korea and the U.S. could provide North Korea with incentive to undermine American democracy, and prompt future attacks.

The "How" Behind Cyber Attacks and Information Operations Targeting Elections

From a cyber perspective, every part of the election process that involves some type of electronic device or software is vulnerable to exploitation or disruption. When discussing election cybersecurity, the focus is often on voting machines. However, voting machines are only one part of a complex, interconnected system. Securing elections requires securing the entire process, because any element of the system could be the weak point that a malicious actor exploits.

We have broken the election system and its components into three levels of operation relating to cybersecurity risk. Officials in all jurisdictions, regardless of size, must secure the process at each level. The first level ❶ includes the core systems that make elections run: voter registration databases (VRDBs), electronic poll books, vote capture devices, vote tally systems, and election night reporting (ENR) systems. The second level ❷ includes two intermediary government functions that connect to multiple election system components: other state and county-level systems, and election officials' internal communication channels. The third level ❸ involves external functions that touch the entirety of the elections process: vendors, and traditional and social media at the local and national level.



Computers and software are present in every component of the election process, which means so are vulnerabilities. Depending on a malicious actor's motives, they could look to actually undermine the integrity of the vote, diminish public confidence in the process, or both. The potential attack vectors into an election system are both technical and human. They include those who develop and maintain the system, as well as the system itself. Ultimately, most cybersecurity breaches result from malicious actors exploiting human behavior, not technical shortcomings. This is true across all sectors and industries, and election systems will likely be no exception. Vendors of election systems or election software are also easy, valuable targets for malicious actors.

THE EXTENT OF VENDOR INVOLVEMENT IN ELECTIONS

Vendors play a critical role in supporting elections at both the state and local levels: from the computers used to access information, the servers that house information, the management of the databases that contain the information, the machines used to cast and tally votes, the websites and software used to display information and results, to the software that creates ballot designs or helps transfer information across systems. Some vendors are involved on such a broad scale that they can become a single point of failure at a national or state level. For example, over 60 percent of American voters cast ballots on systems owned and operated by a single vendor. In the 2012 presidential election, this vendor produced over 100 million ballots in more than 4,500 election jurisdictions and 40 states. The same single point of failure can exist at the state level. For example, one state contracted with a single vendor to do all of its state maintenance and ballot definition files for the 2018 elections.

The following figure describes common cyber and information operations that target each level of the election system. It provides a basic overview of the threats that election officials face from malicious actors.

Cyber and Information Operations

Some of the most common means and methods behind cyber and information operations used by malicious actors to target elections.

CYBER OPERATIONS

Social engineering is a category of attack in which malicious actors manipulate their target into performing a given action or divulging certain information (often a login or password).

Spear-phishing is a social engineering attack in which malicious actors send an email attachment or link that is designed to infect a device or obtain sensitive information. Malicious actors often review a target's social media accounts and work environment to tailor an email to appear enticing and convincing.

Hacking refers to attacks that exploit or manipulate a target system in order to disrupt or gain unauthorized access.

SQL injection is a way for attackers to read and/or alter the contents of a user's database by manipulating forms that are publicly available or exposed. Properly validating any incoming information from users can help prevent this method of attack.

Port scans are similar to checking whether doors are locked and walking through those that are open. Attackers often use it to profile potential targets and conduct surveillance on the systems they are running. A skilled attacker can use this method to gain access to unprotected servers or networks.

Man in the middle (MITM) attacks occur when attackers insert themselves between two or more parties and gain access to any information in transit between those parties.

Distributed Denial of service (DDoS) attacks seek to prevent legitimate users from accessing information (e.g., databases, websites) or services by disrupting access. Attackers disrupt service by using multiple computers and Internet connections to flood a target with excessive traffic, causing the service to crash.

Insider threat is a category of attack in which a current or former employee or authorized individual with access to a network, system, or data deliberately uses their access for malicious purposes.

INFORMATION OPERATIONS

Information Operations (IO) include propaganda, disinformation, and other tools used to manipulate public perception. Digital technologies have enabled adversaries to conduct IO at an unprecedented scale and to an unprecedented effect. In the context of elections, adversaries might use IO to undermine trust in an election result, exacerbate political divisions, or sow confusion and dissent.

Leaking stolen information: Attackers penetrate networks to obtain and leak sensitive information. Leaking information about budgets, election system vulnerabilities, or sensitive processes can reduce public trust.

Spreading false or misleading information: Attackers may hijack official accounts, or use social media or paid ads to distribute false information (e.g., polling times/places, election results), discredit a candidate, election officials, or voting system integrity.

Amplifying divisive content: Malicious actors often use existing social or political tensions to stoke divisions, distract, and disrupt a target to divert their resources.

Interrupting service to public-facing online resources: Attackers may use this tactic to accomplish a broader strategic objective. A DoS attack can serve to undermine trust in electoral systems or government services.

Common Ground

10 Best Practices that Apply to all Election Jurisdictions

Despite variations in election systems across states and localities, our 10 best practices can make any jurisdiction more secure. The list below provides overarching, high-level concepts. In the Technical Recommendations section, we operationalize these best practices into risk-mitigating recommendations addressing five components of the election system: voter registration databases, vote casting, vote tallying systems, election night reporting, and internal and public communications.

1. **Create a proactive security culture.** Risk mitigation starts with strong leaders who encourage staff to take all aspects of election security seriously. Most technical compromises start with human error—a strong security culture can help prevent that. A strong security culture also makes a big difference as to whether a malicious actor: (1) chooses to target an organization, (2) is able to successfully do so, or (3) is able to create public perception that the organization has been compromised. Any state could experience a cybersecurity threat to their elections process—it is the job of leaders to make sure they are prepared.

   Lead by example. Senior leadership, especially Secretaries of State, Election Administrators, and other heads of municipal jurisdictions, need to set an example for the rest of the organization. Issue guidance about the necessity of applying cybersecurity standards (such as those recommended in this Playbook), stressing the importance of cybersecurity for staff by personally introducing orientations and trainings, and following up with operations personnel on a regular basis about the implementation of improved cybersecurity protections. Leaders also need to ensure that those charged with implementing a cybersecurity program have the authority to enforce policies and procedures. Without enforcement, these are only words on paper.

   Develop a detailed cyber incident response plan. As with contingency plans for physical threats, teams should understand critical election system vulnerability points and create a detailed response plan (both internal processes and communications) for any system compromise. Leadership should also mandate frequent testing of critical systems to ensure both their resilience and officials' comfort with crisis management. Officials should extensively document any real or simulated incidents and review these periodically for training purposes.

   Use external resources to assist in improving cyber defense capabilities and building expertise. Department of Homeland Security and private sector technology companies are

available to provide support for prevention and detection. Recognizing Constitutional and other legal restraints, National Guard cyber units, operating under state authorities, can also be a resource to help identify network vulnerabilities. These units are often made up of highly trained professionals involved in private sector cybersecurity.

Be diligent in selecting who is involved in election administration. Election systems qualify as national critical infrastructure, which raises the security expectations for those involved. Conduct background checks on all personnel involved in accessing sensitive information and privileged systems. Require vendors to do the same.

2. **Treat elections as an interconnected system.** Adversaries can target not only individual parts of the elections process but also the connections between them. Attackers look for seams: they seek the weakest point and move from there to their intended target. External systems (e.g., Department of Motor Vehicles databases and vendors) with election system access must be included in the system landscape because they can be penetrated to gain access. The compromise of one part of the election system or an external source can potentially corrupt seemingly unrelated parts of the system. This is true even if the system is not technically connected to the Internet—hacks can be executed using thumb drives and other external storage devices.

   Safeguard computers and digital devices that touch the process, regardless of whether they are owned by a vendor, the state or local government, or are the personal device of an official or volunteer.

   Centralize and streamline device security management by incorporating election offices into existing technology security plans.

3. **Have a paper vote record.** To protect against cyber attacks or technology failures jeopardizing an election, it is essential to have a voter-verified auditable paper record to allow votes to be cross-checked against electronic results. Without a paper vote record, accuracy and integrity of the recorded vote tally depends completely on the correctness and security of the machine's hardware, software, and data; every aspect from the ballot displayed to the voter to the recording and reporting of votes, is under control of hardware and software. Any security vulnerability in this hardware or software, or any ability for an attacker to alter (or reload new and maliciously behaving) software running on a machine that does not produce a paper record, not only has the potential to alter the vote tally but can also make it impossible to conduct a meaningful audit or recount (or even to detect that an attack has occurred) after the fact.

   Create an auditable paper record for every vote cast that is verified by the voter to ensure if the electronic vote count is maliciously altered, a true record still exists on paper. Make sure that this verifiable paper record has a rigorous chain of custody associated with it.

4. **Use audits to show transparency and maintain trust in the elections process.** Audits are a mechanism to detect intrusions or manipulations on electronic systems that may go unnoticed and reassure the public that the elections process works. This is an important part of the public engagement strategy that builds confidence and demonstrates transparency. *When combined with #3, having an auditable paper vote record, this substantially reduces the risk of a malicious actor delegitimizing an election.*

   Embed auditing at points in the process where data integrity and accuracy are critical; for example, with voter registration records.

   Make post-election audits standard practice, using paper records to confirm electronic results.

5. **Implement strong passwords and two-factor authentication.** Malicious actors frequently use stolen user credentials (e.g., username and password) to infiltrate networks. Although strong passwords are important, *two-factor authentication is one of the best defenses* against account compromise. Two-factor authentication typically requires a user to present something they *know* (a username/password) and something they *have* (such as another associated device or token) in order to access a digital account. Only by having *both of* these things will the user confirm their identity and be able to gain access to the system.

   Require strong passwords not only for official accounts but also for key officials' private email and social media accounts. For your passwords, create `SomethingReallyLongLikeThisString`, not something really short like `Th1$`. Contrary to popular belief, a long string of random words without symbols is more difficult to break than something short, with lots of `$ymB01$`.

6. **Control and actively manage access.** Everyone with access to the computer network can become a target and often only one target needs to be compromised for an attack to succeed. The more people who can use a system, and the broader their access rights, the greater the opportunities for malicious actors to steal credentials and exploit them.

   Limit the number of people with access to the system to those who need it to complete their jobs (the "who").

   Restrict what each user is authorized to do using the principle of "least privilege," meaning give users the minimum level of access that they require to perform their jobs (the "what"). For example, not every official from County A needs the ability to view or modify voter registration records in County B.

   Quickly remove those who no longer need access, regardless of their privilege level. Make this a part of standard offboarding procedures for staff.

7. **Prioritize and isolate sensitive data and systems.** Risk is where threats and vulnerabilities meet. To reduce risk, officials need to think about what vulnerabilities will cause the most damage, given the threat environment. Officials consider two things when making a risk assessment: (1) what data is most sensitive and (2) what disruption could be most damaging to voters' trust in the election. They should then prioritize mitigating the vulnerabilities that could lead to this damage by isolating and protecting these systems the most. Every part of the system is important, but a good security strategy will determine which systems are most sensitive and prioritize efforts there, since these extra protections create operational hurdles and increase costs.

   - **Configure devices with sensitive data** to only be used for their specific purpose in the elections process (e.g., the software on a vote tallying computer is only what is necessary to run the election management system; or it operates on an isolated network so all wifi/bluetooth is disabled).

   - **Restrict the use of removable media devices** (e.g., USB/thumb drives, compact discs) with these systems. A "one way, one use" policy is best.

8. **Monitor, log, and back up data.** Monitoring, logging, and backing up data enables attack detection and system or data recovery after an incident. When it comes to monitoring, a combination of human and technical means is best. Local officials highly knowledgeable about their jurisdictions can identify many irregularities. However, this alone may leave gaps in detecting attacks. Automated forms of data monitoring, especially at the state level to detect cross-county patterns, are critical for detecting anomalies and highlighting when manipulation or intrusion occurs.

   - **Log any changes to the voter registration database**, and monitor the database with both a human check and anomaly detection software.

   - **The adage is that "your data is only as good as your last backup."** This means that (1) backups should be regularly performed, either through automation or as part of a scheduled manual process, (2) backups should be read-only once created to prevent data corruption, and (3) backups should be regularly tested by performing a complete restore from backed-up data. Database technology vendors provide guidance and best practices specific to their technology and database architecture for validating and testing restoration of backups; consult these recommendations when developing your plan. In addition to those recommendations, ensure backups are stored in a different physical location than the master database and are physically secured.

9. **Require vendors to make security a priority.** 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 elections. Conversely, smaller vendors may not dedicate the necessary resources to cybersecurity, making them unable to defend against sophisticated attacks. (*For more details, see* **Appendix 1: Vendor Management**)

Include explicit security stipulations in requests for proposals, acquisition, and maintenance contracts to ensure that vendors follow appropriate security standards, and guarantee state and local governments' ability to test systems and software.

Remember that skepticism is healthy. Verify security claims of vendors with independent analysis or reports from trained professionals.

Require vendors to provide notification of any system breach immediately after they become aware of it.

10. Build public trust and prepare for information operations.

Communication is the cornerstone of public trust. Transparency and open communication will counter information operations that seek to cast doubt over the integrity of the election system. For additional information on communication strategies and planning see the D3P "Election Cyber Incident Communications Coordination Guide" and "Election Incident Communications Plan Template".

Communicate repeatedly with the public to reinforce the message that integrity is a top priority.

Before elections are held, start informing the public about cybersecurity threats, the steps taken to counter them (withhold specific details that could aid an attacker), and your readiness to respond in the event of an attack.

Establish processes and communications materials to respond confidently and competently in the event of an attack.

Build relationships with reporters, influencers, and key stakeholders to establish trust and have good communications channels before an incident occurs. It is especially important to do this with candidates and party officials.

Routinely monitor social media, email accounts, and official websites, and establish points of contact with social media firms (e.g., Facebook, Twitter) to enable quick recovery of hacked accounts.

Security Insights by Election System

During our field research we learned a lot of great insights from election officials who are making cybersecurity a reality. This list reflects many of those ground-level insights, classified by the key components of the election system. For detailed technical specifications, refer to the Technical Recommendations section.

VRDB

- Patch and update all computers and servers that connect to the database.
- Ensure the database server is not accessible over the public Internet. Restrict which external systems can write directly to the database.
- Establish a baseline for normal data activity (new entries and edits to existing entries). Monitor activity against this baseline and investigate anomalies. Add human review for data changes—at a minimum, review weekly change summaries; ideally have an official review automated updates.
- Limit access to only those who need it. For those with access, restrict access to only their area of responsibility (e.g., a county official can only edit files for his/her county but may have read access to others). Regularly adjust access and permissions as personnel change.
- Require two-factor authentication for anyone to log into the database—no exceptions.
- Make frequent backups of the VRDB. Conduct routine recovery drills to ensure they work.

For Online Voter Registration

- Do NOT allow web servers to connect directly to the VRDB.
- Have mechanisms in place to mitigate DDoS attacks on the voter registration website.

For e-Pollbooks

- Restrict device functionality to only what is required and confirm, through pen-testing, that all unnecessary features are disabled (e.g., wifi, bluetooth). Disable functionality in hardware when possible.
- Make them single-purpose devices; software on them should only be what is necessary.
- Understand how voter information is loaded onto the e-Pollbooks; cryptographically confirm the e-Pollbook file on the device matches the original file.
- Physically disable or otherwise seal exposed ports if possible.

Vote Casting Devices

- Every machine should have an individual voter-verified paper trail.
- Do election audits. Make them a regular part of the elections process.
- Restrict device functionality to only what is required and confirm, through pen-testing, that all unnecessary features are disabled (e.g., wifi, bluetooth). Disable functionality in hardware when possible.
- Do not connect machines to any network for longer than necessary (i.e., if wifi is used to update, ensure it is enabled only for the required time window).

- If vote tallies are transmitted directly from the machine, ensure the data transmission is encrypted.
- Treat all removable media as a potential delivery mechanism for malware. Institute a "one-way, one-use policy:" only use physical media once, from one system to a second system, then securely dispose of it.
- Ballot definition files could be corrupted—secure the creation, transfer, and upload process.

Vote Tallying Systems

- Vote tallying systems should be single-purpose systems, with only software installed required for running the vote tallying system—nothing else, and isolated with no network or Internet connectivity.
- Electronic vote tabulation data should be encrypted when transmitted between sites.
- Address security vulnerabilities by patching and updating vote tallying system devices.
- Use two different forms of communication to report and confirm vote tally reports (e.g., electronic file submission, then phone call).
- Treat all removable media as a potential delivery mechanism for malware. Institute a "one-way, one-use policy." Only use physical media once, from one system to a second system, then securely dispose of it.

Election Night Reporting

- Ensure websites are up to date and create a plan for DDoS mitigation.
- Limit access/edit privileges for users, similar to VRDB access.
- Prepare a contingency communications plan for disseminating results.
- Verify that results shown to the public on the official ENR website match reported results.
- Monitor the ENR system for anomalies in traffic or access during election night.
- Conduct searches/media reviews during election night to check for false sites and social media accounts.

Internal and public-facing communications

- *Email:* Use two-factor authentication for email accounts.
- *Public-facing websites beyond ENR (e.g., to communicate election day logistics):* Keep sites up to date to decrease potential for manipulation; have an action plan for potential DoS; know how to recover hijacked accounts.
- *Official social media accounts:* Use two-factor authentication. Limit access. Understand third-party apps can be a vulnerability if they are compromised. Identify points of contact and establish relationships with key social media firms for responding to issues when they arise. Know how to recover hijacked accounts.
- *Private social media accounts*: Private accounts of key officials need to be secured as they are also likely targets.

Vendors

- Require vendor security measures. Vendors can connect to every part of this system. Their internal security matters—vendor access points could be the weak link that gets exploited and corrupts other parts of the process.
- Ensure security requirements and considerations are included in vendor contracting and enforced.

Technical Recommendations

Securing State Election Systems

There is no such thing as perfect security; however, there are preventative measures that make the process much more secure. In the Common Ground section, we provided best practices that apply across all election jurisdictions and some system-specific insights. In this section, we elaborate on these concepts with specific technical recommendations as they relate to five components of the election system: voter registration databases, vote casting, vote tallying systems, election night reporting, and internal and public communications. As we highlighted in Common Ground, system defense is a critical first step in securing the elections process. For this reason, the majority of our recommendations fall into the category of "Protect." Because election systems are decentralized and varied in nature, not all recommendations apply to every state or locality.

As we said in the introduction, our recommendations represent a baseline. It would be impossible for us to cover every vulnerability, as new malicious actors and attack vectors constantly emerge. For this reason, we have focused on the most likely and most serious cybersecurity and information operation risks that elections face. This is not intended to be a comprehensive technical reference for IT professionals. But we do want to emphasize IT professionals are critical to establishing and maintaining a secure election system and their expertise will be needed for many of our recommendations. Threats are constantly evolving and IT professionals will help you get beyond what this Playbook provides and keep you abreast of the latest threats and defenses.

Voter Registration Databases and e-Pollbooks

Voter registration databases (VRDBs) store information on registered voters in a given state. The Help America Vote Act requires that all states implement a "single, uniform, official, centralized, interactive, computerized voter registration list," unless the state has no voter registration requirement. Throughout this document, we refer to this centralized, computerized list as the VRDB.

Different states follow different processes for managing and updating their VRDB—in some states, all new entries, deletions, and edits are implemented as processes at the state level, whereas in other states this happens at the county level (with changes pushed up to the state-held "master"). In many states, ***third-party systems***, such as Health and Human Services and the Department of Motor Vehicles, provide data to the VRDB in an effort to keep voter records up to date. Some states offer ***online registration***, allowing voters to register and edit their record via a public-facing online portal connected to the VRDB. Some states offer ***same-day registration***, while others require voters to register before election day.

Closely linked to VRDBs are the pollbooks used on election day. States may choose to only use paper pollbooks, or may use ***electronic pollbooks (e-Pollbooks)*** to process voters on election day. e-Pollbooks are electronic versions of voter rolls used by polling site officials to verify legal voter registration and related details on election day. These are usually tablets or laptops and can be networked into a central voter registration system (allowing them to check and update voter records in real time, for example to allow for same-day voter registration), or they can be standalone at the precinct (containing a separate, offline copy of the electors list). Regardless of whether a state/county uses paper or e-Pollbooks, their creation requires an export of files from the VRDB for either printing or translation into an e-Pollbook compatible file.

Across both VRDBs and e-Pollbooks, states may choose to develop and maintain the software in-house, or may outsource this work to an external ***vendor***.

Core VRDB issues

KEY THREATS:

Unauthorized access to the VRDB from Internet exposure: Leaving the VRDB exposed to the Internet makes it vulnerable to attacks. Once it is connected to the database, an attacker can add, edit, or delete voters, allowing for false votes to be cast on election day or forcing voters to cast provisional ballots. Even if this does not affect actual vote outcomes, the perception of vote manipulation or voter suppression can significantly undermine the credibility of an election.

Maintenance: An insufficient or poorly timed maintenance and patching regime leaves security vulnerabilities open and can expose the VRDB to attacks.

Account compromise: Attackers might compromise the accounts of election officials with access to the VRDB; without proper controls in place this could allow the attacker to add, edit, or delete voter entries. In the absence of proper logging and monitoring, these changes may go unnoticed until election day and affect the ability of voters to cast ballots.

Third-party system compromise: Third-party systems (e.g., DMV, HHS) linking into the VRDB can be compromised, or the transmission of these entries to the database could be compromised along the way. If these systems are allowed to feed directly into the VRDB, or if the review and approval process at the state and county level is insufficient, there is a risk that the compromise could allow malicious actors to manipulate voter status.

Recommended actions:

Identify

Map how other systems connect to the VRDB. They will commonly be connected to sync or add voter information (e.g., from DMV records).

Know where the VRDB is hosted and what defenses exist on the servers and the underlying network infrastructure.

Know what accounts have access and what level of access each account has (e.g., can a county official change records from other counties?). Use a test account to verify that restrictions are operating as intended.

Determine which of the servers can be accessed over the Internet. Close connections to any that do not require access.

Protect

Require strong passwords and implement two-factor authentication. This should apply to everyone who can edit the VRDB. Account security is crucial for all VRDB users and especially those with elevated or administrative privileges.

Conduct penetration tests, source code audits, and encourage vulnerability discovery efforts. Regardless of whether your VRDB software is built in-house or by vendors, third-party auditing and penetration testing should be performed to provide awareness of security vulnerabilities. Develop and maintain a continuous program that tests your organization's susceptibility to spear phishing and other social engineering attempts. It is important to do this regularly, both to spot new vulnerabilities that might arise, and to prevent staff from becoming complacent.

Apply software updates and patches. Applying software updates and patches on all devices connecting to the VRDB is essential to preventing malicious actors from gaining access. Check for patch signatures to ensure they are authentic. Using endpoint management software and vulnerability software on official computers can help automate the patching process to ensure systems stay up to date.

To prevent interference with election day operations, **establish cut-off days for applying and testing patches** to ensure optimal functionality during election periods. Only critical updates should be done after the cut-off window and all patches should be tested for functionality as well as security.

Create automated scans to look for vulnerabilities on the VRDB portal.

Ensure that your underlying database server is not accessible over the Internet.

Restrict external systems' access to the VRDB. Data from other systems (e.g., the DMV) should go through validation (either manual or automated) rather than allowing those systems to directly write to the database. This prevents the database from being directly edited if an external system is compromised.

Log changes. As a rule, changes to the VRDB should be recorded securely and be reviewed, preferably both by a human and an automated system. Establish a baseline for normal data activity (e.g., new entries, edits to existing entries, change in voter status) so that atypical behavior can trigger an alert.

Limit account access to the VRDB. Restrict access to the database to those who need it and diligently maintain and review this access list. For example, state or local offices responsible for updating voter registration information require access. However, the software developers who designed the system do not. Account management includes revoking the access of old employee accounts immediately after they depart or change roles. Vendors responsible for the software will need access, but should not retain that access any longer than necessary.

Implementing these limitations requires an individual to be responsible for constantly managing accounts, ensuring existing accounts belong only to those who need them, and that system permission changes were approved.

Permissions Management for VRDB accounts. Everyone who has an account should be given specific permissions that dictate what they can and cannot do. More people with more access means an increase in potential avenues of attack on the VRDB, so limit the degree of access for each account to only what is necessary for that employee to do their job.

> The most common levels of permission variation are "read," "write," and "admin" access. Someone with "read" access can only read the data, but not alter it; someone with "write" access can change data; and someone with "admin" access can alter permissions for other users.
>
> Even within those levels of permissions the scope of access should be tailored. For example, a county administrator may need access to their own county's information, but should not be able to access information from another county.
>
> **Consider implementing permission restrictions** that limit the number of changes one user can make during a certain time window to stay in line with normal activity patterns—this helps guard against both insider threats and account compromise.

Require users to access the VRDB portal using a VPN. This ensures that even if an account is compromised, the attacker is unable to use it without VPN credentials.

> **Whitelisting** can also be used to limit either what devices a user can connect from or which locations. Paired with a device inventory database, requiring device certificates will allow you to restrict access to managed devices that are verified as secure. Another option is IP whitelisting, which can restrict access to users at specific location. This would require coordination with remote offices' IT departments to identify what addresses should be whitelisted. Using IP whitelists would force an attacker to compromise a machine at one of the locations before they were able to begin an attack against the VRDB.
>
> Establish policy that does not allow connections to the VRDB from public, unauthorized, or unknown devices.

Detect

Monitor activity against a baseline and investigate anomalies. This allows you to notice unusual trends that deviate from the norm. At a minimum, this should be a technical (automated) check which occurs at both the state and county level. Automated monitoring of anomalies at the state level is critical to detect broad changes across the state that may not be noticeable when monitoring only at the individual county level.

Incorporate a human review into data change monitoring to augment technical monitoring. Experienced election officials providing human monitoring at the local level may reveal subtle manipulations. Election officials should trust their instincts—they are more

familiar with this data than anyone else. Empower these officials to flag suspicious behavior or anomalies and investigate them. While human review of every record change is not realistic for all localities, weekly change summaries should be required at a minimum.

Monitor permission changes: Make sure that when changes are made, they are reviewable by those with similar access levels. Create the framework for conducting regular reviews of those changes. This process will allow unusual activity to be detected sooner.

Mail confirmation of changes in registration to voters (ideally both to their old and new address).

Respond

If the incident involved an attacker gaining access to VRDB, perform a thorough review of the system's accounts and access controls to ensure that any backdoor the attacker might have left open is purged.

If a physical machine was compromised, disconnect the machine from the network and seek professional forensic assistance. Discard the machine afterwards: reformatting the machine is not always sufficient to remove exploits. If the machine was connected to any other machines, systems, or components, review those as well.

Recover

Execute the recovery plan during an incident or after one occurs. Include the following categories in your plan: Recovery planning, improvements, and communications.

Public communications around a voter registration-related incident is a CRITICALLY IMPORTANT issue when it comes to public trust and elections transparency. It must be deliberately executed with tremendous care. See D3P's *Elections Cyber Incident Communications Plan Template*.

Practice restoring from VRDB backups. If there is a second live VRDB system, be sure to practice using the secondary system.

Lessons learned should be shared and incorporated into the existing recovery plan. Where possible, update your system to prevent a similar failure or exploit from occuring again in the future.

Vendor Considerations

The most common forms of vendor support for voter registration databases are:

- Vendors building and maintaining the VRDB
- Vendor building and state or county maintaining of the VRDB (to include modifications to initial vendor build)
- Vendor and state jointly building and maintaining
- Third party vendor used to assist with maintenance

The General Vendor Recommendations 1-8 at the bottom of the Technical Recommendations section provide best practices for working with vendors and mitigating potential cyber vulnerabilities. The type of vendor involvement and timeframe (set time period involvement versus continuous) will impact how they apply for each state/county. Additional contract specific recommendations are also provided in **Appendix 1: Vendor Selection and Maintenance.**

Online Voter Registration

States that offer online registration are exposed to the following additional threats:

KEY THREATS:

Website spoofing: Attackers could pose as the official website to either give voters the illusion that their information is updated or in an attempt to capture that information.

Distributed Denial of Service: Attackers can conduct DDoS attacks on the public-facing voter registration website, preventing voters from registering and potentially discouraging them from participation.

External connectivity: An unsecured website presents another vector for a malicious actor to penetrate the VRDB. If it is not properly secured, an attacker may be able to use it to change any vote record.

Large-scale data alteration: An attacker could use information leaked on the Internet to impersonate many different voters and attempt to update their registration details.

Recommended actions:

Identify

Know who the domain name registrar and web hosting provider are and how to contact them.

Determine who is responsible for keeping the website software up-to-date.

Know who has the ability to edit the website.

Protect

Do NOT allow web servers to connect directly to the VRDB. This restriction significantly reduces the possibility of a website vulnerability leading to a compromise of voter records.

Require a CAPTCHA to change a voter's registration. This is a short task, ranging from clicking a checkbox to typing the characters shown in an image, which verifies that an online form is being submitted by a human and not a machine. It increases the difficulty of a computer program changing hundreds or thousands of voter registrations at once.

Protect the online voter registration website against DDoS attacks.

See the **Website** section for additional details on securing the public-facing component.

e-Pollbooks

KEY THREATS:

e-Pollbook Data Manipulation: A malicious actor is able to gain access to the device either using a wireless connection or because the physical device was not properly secured. Once on the device they are able to manipulate the voting roll—either deleting or altering existing voter registration data.

Altering of State Voter Roll via e-Pollbook: If an e-Pollbook has a live connection to the state election day voter roll, compromising one device could be used to change statewide records.

Maintenance/patching of e-Pollbooks: The difficulty in which an e-Pollbook device is compromised depends heavily on whether it is updated and patched. Failure to do so will provide malicious actors an opening into the device.

Recommended actions:

Identify

Examine all the possible functionalities of the device and identify the components you intend to use. Specifically pay attention to the wireless and networking functionality.

Know what kind of network connections your e-Pollbooks need.

Understand how voter information is loaded onto the e-Pollbooks.

Protect

E-Pollbooks should be single-purpose devices. Software on the device should be limited to what is necessary for their use.

Verify the integrity of the e-Pollbook file.

Cross-check the data on the pollbook with what is in the VRDB.

Use digital signatures and hashes to verify the integrity of data contained in voter roll files that are transferred between systems and to ensure data has not been maliciously altered or compromised. If using a method that requires data transmission over a cellular network or the public Internet, use a virtual private network (VPN) to secure those transmissions.

VERIFYING FILE INTEGRITY USING HASHES AND DIGITAL SIGNATURES

A hash is like a fingerprint for digital files—the *hash* of a file will not change unless the actual file changes. Using a hash while transferring files will allow you to confirm that the file has not been altered in transit if the hashes computed by each party are the same. If you decide to use a hash, transfer it through a different channel than you used to obtain the files and compare it to the hash you compute. By sending them separately, such as downloading the file from a website and reading out the hash over the phone, you prevent the attacker from changing the hash at the same time as the file.

A more secure option is to use a digital signature. It is a form of encryption which is equivalent to a seal on a physical document; it guarantees that the file came from a specific trusted source and that its contents have not been modified in transit.

Ensure all devices are updated and patched. Test the e-Pollbook to ensure that it is fully functional after patches have been applied.

If you do not need the e-Pollbook to be connected to a vendor, VRDB, or the Internet while voting is taking place: **turn off bluetooth and wireless capabilities on the devices.** It is better to disable these functions at the hardware level (e.g., removing the wireless card) than to change a setting whenever possible.

If you need to connect to external systems:

> **Connect over a VPN** or other encrypted channel.
>
> **Ensure that the entire setup is preconfigured** and that turning on devices is the only action required by election site workers (they should not need to change any settings on the devices).
>
> **Do not connect e-Pollbooks directly to the VRDB.** Set up a separate system (essentially a copy of the VRDB) to handle changes to voter information, which prevents the VRDB from being impacted if an e-Pollbook is compromised.
>
> **Restrict edit access only to juridictions that need it.** If state law requires you to vote in precinct and there is not same-day registration, an e-Pollbook in one precinct should not be able to modify the voter's record from another precinct.

Have a paper backup of the e-Pollbook.

Ensure physical security. Cover exposed ports (e.g., USB) to prevent them from being accessed by anyone intending to inject malware via a USB or other portable device. Do not use anything other than the charging cords provided with the e-Pollbook on receipt (e.g., do not use an iPhone charger or other similar charger that is not actually part of the e-Pollbook election day pack).

Detect

Monitor data changes. Counties or vendors, as applicable, should monitor voter roll files for anomalies in changes or access. Implement data controls around normal data activity that prevent large-scale changes.

Perform vulnerability scans of e-Pollbook devices to identify ~~those th~~at do not have the latest security updates. Apply patches to minimize vulnerabilities.

Respond

If the incident involved an attacker gaining access to a networked voter roll file shared beyond a single polling site, perform a thorough review of the system's accounts and access controls to ensure that any backdoor the attacker might have left open is purged.

If the e-Pollbook device was compromised, disconnect the machine from the network and seek out professional forensic assistance. Discard the machine afterwards: reformatting the machine is not always sufficient to remove exploits. If the machine was connected to any other machines, systems, or components, review those as well.

Recover

Have a backup paper copy of the pollbook on site and backup devices pre-programmed for deployment to sites, if necessary.

Vendor Considerations

The most common forms of vendor support for e-Pollbooks are:

- Building and/or maintaining of e-Pollbook devices and software.
  - Can overlap with vendor support for VRDBs.
  - Can involve live monitoring of e-Pollbook operations on election day.
- Building electronic voter roll files for e-Pollbooks based on VRDB info where a compromise of the vendor could result in voters being missing, or incorrectly added to, the roll.

See General Vendor Recommendations 1-8 at the bottom of Technical Recommendations section for best practices that apply to working with vendors and mitigating potential vulnerabilities. Additional contract-specific recommendations are also provided in **Appendix 1: Vendor Selection and Maintenance.**

Vote Casting Devices

Overview: Vote casting devices serve as the primary conduit for the actual ballot marking or mark recording process on election day. Most states and counties today use some variation on two types of vote casting devices:

Optical Scanner (OS) or Digital Image Scanner: A machine that scans (and often digitally records an image of) marked paper ballots. Voters cast a ballot via traditional pen and paper, an electronic ballot marking device, or some alternative marking method. The marked paper ballots are then run through these scanning machines which records the appropriately marked vote for each race, and then calculates running vote totals for all ballots scanned on the machine. The machine prints a total result after polls close. The initial paper ballot ensures that a physical record exists for audit or other vote verification purposes.

Direct Recording Electronic (DRE): A DRE system presents a digital ballot image to a voter, collects the voter's selections, and records those choices directly onto electronic media. DREs may be fitted with voter-verified paper audit trail (VVPAT) subsystems to create a paper artifact of the voting transaction.

In recent years, alternate voting methods, particularly vote-by-mail and early voting, are becoming increasingly popular with voters. These jurisdictions often utilize central count facilities where paper ballots are consolidated for tallying. At central count facilities larger variations of the optical scanner/digital image scanner are often used for paper ballot counting.

KEY THREATS:

Device tampering: Voting machines can be compromised via physical tampering (including using removable media) or through external connectivity (e.g., WiFi). This would allow the attacker to change the reported vote information.

Inability to detect tampering: Some DRE machines do not produce a VVPAT (because optical scanner systems scan paper ballots, they do not face this threat). Should a malicious actor compromise such a machine, votes could be lost and results thrown into question.

Recommended actions:

Identify

Examine all the possible functionalities of the device and of any of its subcomponents. Specifically pay attention to the wireless and networking functionality.

Know the certification status of all your equipment. The Election Assistance Commission's (EAC) Voluntary Voting System Guidelines (VVSG) provides federal level certification standards. Many states have their own certification process.

Protect

If you have a DRE machine that does not produce a paper trail, **you should either replace the device or purchase an add-on (VVPAT adapter) that creates a paper trail.**

Physical Security/Access Seals. Use serialized tamper-evident security seals and chain of custody logs to limit physical access to voting machines and track whenever removable media is plugged into the scanners.

Penetration test systems. Conduct, or hire a third-party firm to conduct, a source code audit and penetration test of all vote casting devices.

Restrict device functionality to what is required. Even if you have disabled a feature through a settings page (such as wifi connectivity), those features could still be exploited. You should not trust that toggling a switch in software will actually disable the functionality. If possible, the hardware should be removed.

Isolate the device from external connectivity. Do not connect the device to a network, which includes not using a cellular modem. If network connectivity cannot be avoided, make sure to keep the network connection disabled until you intend to transmit the results.

Create a copy of the results (either a printout or by saving it to removable media) before you connect to the network.

If removable media is used to transfer data (e.g., ballot definition files, vote tallies):

Have a procurement strategy for devices. Purchase physical media devices directly from a trusted vendor and obtain assurance that the suppliers from whom your vendors procure their memory can also be trusted. If you must use devices from an unverified source, obtain them from a location that you would not otherwise use, to make it less likely that a bad actor could plant USB devices that could infect your systems.

Protect device chain of custody. Once devices are procured, ensure that they are stored securely and access is limited to the appropriate audience. When in use, maintain a physical

record of the device—including where the device has been and who has been in contact with it— to limit the opportunity for manipulation.

One-way/one-time use: Only use physical media once, from one system to a second system, then securely dispose of it. A USB device could either (1) transfer data from one air-gapped machine to another or (2) transfer data from an air-gapped machine to an outside one prior to disposal, but not both. When feasible, use write-once memory cards or write-once optical disks instead of USB devices. This ensures one-time use is self-enforced by the technology.

Scan media devices for malware. If you detect abnormalities, don't use the device and contact forensic experts for assistance.

Detect

Perform logic and accuracy testing of the programmed device.

Verify the seals and chain of custody logs via a unique identifier (e.g., seal number).

Respond and Recover

Follow the jurisdiction Incident Response and Recovery Plan for vote casting device compromise.

Vendor Considerations

Vendors are integral to vote casting devices as every device has been physically constructed, programmed, and is often maintained by various vendors. A compromise or oversight at any of these points would allow an attacker to change or erase election results.

See General Vendor Recommendations 1-8 at the bottom of Technical Recommendations section for best practices that apply to working with vendors and mitigating potential vulnerabilities. Additional contract-specific recommendations are also provided in **Appendix 1: Vendor Selection and Maintenance.**

Handling ballot definition files and other software updates

KEY THREATS

Supply chain interdiction: A malicious actor could use vendors as a pathway to plant malware to modify or compromise a ballot definition file before it reaches the hands of election officials.

Manipulation of ballot definition files: If an attacker obtains access to the original ballot definition file, this could leave machines susceptible to destructive attacks and/or could affect tallies.

Recommended actions:

Identify

Determine who is responsible for, and what machines are being used, to create the ballot definition file.

Determine how the ballot definition file is being transmitted to the vote casting device.

Protect

Treat the ballot definition file as critical information. As such, limit its exposure to compromise as much as possible. The system used to develop the file should be isolated from external network connectivity. Place a tamper-evident seal over the media containing the ballot definition file.

Conduct testing (e.g., logic and accuracy, parallel testing) on the systems that the ballot definition files have been loaded onto before deploying them for use.

Review ballot definition file source code to prevent malicious code distribution. When possible, review source code before final distribution of ballot definition files to avoid dissemination of malicious code.

Secure the creation mechanism of the ballot definition file: The ballot files should be generated on a secure single-purpose and air-gapped machine

Secure the transmission of the file:

If possible, use digital signatures on the file. Forcing the voting machines to verify the file signature before loading it will prevent attempts to change the ballot files after it has been created.

If using removable devices to transfer the files, follow all best practices, including one-way and one-time use. The section on vote casting devices above discusses more specific recommendations for removable media.

Detect

Verify the seals over media containing the ballot definition file.

Scan ballot definition files for malware. If you detect abnormalities, don't use the files and contact forensic experts for assistance.

Recover

Follow the jurisdiction Incident Response and Recovery Plan for vote casting device compromise.

Vendor Considerations

Vendors often interact with ballot files by:

Creating the files themselves

Transferring the ballot files to the voting machines

See General Vendor Recommendations 1-8 at the bottom of Technical Recommendations section for best practices that apply to working with vendors and mitigating potential vulnerabilities. Additional contract-specific recommendations are also provided in **Appendix 1: Vendor Selection and Maintenance.**

Vote Tallying System

Vote tallying covers the various devices and networks used to tabulate ballots and aggregate results. Based on differences in setup across states and counties, this process can start at the polling site (for example, precinct count optical scanners that tabulate ballots onsite), or at more centralized counting facilities. In many instances vote tallying is conducted at the county level, where voting sites through a variety of methods (e.g., phone call, email, thumb drive/USB) provide counties with their respective vote tally totals. This section discusses common threats and remedies seen across many system set-ups.

KEY THREATS:

Manipulation of tabulation systems: A compromised tallying machine at a polling site or central counting facility could allow an attacker to directly manipulate tallies before they are transmitted to the county or state.

Data transmission with removable media: USB devices—and other portable physical media—are often used to transmit results from precincts or centralized counting facilities to segmented county/state networks. USB devices can be exposed to malware and compromised at the supplier level or through a previous use in an infected machine. This compromise could result in manipulated data and could also lead the tallying machine itself to become compromised, exposing the system to future exploits.

Networked data transmission: In tallying setups where votes are tabulated at the polling station and transmitted to the county, or are transmitted from the county to the state through a system other than the election night reporting system, configuration errors in the modem, wifi, or cellular network connections used for transmission can leave the process vulnerable to "man-in-the-middle" attacks. These allow adversaries to manipulate results before they are received at the county (or state) level.

Denial of service: Counties or, where relevant, states, receive results from precinct or centralized counting facilities over the network. Servers can be targeted with a DoS attack by an adversary, resulting in delays in vote reporting during election night.

Recommended actions:

Identify

Know the certification status of all your equipment. The EAC's Voluntary Voting System Guidelines (VVSG) provide federal level certification standards. Many states have their own certification process.

Protect

Vote tallying systems should be isolated from any networks or overall Internet connectivity (commonly referred to as "air-gapped"). This includes connecting to voting machine modems. In the case where you cannot achieve total isolation, restrict network access to precincts and counties to prevent outsiders from accessing or slowing down the system. Again, the best practice is to keep these machines totally isolated and to transfer results to them using removable media as they arrive. As for all removable media, practice the "one-way, one-use" rule.

Use a dedicated single-use system for vote tallying. Using a system solely for vote tallying and disabling unnecessary functionality, like network connection, can limit exposure to attackers.

Require strong passwords and implement two-factor authentication to access the vote tally system device. There are two-factor authentication methods that do not require network connectivity, and that can be implemented.

Use a digital signature to verify the source of vote tallies. Requiring each voting machine to digitally sign its report will prevent a malicious actor from introducing fake results into the tally process.

Keep devices up to date and fully patched. Despite the tally system being air-gapped, it is still important to keep the software on them updated. Review available updates, test how they work with your system, and apply them. You should establish a cut-off date prior to the election after which you will not change the software in order to provide enough time to test the system.

System testing. Include the tallying system in your tests of the system. While conducting penetration tests, teams should look for ways they could access these machines despite the air gap (including testing the physical security) and other ways to force errors in the tallying process.

Detect

Report vote tally totals using multiple forms of communication (redundant communication). For example, electronic vote tally submissions should be confirmed with a follow-up call or text.

Recover

If the electronic system is compromised, implement hand-count procedures.

Vendor Considerations

In many cases, the machines used to tally results will have been provided by vendors who will be involved in the maintenance of those machines. A compromise at this level could cause vote totals to be calculated incorrectly, compromising public trust in the election even if the correct totals are eventually reported.

See General Vendor Recommendations 1-8 at the bottom of Technical Recommendations section for best practices that apply to working with vendors and mitigating potential vulnerabilities. Additional contract specific recommendations are also provided in **Appendix 1: Vendor Selection and Maintenance.**

Election Night Reporting (ENR)

Election night reporting (ENR) consists of the systems and processes for aggregating and communicating the unofficial election results to the public and media after polls close, usually via a website. Counties and states may also report election night results via social media—please see the Internal and Public-facing Communications section for best practice in securing social media accounts. ENR setups vary by state across three principal dimensions defined below:

How ENR relates to the vote tallying process. ENR can be closely linked to the vote tallying process (e.g., a state's non-public vote tallying system might automatically submit results to the state's public ENR website), or can be run separately and in addition to the tallying process.

Whether ENR is run by the state, counties, or a combination of both. Most states run ENR centrally, with counties (or in some cases municipalities) submitting results to the state via a centralized ENR system. In some of these cases, the counties run separate, additional ENR systems (e.g., to provide further granularity on results). In a small number of states, ENR is managed at the county (or municipality) level.

Who builds/maintains the ENR system. Regardless of whether ENR is run at the state or county level, ENR systems can be developed and managed in-house (by the state or county), developed by a vendor but managed in-house, or developed and run by a vendor.

KEY THREATS:

Transmission: In a state-run ENR setup, counties submit their vote reports to the centralized system provided by the state. A configuration error could make this transmission vulnerable to "man-in-the-middle" attacks, where adversaries manipulate vote reports before they are received by the state.

Manipulation of ENR systems: Configuration errors can leave ENR systems vulnerable to exploits or unauthorized access, allowing adversaries to manipulate the vote counts after they have been received in the (state or county) ENR system.

Denial of service: In a state-run ENR set-up, a DoS attack on the transmission of ENR results can lead to a lack of results being reported for one or more counties. In addition, attackers can conduct DoS attacks on the public-facing ENR website, making result reporting unavailable to the public/media altogether during election night.

KEY THREATS (CONTINUED)

Website spoofing: Attackers could redirect public inquiries to a spoofed website, which pretends to be the official ENR system but in reality is controlled by a malicious actor. For example, this could be used in disinformation campaigns to depress voter turnout by saying an election has already been called.

Recommended actions:

Our recommendations should be implemented by the county, state, or external vendor, as appropriate.

Identify

Identify which offices need access to the ENR site or other medium through which they report and consolidate results.

Protect

Require strong passwords and implement two-factor authentication. This should apply to everyone who can access the ENR system.

Secure transmission channels. Require users to authenticate themselves when adding result information and restrict the results they are able to change to only what is within their purview. Ensure all network traffic is secure (e.g., enable SSL on a web-based portal).

Limit access through restricting write privileges for users across the state and counties or within the county as applicable. In state-led ENR systems, specifically ensure that each county can only edit its own vote reports (not those of other counties).

Log incoming election results to help trace and correct inaccurate reports.

Prepare a contingency communications plan for disseminating results if the primary medium is unavailable.

Publicly communicate about ENR process to preempt spoofing. Communicate clearly, ahead of any election, how the state or county will report vote results during election night, to preempt false ENR websites from popping up.

Protect ENR websites against DoS attacks. See Website section for additional recommendations.

Report election night results using multiple forms of communication. They should be confirmed over a second channel; for example, a follow-up call, on top of being sent through the primary channel.

Detect

Each county/precinct should verify that results shown to the public on the official ENR website match the results they reported.

Monitor the ENR system for anomalies in traffic or access during election night. Especially monitor any attempts to change the displayed results (e.g., failed login attempts to the portal) or traffic that may be part of a DoS attack.

Respond and Recover

Public communications around election night reporting are critical. Have a backup plan for how to publicize either that your reporting website is showing no results, or incorrect results. Include the specifics in your communications incident response plan.

Vendor Considerations

Vendors are often responsible for building and/or running both the system for updating results and the webpage that displays those results to the public.

- Be sure that you have an internal (state and local level) backup plan for how to publish results if the vendor system is unavailable.

See General Vendor Recommendations 1-8 at the bottom of Technical Recommendations section for best practices that apply to working with vendors and mitigating potential vulnerabilities. Additional contract-specific recommendations are also provided in **Appendix 1: Vendor Selection and Maintenance**.

Internal and Public-facing Communications

Running successful elections requires extensive communication—both within state/county election teams, and with the public. This tends to consist of four key communication channels: internal email communication, official election-related websites, official social media accounts, and the private social media accounts of key officials. All of these communication channels could come under attack by adversaries who abuse them to cause confusion about election logistics before or during election day, and/or to undermine the credibility of the election overall.

INTERNAL COMMUNICATION

Email communication ahead of and during the election is crucial for the election team to coordinate activity internally among states, counties, and precincts/polling stations.

KEY THREATS:

Account compromise: Attackers could compromise key officials' email accounts to send out false information to members of the election team—for example, asking for polling stations to close early or for polling stations to switch to paper pollbooks due to an alleged issue with e-Pollbooks (resulting in delays and lines forming). In addition, compromised accounts could be used to distribute malware across the election team's devices. Clearly, access to the email account of any member of the election team—even at a low level in the organization—exponentially increases the chances of subsequent attacks on the email accounts of more senior members of the election team succeeding.

Recommended action:

Implement two-factor authentication for all official accounts. In most cases, adding a second factor will be enough to prevent an attacker from compromising an account. In addition to this, require strong passwords.

Require all messages to come from official accounts. While officials should take steps to secure their personal accounts as well, all official communication should be done through accounts that have been carefully secured by your IT department.

PUBLIC-FACING COMMUNICATION

Election officials communicate extensively with the public through both ***official election websites*** and ***official social media accounts*** (e.g., Election Board's Twitter account, Secretary of State's official Facebook account). This communication is separate from, and in addition to, election night reporting (which we cover in the section above), and includes, for example, communication to raise awareness of upcoming elections, key deadlines, (e.g., for online registration) and election day logistics (e.g., poll locations, opening hours, ID requirements).

While not officially part of a state's or county's public-facing communication, the ***private social media accounts of key officials*** (e.g., the Secretary of State's private Facebook account) could be used to communicate false election-related information to the public. These should be protected with the same care as the organization's public accounts.

Official Websites

KEY THREATS

Website manipulation (e.g., changing information on polling place location): Malicious actors could look to sow confusion or discourage voters by manipulating the information on official websites. For example, attackers could alter polling site locations and times to make it harder for voters to find their designated vote site

Spoofed websites: To sow distrust in the process, attackers may replicate the official state or county website and post the opposite results than is being reported—for instance the winner of Race A is now the loser.

Distributed denial of service attacks: Similar to voter registration sites, attackers could attempt to shut down official websites on election day to inhibit voters from knowing their designated voting location.

Recommended actions:

Identify

Know who your web hosting provider is and how to contact them.

Determine who is responsible for keeping website software up-to-date.

Know who has the ability to edit your website.

Protect

Have automated procedures to keep software (e.g., Wordpress, Apache) up-to-date. Website software needs to be updated on a regular basis in order to patch vulnerabilities as they are discovered. Have a system for tracking what version of software you are using and what vulnerabilities are discovered and ensure that those vulnerabilities are patched.

Conduct penetration testing and security audits for all resources. Regardless of whether your website was developed by your staff or by vendors, a third-party audit and penetration test can identify vulnerabilities. This should be done anytime a major change is made to website software.

Ensure that developers have been trained on what the common attack vectors are. One good guide for these is the Open Web Application Security Practice (OWASP) Top-10 list.

Ensure sufficient capacity to receive increased site traffic during high-use periods. Provision servers accordingly and conduct load tests ahead of time to be sure that the infrastructure can handle the additional traffic.

Ensure that your website is protected against DDoS attacks and monitor traffic to detect anomalies. Free DDoS protection and mitigation services are available, such as Google's Project Shield and Cloudflare's Athenian Project.

Detect

Have a dedicated person with the job of looking for fake content or spoofed websites in search engine results.

Recover

Have a backup version of the website hosted elsewhere in case the primary site goes down. This version should contain only barebones, essential information (e.g., precinct locations / hours).

Vendor Considerations

Official websites are often created by vendors, and in many cases vendors are also responsible for making changes to them.

See General Vendor Recommendations 1-8 at the bottom of Technical Recommendations section for best practices that apply to working with vendors and mitigating potential vulnerabilities. Additional contract-specific recommendations are also provided in **Appendix 1: Vendor Selection and Maintenance**.

Social Media (official and private accounts)

KEY THREATS:

Account compromise: Attackers use spear-phishing to learn the username and password for the county Facebook page which did not have two factor authentication enabled. The attackers then post misinformation about certain voting sites having several hour wait times and direct voters to alternate sites which are then overwhelmed.

Fake accounts: Malicious actors create a fake Twitter account for an election official (e.g., Secretary of State, Election Director) which gains traction because it is retweeted by a bot farm controlling several thousand accounts. The fake account then posts the wrong unofficial election results after polls close.

Recommended actions:

Identify

Be cognizant of which accounts could be used to disseminate information about an election. This includes accounts for your organization, as well as both the professional and personal accounts for officials. Determine who has access to each of these accounts.

Identify points of contact and establish relationships with key social media firms like Facebook and Twitter. Confirm a point of contact in case social media accounts connected to the election are compromised; or in case malicious fake accounts surface. Confirm the requirements for regaining control over accounts and shutting down malicious fake accounts.

Know key stakeholders for communication channels (media, political party contacts, advocacy groups, etc.)

Protect

Inform key officials that their private accounts might be targeted. Establish clear policies for officials and staff on use of private accounts for sharing official information, including policies for communicating indications of malicious cyber activity.

Secure social media accounts. Social media services such as Twitter and Facebook support two-factor authentication for accounts, and enabling this capability is the best step you can take to keep your accounts secure and should be done for both official accounts and the personal accounts of key personnel. In addition to this, require that the passwords for your official accounts be secure.

Understand third-party apps can be a vulnerability if they are compromised. Use third-party social media management platforms judiciously to reduce your threat surface. Periodically review linked accounts and connected apps and remove any that are no longer required.

Detect

Have a dedicated person responsible for looking for fake content in search engine results or on social media.

Recover

See the **Election Cyber Incident Communications Playbook** and **Election Cyber Incident Communications Plan Template** *for State and Local Election Officials*.

Engage with social media firms to recover/disable accounts.

If an account has been compromised, review what permissions it has granted to third-party apps and reset them to prevent further access by unauthorized parties.

Vendor Considerations

If you need to use a third-party social media application to manage social media accounts, then research the applications security practices and access policies to understand what vulnerabilities using it presents.

Vendor Considerations

*(See **Appendix 1, Vendor Selection and Management**, for best practices related to vendor contracts.)*

1. **Clearly define** the division of labor and responsibilities between the vendor and the local officials. Identify any gaps between the two parties and specifically assign responsibility to fill those gaps.
2. **Create and enforce contractual requirements.** Require vendors to adhere to well-defined security practices ensuring safe handling and protection of data.
3. **Require vendor assessments.** State/local contracts with vendors should include provisions requiring vendors to conduct third-party vulnerability assessments of their systems and share the results. See vendor appendix for more details.
4. **Mandate that vendors permit penetration testing of systems**, including voting machines, as part of RFP contracts.
5. **Secure access.** Unnecessary personnel should not have access to systems. Vendors who need access to secure systems should be granted temporary credentials and exercise that access under the supervision of a state or county official. Once a developer has finished building an application, ensure that they do not have access to the production system.
6. **Secure data transmissions.** Require vendor systems to use digital signatures to ensure the integrity of all received and transmitted files.
7. **Require audit logs for any vendor-run system.**
8. **Mandate patching** as part of a vendor request for proposal (RFP) contracts and ensure that the patching is conducted securely and frequently.

Appendices

Appendix 1. **Vendor Selection and Management**

Election system vendors are key partners in addressing cybersecurity risks. Their systems, by definition, increase the attack surface and present additional risk factors that must be mitigated to address cyber threats. Since vendors often develop and maintain systems critical to elections (such as ballot counting equipment and VRDBs), it is crucial to ensure that their protocols and practices meet rigorous cybersecurity standards.

Performing a security risk assessment of vendors during the request for proposal (RFP) process can reveal vendor vulnerabilities and reduce future exposure to external attacks. This risk assessment should be conducted in two steps: 1) during the procurement process, ensure that all vendors are willing and able to comply with security standards that meet, or exceed, election agency expectations, and 2) validate vendors' ability to meet their commitments via thorough due diligence, and ensure that vendors are reviewed periodically, not just at the time of selection.

When assessing a vendor, there are three general principles to consider:

Organizational security practices. Evaluate the extent to which cybersecurity activities and outcomes are embedded across the organization, from the executive level to the implementation/operations level, such as hiring, subcontracting, policies and procedures, cybersecurity awareness and training, network and system management, vendor management, vulnerability management, and software/hardware development.

Ongoing partnership capacity. Vendors should be your partners in addressing cybersecurity risks! Evaluate the levels of transparency associated with their cybersecurity processes, and to what extent they will collaborate with you on key security risk-mitigation activities, including consequence management after a cyber incident. These would include code reviews, vulnerability scans, patching, and implementing controls to strengthen their security posture, while also closing critical gaps.

Maintenance strategy. Cybersecurity is not a "point in time" activity and you may have a long-term relationship with a vendor. As new attacks emerge, software and hardware should be updated commensurate with the nature of evolving risks and the state of the art in cybersecurity safeguards. This expectation must be built into vendor contracts.

Specific security requirements for vendor agreements

With the above principles in mind, security requirements should be clarified in RFPs to ensure that vendors are limiting cyber risks while working with the states or counties. The following set of core security requirements are not exhaustive, but they do provide a foundation to include in vendor RFPs. Each vendor bidder should be required to:

- State how system access in the proposed solution will be managed.
- Describe what type of data will be processed and how it will flow through the system, including any relevant data processing or data storage vendors and, if applicable, locations.
- Describe security at all layers of the solution—application, server, database, data exchange, and network security layers should all have the ability to manage access and privileges at a granular level.
- Describe how security measures will protect data for the entire data life cycle, ensuring that data remains protected for as long as it is in the control of the vendor and, when required, is securely destroyed.
- Describe how the proposed solution meets or exceeds compliance with all state- or county-level security requirements.
- Describe how encryption will be implemented for data "at-rest" and "in-transit."
- Describe how User Access Management will be handled under the principle of "least privilege" (i.e., provide only the minimum level of access required for the user to perform his or her core job), as well as how it will be maintained and pared over time.
- In your Service Level Agreements (SLAs), include clauses for vendors to notify you in the event of a cybersecurity breach of their systems or other unauthorized access immediately after they become aware and to cooperate with any consequential investigation, response, and mitigation.

Transparency requirements should also be established in the RFP to ensure that officials have the ability to perform due diligence and conduct independent security risk assessments. Moreover, transparency will aid in identifying potential conflicts of interest. Non-Disclosure Agreements will protect vendor proprietary information, in exchange for receiving access to:

- **Corporate governance relating to security practices.** Officials should have the ability to review vendors' security policies, standards, and guidelines. They should be able to

assess whether these are implemented in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level.

Internal security audits. State officials should perform audits (and retain the right to do so) of a vendor's security practices and protocols. This activity provides assurance that the vendor's cybersecurity practices are robust and meet state and local security standards, including those outlined in the above section. This is especially important in the months and years after vendor contracts are signed. Vendor-provided system logs should be contractually viewed as customer owned data not vendor owned data. For instance, voting system audit logs should be readily available to election officials and considered by contract as their data.

Source code. Election officials should have access to the source code for any critical system to perform internal or third-party reviews. This can be a sensitive subject because of intellectual property concerns, but being able to independently audit vendor-created code allows officials to ensure that the code is secure. It also guarantees that the code does not contain any potentially unwanted networking requests, transfers of sensitive information, or modifications to key algorithms and counting mechanisms.

Penetration testing. Penetration testing is a critical element in ensuring that vulnerabilities in vendor environments are proactively identified and closed. The RFP should clearly include requirements for the vendor to allow penetration-testing by state officials or third parties of their systems to discover weaknesses. Vendors may resist these provisions, especially if they hold broader state contracts that could be affected if vulnerabilities are discovered. Nonetheless, conducting these tests represents the best way to identify cracks in critical infrastructure before malicious actors do, and should be part of any contract with vendors who work on and maintain these systems.

Data flow transparency. Officials should have full visibility into data flows for voting system data. Therefore, it is essential for officials to request that the vendor provide its applicable data retention and destruction policies, a list of relevant physical locations where data will be processed, stored, or otherwise accessed, and an exhaustive list of subcontractors who may process, store, or otherwise access voting data or systems. Depending on the nature of the vendor's services, it may be necessary to impose flow-down security and audit requirements on subcontractors, including on the vendor's infrastructure vendors, or, if relevant, to explicitly restrict data storage locations.

Appendix 2. **Election Audits**

While following cybersecurity best practices will help deter and defend against malicious actors, there is no such thing as an impenetrable system. Even if an election system is not attacked, software or hardware errors could lead to an incorrect vote tally. To protect against technical manipulation or failures undermining the process, elections should be "software independent," meaning that they do not rely on a computer to provide a vote count, but instead have an independent auditable paper record for definitive results.

You should conduct a post-election statistical audit with these paper voting records. Such audits provide two critical benefits: (1) they offer transparency and build public confidence in the system and process; (2) they confirm the accuracy of the results, or, on rare occasion, identify that an error has occurred and must be addressed. Post-election audits are designed to be an independent confirmation of the election result. These audits should be observable and reproducible by external third parties. This requires making data necessary to conduct the audit publicly available to independent parties so that they can confirm audit results.

There are two main methods of post-election audits. Since performing a full hand-count of every ballot is extremely time-intensive and the results will likely be inaccurate, other methods are used to inspect the results with a manageable amount of work.

The first audit type uses a fixed percentage of ballots cast. This method, however, can overestimate or underestimate the necessary number of ballots required for a successful audit. In the overestimation case, the audit is inefficient and a waste of resources; in the underestimation case, the audit doesn't fulfill its purpose. That said, a fixed percentage audit is still better than no audit at all and is regarded as a "good" standard of practice.

The second type is the statistical audit where statistical methods are used to determine and inspect the minimum number of ballots required to confirm that an election has not been altered—this would be considered an "enhanced" standard of practice. As the margin of victory between the winner and loser narrows, more ballots are required to ensure an accurate audit. Typical implementations of statistical audits could require multiple rounds of ballot inspection if discrepancies are found with recounted ballots. If the statistical audit fails, a full recount of all ballots is necessary to ensure the election has not been compromised.

The following section discusses the "good" and "enhanced" audit techniques: (1) *Good:* fixed-percentage audits; (2) *Enhanced:* risk-limiting audits with two variants (a) comparison audits, and (b) ballot-polling audits.

Fixed-Percentage Audits

Fixed-percentage audits provide some evidence that results are valid. One example process: Counties indicate to the Secretary of State (or State Election Director) which machines they will use in the election, then the Secretary of State (or Election Director) randomly selects one DRE and one optical ballot scanner per county. The county must then audit a fixed percentage (e.g., 20 percent) of the ballots tallied by the optical scanner, as well as manually counting all the paper vote records produced by the DRE and comparing this number to the DRE's electronic vote count. This process ensures that, for the randomly selected machines, the pre-election logic and accuracy tests were successfully conducted, a chain-of-custody was maintained, and the devices functioned properly on election day. The weakness of a fixed-percentage audit is that specific devices, rather than the election itself, are audited. Election officials cannot be certain that the election as a whole was conducted correctly, but this may be the best available option for some counties with limited resources or technology.

Risk-Limiting Audits (Enhanced Statistical Methods)

The first step in any risk-limiting audit is setting the risk limit. Setting a 5 percent limit means that if an audit is conducted on an election that did, in fact, experience tampering, there is at most a 5 percent chance that the audit will not discover the error and at least a 95 percent chance that the audit will find the election outcome to be manipulated. The number of ballots required for a risk-limiting audit is determined by the risk limit and margin of victory. A closer election or lower limit requires more ballots to be audited. There are two types of risk-limiting audits: (1) comparison audits and (2) ballot-polling audits.

A. **Comparison vs. Ballot-Polling Audits.** A comparison audit involves recounting a randomly selected set of ballots and comparing those results with the original machine-recorded tabulation of those exact ballots, called the Cast Vote Records (CVRs). Comparison audits are typically recommended over ballot-polling audits for greater efficiency. Unlike a ballot-polling audit, a comparison audit requires knowing the original tabulation results of the specific ballots you are auditing (in the CVR) and comparing

discrepancies. A ballot-polling audit simply looks at the outcome of the ballots inspected. Because of this precision, comparison audits require far fewer ballots to be counted than do ballot-polling audits. However, comparison audits require specific data (machine tabulation and associated paper vote record from a given voting machine), which may be infeasible for some counties.

B. **Audit Level.** Audits can operate on different levels depending on the infrastructure available. A unit could be a single ballot, a batch of ballots, all the ballots processed by a machine or all the ballots in a given precinct. For a given unit, samples are typically selected randomly then the ballots within that unit are inspected. For statistical risk calculations, the larger the unit, the larger the total number of ballots that will need to be inspected to have the same risk of missing an incorrect outcome. Ballot-level comparison audits are most efficient in terms of number of ballots considered for a given margin of victory and risk limit because they spread the audit across many ballots in multiple precincts. This means this audit is more likely to find any election meddling. Batch, machine, or precinct level audits require doing a comparison audit on batches of ballots only at certain precincts. This is less likely to find election meddling and requires auditing more ballots to ensure the same level of confidence that an election outcome is true, but may be more feasible for some counties.

There has been extensive research on this issue by leading experts in the field of election auditing. The following reports can provide additional information:

"A Gentle Introduction to Risk Limiting Audits" Mark Lindeman and Philip B. Stark

"Bayesian Tabulation Audits: Explained and Extended" Ronald L. Rivest

"On the Notion of 'Software-Independence' in Voting Systems" Ronald L. Rivest and J.P. Wack

"Evidence-Based Elections" by Philip B. Stark and D.A. Wagner

External Resources Guide

There are many threats that could undermine the democratic process; fortunately, election officials are not in this alone. There are resources available that can help defend against those threats, including free ones.

Federal Support

The Department of Homeland Security (DHS) Office of Cybersecurity and Communications (CS&C) offers a variety of services at no cost or minimal cost for states and counties. Services include:

1. Cyber Hygiene checks, which scan election and other Internet-accessible systems (such as public-facing VRDB portals) for vulnerabilities and configuration errors. DHS can also provide a report that outlines steps to address or mitigate vulnerabilities detected in the scan.
2. Risk and Vulnerability Assessments (RVAs), which involve DHS teams performing in-depth on-site analysis of a state or local election facility's internal and external networks. RVAs can include penetration testing, vulnerability scanning and testing, database and operating systems scans, Web application scanning and testing, and several other services.
3. The National Cybersecurity and Communications Integration Center (NCCIC) is a cybersecurity situational awareness, incident response, and management center that operates 24 hours a day, 7 days a week. NCCIC collaborates with the Multi-State Information Sharing and Analysis Center (MS-ISAC) to provide information to State and local governments.
4. MS-ISAC disseminates early warnings on cyber threats to state and local governments as well as security incident information and analysis through a 24-hour security operations center. MS-ISAC also provides intrusion detection.
5. Cyber Security Advisors (CSA) and Protective Security Advisors (PSA) are security professionals deployed in all 50 states to provide direct assistance, such as vulnerability assessments, and reach-back to additional government resources and capabilities.

Private Sector Support

For defending election system-related public-facing websites, Google's Project Shield and Cloudflare's Athenian Project are free services that defend websites from distributed denial of service (DDoS) attacks. Other software development firms are developing free open source software to assist states and localities in conducting risk-limiting audits. Several highly experienced cybersecurity firms also offer penetration testing and risk vulnerability assessments.

National Guard Collaboration

The National Guard is building cyber units in many states and territories. These units align with the Army and Air Force. When not performing their federal mission, these units may be available for state-specific tasking under state authorities. Several states have employed their National Guard cyber capabilities to participate in activities such as vulnerability assessments and penetration testing.

Recognizing that there are Constitutional and legal sensitivities, states interested in exploring opportunities with their National Guard units should work through their governor's office and ultimately their state's Adjutant General office. If states do not have a resident National Guard cyber capability, they can potentially partner for support with nearby states who do have this resource. In some cases, support can be provided through the Emergency Management Assistance Compact (EMAC) process, similar to other civil support capabilities. These compacts act as a complement to the federal disaster response system, providing timely and cost-effective relief to states requesting assistance. A useful analogy is to consider National Guard support in cyberspace in a similar light as the laying of sandbags before a storm in the physical world.

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DEFENDING DIGITAL DEMOCRACY
FEBRUARY 2018

What Every Election Staffer Should Know About Cybersecurity

1. **Everyone is a security official**
   Take cybersecurity seriously. Take responsibility for reducing risk, training your staff, and setting the example. Human error is the number one cause of breaches. Spear-phishing attacks and other attempts at interference can be thwarted with cybersecurity vigilance.

2. **Use two-factor authentication (2FA)**
   Use two-factor authentication for everything: official work accounts, personal email accounts, social media accounts, and any data storage services. Use a mobile app (such as Google Authenticator, Duo, or Authy) or a physical key (such as Yubikey or other U2F devices) for your second factor, not text messaging. 2FA is an extra step, but is very effective at preventing unauthorized access.

3. **Create long, strong passwords**
   Current computing capabilities can crack a seven-character password in milliseconds. For your passwords, create `SomethingReallyLongLikeThisString`, not something really short like `Th1$`. Contrary to popular belief, a long string of random words without symbols is more difficult to break than something short, with lots of `$ymB01$`.

4. **Keep credentials secure**
   When collaborating with others, resist the temptation to share credentials to systems with them, regardless of who they are.

5. **Practice cyber hygiene**
   Follow all applicable guidance for patching and software updates. Ensure that your systems have the most updated antivirus software.

Glossary

Based on the Election Assistance Commission's Common Cybersecurity Terminology and Information Technology Terminology Glossaries

Cybersecurity Terms:

Access
Ability to make use of any information system (IS) resource.

Access control
The process of granting or denying specific requests: (1) obtain and use information and related information processing services; and (2) enter specific physical facilities.

Advanced Persistent Threat
An adversary who possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.

Air gap
An interface between two systems at which (a) they are not connected physically and (b) any logical connection is not automated (i.e., data is transferred through the interface only manually, under human control).

Asset
A major application, general support system, high impact program, physical plan, mission-critical system, personnel, equipment, or a logically related group of systems.

Attack
An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality.

Attacker
A party who acts with malicious intent to compromise an information system.

Authentication
Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Backups
A copy of files and programs made to facilitate recovery if necessary.

Black-box testing
A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. Also known as basic testing.

Blacklist
A list of entities that are blocked or denied privileges or access.

Breach
Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, protected information.

Compromise
A violation of the security policy of a system such that an unauthorized disclosure, modification, or destruction of sensitive information has occurred.

Critical infrastructure
System and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national security, economic security, national public health or safety, or any combination of those matters.

Cybersecurity
Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Data Loss
The exposure of proprietary, sensitive, or classified information through either data theft or data leakage.

Decryption
The process of changing ciphertext into plain text using a cryptographic algorithm and key.

Denial of Service
The prevention of authorized access to resources or the delating of time-critical operations.

Encryption
The process of encoding messages or information in such a way that only authorized parties (or software applications) can read it. Encryption does not prevent interception, but denies the message content to the interceptor. Encrypted information must be decrypted before it can be rendered into plain text or other usable format. Encryption and decryption add overhead to processing and can slow systems down. Voting systems will commonly encrypt data within a voting system component before transmitting it to another device.

Firewall
The process integrated with a computer operating system that detects and prevents undesirable applications and remote users from accessing or performing operations on a secure computer.

Hack
Unauthorized attempt or access to an information system.

Hash Function
An algorithm that computes a numerical value (called the hash value) on a data file or electronic message that is used to represent that file or message, and depends on the entire contents of the file or message. A hash function can be considered to be a fingerprint of the file or message.

Incident Response Plan
The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attack against an organization's information systems(s).

Intrusion
A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without having authorization to do so.

Multi-factor Authentication
Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something that identifies who you are (e.g., biometric).

Password
A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

Patch
An update to an operating system, application, or other software issued specifically to correct particular problems with the software.

Penetration Testing
Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability.

Phishing
Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.

Port
The entry or exit point from a computer for connecting communications or peripheral devices.

Port scanning
Using a program to remotely determine which ports on a system are open (e.g., whether the systems allow connections through those ports).

Private key
A cryptographic key that is used with an asymmetric (public key) cryptographic algorithm. For digital signatures, the private key is uniquely associated with the owner and is not made public. The private key is used to compute a digital signature that may be verified using the corresponding public key or to decrypt information which has been encrypted using the public key.

Risk analysis
The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment.

Risk assessment
The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls that are planned or in place.

Spear Phishing
A colloquial term that can be used to describe any highly targeted phishing attack.

Spoofing
Faking the sending address of a transmission to gain illegal entry into a secure system.

Structured Query Language (SQL) injection
An attack technique that attempts to subvert the relationship between a webpage and its supporting database, typically in order to trick the database into executing malicious code.

Supply Chain
A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers.

Tabletop Exercise
A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.

Threat
Any circumstance or event with the potential to adversely impact organizational operations, (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Trojan horse
A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

Unauthorized access
Any access that violates the stated security policy.

Vulnerability
Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Whitelist
A list of discrete entities, such as hosts, email addresses, network port numbers, runtime processes, or applications that are authorized to be present or active on a system according to a well-defined baseline.

General Information Technology Terms:

Air Gap
An air gap is a physical separation between systems that requires data to be moved by some external, manual procedure. Also called "Sneaker Net." Election systems often use air gaps intentionally to prevent or control access to a system. Copying election results to a CD or USB drive, then walking that media to a different computer for upload and use in a different system is an example of an air gap.

Audit
A review of a system and its controls to determine its operational status and the accuracy of its outputs. Election system audits seek to determine if controls are properly designed and functioning to ensure the correctness of intermediate and final results of the system's processing.

Audit trail
The records that document transactions and other events. Some audit trails in election systems are event logs, paper records, error messages, and reports.

Authentication
The process of identifying a user, usually by means of a username and password combination. Election systems use authentication methods to assure that only those users with appropriate authority are permitted access to the system. Authentication schemes should not permit group logins.

Blacklist
A list of URLs, domains, users, or other identifiers, that have had system access or privileges blocked. Election offices may wish to "add" domains to be blocked to a blacklist, maintained by their system administrator.

Code
n. Synonym for program or software.
v. to create or modify software.

Data destruction
The removal of data from a storage medium. Election officials should destruct all data on election systems before selling or disposing of the systems. Any election system that is to be destroyed should use a reputable company and best practices for destruction, so that data cannot be obtained after it is no longer in the custody of the election official.

Database
A structured collection of data that includes data and metadata (data about the data). Databases are managed by database management systems. The election database stores all of the requisite information to manage election including precinct information, race and candidate information, and data used to prepare the ballots, tabulate, and report results.

Download
Transferring data from a larger computer to a smaller computer or device. An EMS facilitates downloading ballot images to vote capture devices.

Dox
Publish damaging or defamatory information about an individual or organization on the Internet. One method of hacking a campaign is doxing (or doxxing).

File
A collection of related data, stored on media. Files will be identified by a system-valid filename.

Firewall
A gateway computer and its software that protects a network by filtering the traffic that passes through it. Election offices often need to reconfigure the firewall to permit large files or complex files to be passed through the firewall that separates the office from the Internet.

Two-factor Authentication
Authentication mechanism requiring two or more of the following: something you know (e.g., Password), something you have (e.g., Token), something that identifies who you are (e.g., biometrics).

Penetration Testing
Also called Pen Testing. An evaluation method that enables a researcher to search for vulnerabilities in a system. Election systems, such as the VR system, are periodically submitted to a Pen Test to determine their vulnerabilities to cyber attacks.

Ransomware
Malware that holds the victim's device (computer, phone, etc.) and data for ransom, by means of encrypting the files on the device or preventing access to the device. Election office computers should maintain high levels of cyber hygiene, including up-to-date anti- malware systems and adherence to best practices regarding managing browser and email client activities.

Social Engineering
Misleading users into providing information that can be used to compromise the security of a system. Usually low-tech. Social engineering of election officials includes emails and phone calls requesting information that can be used to spoof accounts or hack passwords.

Software
A synonym for program. Computer software is the collection of programs that control the computer and perform a specific collection of tasks. Software has version numbers and is licensed (not sold) to the end user. Software can be altered to change the functionality of the computer. The Election Management System (EMS) used to create election databases is software.

Spear Phishing
A targeted attack by hackers, via bogus emails, that attempts to get the victim to provide login information or personal information to the hackers. Spear Phishing attempts may appear to originate from legitimate, known sources, such as organizational IT or known vendors. Election officials should NOT click through on suspicious links or open attachments without first verifying that the email is legitimate.

Software Patches
Also called fixes or bug fixes. Corrections to existing programs, designed to be integrated into the programs without major release changes. Patches or fixes to voting systems must be tested before being applied, and may invalidate certifications. Do not install software patches without extensive technical review for unintended consequence.

Tabletop Exercise
A discussion-based drill where qualified personnel discuss scenarios and responses in order to validate plans and procedures. Also called Incident Response Planning. Election officials exchange in tabletop exercises to determine the viability of their election continuity plans.

Wi-Fi
Wi-Fi is a wireless networking technology that uses radio waves to provide wireless high- speed Internet and network connections. Wi-Fi is a trademarked phrase for the *IEEE 802.11x* standard. Wireless is less secure than Ethernet connections. Some e-Pollbook and voting system technologies use Wi-Fi or wireless connectivity at the polling place.

Election Administration Technology Terms:

Central Count Optical Scan
Optical scan system that utilizes one or more high-speed scanners at a central location to tabulate ballots. Central count systems are usually paired with Vote By Mail technologies. Central count systems lack overvote/undervote protection capabilities.

Digital Optical Scan System
Optical scan system that converts voter choices on a paper ballot to digital values. Digital op scan systems can accommodate a broader range of paper types, sizes of paper, ballot layout, and voter marks than IR op scan systems.

Direct Record Electronic Voting System (DRE)
A DRE system presents a ballot image to a voter, collects the voter's choices, and records those choices directly onto electronic media. DREs may be fitted with VVPAT subsystems to create a paper artifact of the voting transaction. DREs are capable of audio interaction and image displays, and can hold a large number of ballot styles in multiple languages.

Election Night Reporting Systems (ENR)
A web-based system that aggregates and displays unofficial election results across the jurisdiction. ENR systems can be real-time or near-real-time, and acquire their data from the EMS. ENR systems can provide multiple formats for displaying election results and may provide direct feeds for the media.

Electronic Poll Book (EPB)
Hardware and/or software that permits election officials to review the electors list and mark voters who have been issued a ballot. Also called an e-Pollbook. E-Pollbooks can be standalone at the precinct with a separate copy of the electors list, or can be networked into a central voter registration system and check and update voter records in real time.

High-Speed Central Count Tabulation System
An optical scanner capable of scanning a high number of ballots (hundreds) per minute. These large and complex scanners are typically used in vote-by- mail jurisdictions, in large jurisdictions that have a large number of absentee ballots, or in central count jurisdictions.

Optical Scan System (Op Scan)
A voting system that can scan paper ballots and tally votes. Most older op scan systems use Infrared (IR) scanning technology and ballots with timing marks to accurately scan the ballot.

Precinct Count Optical Scan
Optical scan technology that permits voters to mark their paper ballots within a precinct and submit the ballot for tabulation. Precinct Count systems provide overvote/undervote protection.

Risk-Limiting Audit
Risk-limiting audits provide statistical assurance that election outcomes are correct by manually examining portions of paper ballots or voter-verifiable paper records.

Voluntary Voting System Guidelines (VVSG)
Collection of standards that is developed and maintained by the EAC. The VVSG specifies a minimum set of performance requirements that

Voter Verified Paper Audit Trail (VVPAT)
Contemporaneous paper-based printout of voter choices on a DRE.

Do you see a way to make this Playbook better?

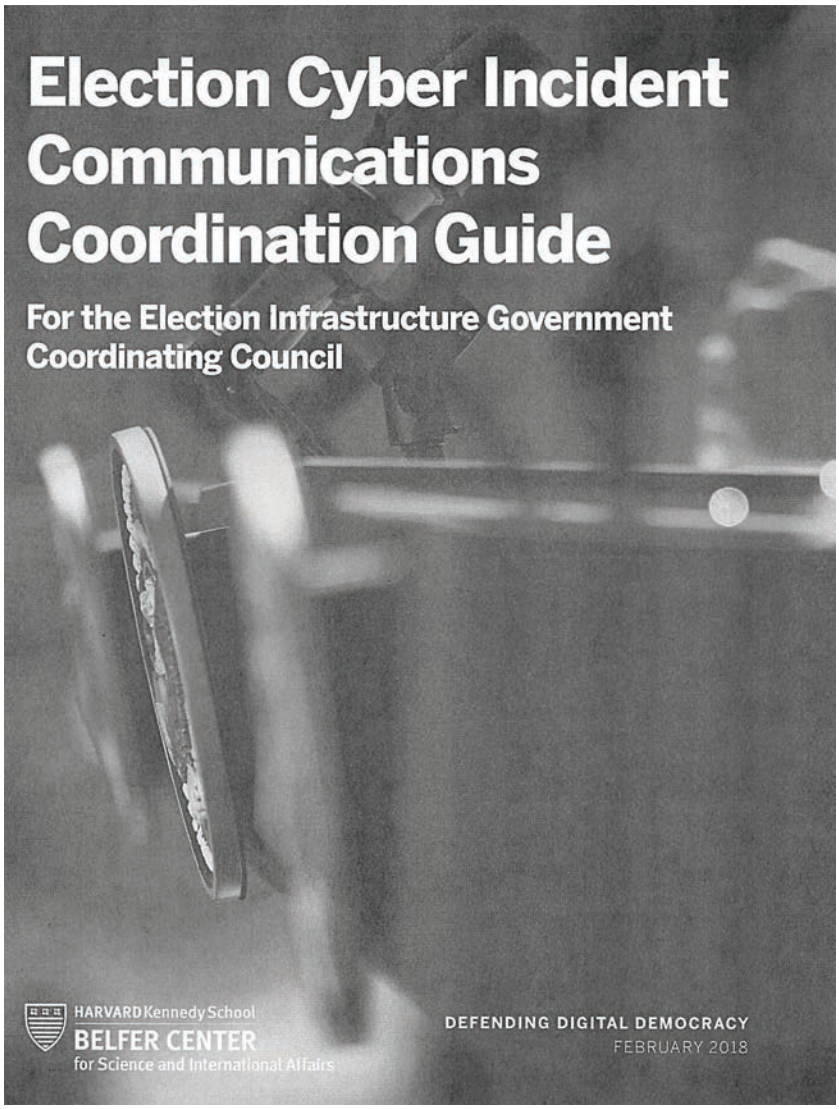
Are there new technologies or vulnerabilities we should address?

We want your feedback.

Please share your ideas, stories, and comments on Twitter @d3p using the hashtag #electionplaybook or email us at connect@d3p.org so we can continue to improve this resource as the digital environment changes.

Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 John F. Kennedy Street
Cambridge, MA 02138

www.belfercenter.org/D3P


Election Cyber Incident Communications Coordination Guide
For the Election Infrastructure Government Coordinating Council
HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs
DEFENDING DIGITAL DEMOCRACY
FEBRUARY 2018

Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/D3P

Design & Layout by Andrew Facini

Cover photo: A view of the podiums during a news conference in the Rose Garden at the White House, Monday, April 2, 2012. (AP Photo/Charles Dharapak)

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DEFENDING DIGITAL DEMOCRACY
FEBRUARY 2018

Election Cyber Incident Communications Coordination Guide

For the Election Infrastructure Government Coordinating Council

Contents

Defending Digital Democracy Project: About Us

We established the Defending Digital Democracy Project (D3P) in July 2017 with one goal: to help secure democratic elections against cybersecurity threats and information operations.

There are two groups on the frontlines of defending democracy: (1) political campaigns, which enable citizens to pursue elected office; and (2) election officials, who ensure the election process is free and fair.

Last year, we set out to provide campaign and election professionals with practical guides to the most applicable cybersecurity best practices in advance of the 2018 midterm elections. In November 2017, we released "The Campaign Cybersecurity Playbook" for campaign professionals.

Now, we are releasing a set of three playbooks designed to be used together by election administrators: **"The State and Local Election Cybersecurity Playbook," "The Election Cyber Incident Communications Coordination Guide,"** and **"The Election Incident Communications Plan Template."** What follows is the Coordination Guide.

D3P is a bipartisan team of cybersecurity and policy experts from the public and private sectors. To better understand the cyber threat and other challenges that election administrators face, our team spent four months interviewing state officials about their communications practices and how they would or would not apply these practices in a cyber incident. We spoke with state and local election officials, as well as key national-level players and members of the Election Infrastructure Government Coordinating Council (EI-GCC).

These interviews exposed the range of challenges election officials confront in the cyber domain. One of the most significant needs we encountered was the ability to communicate consistently across states in the event of a major election cyber incident, in order to maintain public trust.

This Guide is primarily intended for use by the EI-GCC to coordinate multiple voices (and multiple facts) in an election cyber incident that crosses traditional jurisdictions. We are releasing the Guide publicly, because a range of officials may be interested in learning more about how state and local leaders can, and should, coordinate their communications in the event of this type of cyber incident. We hope this Guide becomes a starting point for the EI-GCC to establish its role as a central communications node in the event of an election cyber incident.

Finally, we would like to thank the election officials around the country for whom we wrote this guide You are the frontline defenders of democracy. We hope this effort helps make that tremendous responsibility a little easier.

Good luck,
The D3P Team

Authors and Contributors

This project was made possible by dozens of people who generously volunteered their time. Special thanks are due to **Siobhan Gorman** for leading the project and who, in addition to **Matt Chandler**, **Meredith Davis Tavera**, and **Chris Farley**, wrote this Coordination Guide.

We are also indebted to the people listed below who invested countless hours in reviewing drafts and providing input.

SENIOR ADVISORY GROUP

Eric Rosenbach, Co-Director, Belfer Center; Director, Defending Digital Democracy Project

Robby Mook, Co-Director, D3P

Matt Rhoades, Co-Director, D3P

Heather Adkins, Dir. of Information Security and Privacy, Google

Dmitri Alperovitch, Co-Founder and CTO, CrowdStrike

Siobhan Gorman, Director, Brunswick Group

Yasmin Green, Head of Research & Development, Jigsaw (Alphabet)

Stuart Holliday, CEO, Meridian International Center

Kent Lucken, Managing Director, Citibank

Debora Plunkett, former Director of Information Assurance, National Security Agency

Colin Reed, Senior Vice President, Definers Public Affairs

Suzanne Spaulding, Senior Advisor for Homeland Security, Center for Strategic and International Studies

Alex Stamos, Chief Security Officer, Facebook

CONTRIBUTORS

Lori Augino, Director of Elections, WA Office of the Sec. of State

Matt Chandler, Partner, Frontier Solutions

Caitlin Conley, Executive Director, D3P

Amy Cohen, Executive Director, National Association of State Election Directors

Meredith Davis Tavera, D3P, Harvard Kennedy School

David Forsey, Policy Analyst, National Governors Association

Shannon Cortez, Deputy Director of Elections, WA Office of the Secretary of State

Chris Farley, Associate, Albright Stonebridge Group

David Forsey, Policy Analyst, National Governors Association

Karen Ejiofor, Staff Assistant, Belfer Center

Siobhan Gorman, Director, Brunswick Group

Eben Kaplan, Principal Consultant, CrowdStrike

Jane Khodos, Senior Director, Comms. and Content, FS-ISAC

Matthew Masterson, Commissioner, Election Assistance Commission

Jeff McLeod, Division Director for Homeland Security and Public Safety, National Governors Association

Robby Mook, Co-Director, D3P

Matt Rhoades, Co-Director, D3P

Eric Rosenbach, Co-Director, Belfer Center; Director, Defending Digital Democracy Project

Michelle Tassinari, Director/Legal Counsel, Elections Division, Office of the Secretary of the Commonwealth of MA

BELFER CENTER WEB & DESIGN TEAM

Arielle Dworkin, Digital Communications Manager, Belfer Center

Andrew Facini, Publications and Design Coordinator, Belfer Center

Acknowledgments

The D3P team would like to especially thank Heather Adkins of **Google**, Yasmin Green of **Jigsaw**, the **Hewlett Foundation**, the **Democracy Fund**, and the **Belfer Family**; without whom this Playbook would not have been possible. Additionally, we would like to thank the following organizations and offices for sharing their time with us through conversations, simulation participation, or field visits. Your perspectives were critical in shaping our approach to this document.

Department of Homeland Security (DHS)
National Association of State Election Directors (NASED)
National Association of Secretaries of State (NASS)
National Governors Association (NGA)
National Guard Bureau (NGB)

Election Officials from the Following States and Jurisdictions:

Atlantic County, New Jersey
Nevada County, California
Orange County, California
Santa Clara County, California
State of Colorado
Arapahoe County, Colorado
City and County of Denver, Colorado
State of Connecticut
Escambia County, Florida
Cook County, Illinois
State of Louisiana
State of Maryland
Caroline County, Maryland
Commonwealth of Massachusetts
State of Minnesota
State of Nevada
Clark County, Nevada
State of New Jersey
Mercer County, New Jersey
State of North Carolina
State of Ohio
State of Oregon
Multnomah County, Oregon
Commonwealth of Pennsylvania
State of Rhode Island
State of Tennessee
State of Vermont
Commonwealth of Virginia
State of West Virginia
Harrison County, West Virginia
State of Washington
State of Wisconsin

How to Use this Communications Guide

This communications guide includes best practices and guidelines to help the Election Infrastructre Government Coordinating Council (EI-GCC) quickly coordinate the response to an election-related cyber incident that affects more than one state during the early days of the incident. While every cybersecurity incident is unique, this document provides a foundation on which the EI-GCC can build a response that addresses the incident with the goal of maintaining confidence in the election system.

This Guide should be owned by the communications director, or a similar position, at the EI-GCC and be updated at least annually.

Key topics include:

Strategy, Mission, and Objectives: The purpose of the Guide is to help election officials maintain public confidence in the integrity of the U.S. election system in the event of an election-related cybersecurity incident.

Establishing a Cyber Communications Baseline: This section explains the importance of educating the public and other key stakeholders on cyber threats facing the election process and steps currently being taken to counter them.

Cyber Incident Best Practices: This section includes best practices for communicating with the media and other key stakeholders.

Communications Process Workflow: This component includes diagrams that outline who will manage the cyber crisis communications response and serve as spokesperson during an incident.

Response Checklist: This checklist broadly outlines steps that should be taken during the first several days after learning about a potential incident.

Executive Summary and Purpose

What constitutes a "cyber incident" in elections can range from theft of voter registration data to disruption or manipulation of the vote tally. This Guide is designed to help coordinate and align communications across jurisdictional boundaries in an election-related cybersecurity incident that involves more than one state. Its primary purpose is to maintain (or regain) public confidence in the face of such an incident.

This Guide is written to help the Election Infrastructure Government Coordinating Council (EI-GCC) assist state and local election officials, who will need to communicate across jurisdictions if an election-related cyber event has impacts beyond a single state. While every jurisdiction should have its own plan to respond to a cyber incident, many incidents will have implications beyond state boundaries. It is critical to coordinate the response from the outset, so public comments confidently convey that the issue is being addressed and maintain public trust in election systems across the country.

We recommend the creation of a communications coordination structure within the EI-GCC, including a communications director, or similar role, who would be a key spokesperson in a cyber crisis.

A multistate cyber incident could take many forms. It could be a series of incidents that collectively have a broader impact. It could be one or a few incidents that, because of their strategic significance or other factors, have an impact beyond state boundaries, or receive outsized attention from national media outlets. This could even be a false rumor that requires a coordinated effort to stamp it out.

This Guide provides:

1. A set of best practices for communicating about an election-related cyber incident
2. A process for coordinating multistate communications decision-making, including spokespeople and communications messages

Additional communications response materials, including a sample escalation process and scenario-planning materials, are available to election officials and can be obtained upon request from the National Association of Secretaries of State, the National Association of State Election Directors, or the U.S. Election Assistance Commission.

Strategy, Mission, and Objectives

The potential for cyberattacks on our elections systems is an unfortunate reality of our time. Election officials should recognize, and plan for, a possible incident. **The primary objective of this communications guide is to enable the EI-GCC to help election officials maintain public confidence in the integrity of the U.S. election system** in the event of cyber incidents both locally and crossing state boundaries.

Election officials from both parties and at all levels of government agree that there is a shared national interest in preserving the public trust in our election system.

A central component of maintaining trust is providing the public with timely and accurate information. Equally important is dispelling inaccurate information as quickly as possible, especially in today's perpetual cycle of traditional and social media coverage.

Maintaining public trust is most effectively accomplished when election officials—across parties and jurisdictions—speak with one coordinated voice. If federal officials are contradicting state leaders, as occurred in 2016, the public is left confused and it can become all the more difficult to maintain confidence in the election process. Likewise, if federal, state, or local officials are contradicting one another, it is counterproductive and confusing to the public. For these reasons, EI-GCC will play a crucial role in coordinating the response.

All public statements should demonstrate the incident is being handled competently. Any specifics that are provided should be limited only to those that will not change. The scope of the incident, for example, is likely to shift and shouldn't be discussed publicly at the outset. Modifying your story can undermine confidence in the management of the incident and the election system itself.

To institutionalize a means to maintain public trust, **the communications response strategy underlying this Guide coordinates communications messages and delivery among election officials in a multistate cyber incident** to ensure consistency and accuracy of public information. To enable a unified response, we provide communications best practices and coordination processes.

Elections are governed at the state and local level, and there is a national interest in maintaining the integrity of, and confidence in, our elections system. So it is important to have a process that

will enable officials from all levels of government to: obtain and analyze the information; decide who will speak about the national implications of the incident; and provide information and communications to all elections officials, so they can communicate accurately, dispel rumors, and reinforce coordinated messages.

Beyond the coordinated multistate process outlined in this Guide, election officials at all levels of government should take measures to prepare for a cyber incident.

Among the steps you can take immediately are:

- **Establish (or update) a state or local communications response plan** to an election-related cyber incident. For a template state or local cyber communications plan please see the Election Cyber Incident Communications Plan Template.
- **Ensure that the communications plan is aligned** with the corresponding technical response plan, and that both are regularly updated.
- **Test those plans** with simulations.
- **Obtain regular updates** on cyber threats, particularly as they relate to elections.
- **Maintain relationships with officials** who will be relevant to coordinating a response to any cyber incident, including federal officials at the local level and other local community leaders.
- **Coordinate with political parties.** It is much easier to agree to protocols for sharing information about and responding to a cyber incident before the incident and before an election.
- **Educate the public about the work you are doing.** Set the expectation that there will likely be some cyber threat activity during an election and explain how that activity differs from what would be required to interrupt the elections process.

It is important to update and exercise communications response plans frequently—at least every year—to familiarize new players with the process and ensure you apply lessons learned from past experiences and exercises.

Establishing a Cyber Education Baseline

The public needs to understand the steps state elections officials are taking to counter cyber threats, as well as how difficult it is to execute a cyberattack that will disrupt an election outcome. If the public, and the media, understand the "new-normal," baseline activity of cyber threats targeting elections, they will be less likely to worry unnecessarily about news of small-scale election-related cyber incidents. If you don't have to spend considerable time allaying concerns over inconsequential incidents, you can focus your attention on the consequential ones.

The main point to make is that cyberattacks are now an issue all election officials must contend with, and the states have taken, and continue to take, steps to mitigate those threats. However, not every attempt is successful, and even successful ones are very unlikely to impact the outcome of an election.

Communications in a cyber crisis are most effective when the public has a baseline understanding of:

- The continuing work at all levels of government to counter that malicious activity and try to ensure it does not escalate to a major cyber incident
- The nature of the election data your agency holds, most or all of which is public data
- The malicious, but inconsequential, cyber activity that takes place regularly

We recommend that the EI-GCC consider taking on some of this public education role, which would address issues that extend across the states. The council is in a strong position to draw on data from across the country and across levels of government about both threats and actions being taken to enhance the cyber defenses of election systems. For this reason, we suggest that it consider publishing an annual report on the state of election cybersecurity.

The EI-GCC, perhaps in concert with the relevant associations and Information Sharing and Analysis Centers, could provide a regular cadence of cyber threat information, so the public understands how frequently attempts are made by a range of cyber threat actors to target election

infrastructure. Making this information common knowledge will mitigate the tendency to treat every reported attempted attack as a reason to question the election system.

The type of information you may want to share could include statements such as: "Based on threat information from the Department of Homeland Security and the Federal Bureau of Investigation (or state/local law enforcement), we are taking the following steps to address and mitigate these threats." If appropriate, this effort could take the form of regular background briefings for the media, as well as online materials and public panels or other educational events for other key stakeholders. The EI-GCC could also consider a joint public panel or forum with representatives of both political parties to discuss measures states are taking to mitigate cyberattacks.

The EI-GCC should also consider sharing limited, aggregate information on successful attacks once they have been addressed, which would establish the EI-GCC as a valuable resource for this type of information.

You should couple the cyber threat data with information on the actions states and localities are taking to strengthen the cyber defenses of election systems. This information should be specific enough to be credible while not being so detailed as to undermine your defenses. Work closely with information security and legal experts to strike the right balance.

We discuss how to establish a communications baseline in more detail in the section on communications process on Page 15.

Cyber Crisis Communications Best Practices

Election-related incidents fall broadly into five categories:

Online rumors that seek to undermine confidence in an election

Reconnaissance of election-related systems

Theft of voter or other election data

Data manipulation that could affect an election outcome

Data destruction

The top priority in a cyber crisis will be to maintain public trust. The most effective way to achieve that goal is to respond confidently and quickly. To do this, the EI-GCC will need to prepare, train for, and test its response ahead of time—especially because it is a new organization.

Planning Ahead

Near-term Planning	Longer-term Planning
• **Determine internal roles and responsibilities.** Make sure there is a clear escalation process for the EI-GCC and the right teams are talking to each other in the event of a cyber incident. Make an individual responsible for ensuring that this process is established and updated. • **Assess the current crisis communications plan** and analyze communications gaps and weaknesses. • **Plan your response to a cyber crisis in advance** with a communications plan, including a decision-making protocol and communications materials. • **Ensure that cyber incident response is part of the operational continuity plan.** Make sure there is a backup communications plan and system in place.	• **Conduct crisis simulation and table-top exercises,** coordinated with legal, technical, and outside advisors, including key senior leaders from multiple states, counties, coordinating bodies, and the federal government. • **Conduct stakeholder mapping and a risk analysis** to understand risks to trust in the election system, priority stakeholders, and how to reach stakeholders to address key concerns. Pay particular attention to outreach to voters and political parties. • **Educate the media** through background meetings and public events on the resiliency of the election system, and the current work to mitigate cyber threats. • **Educate the public** through online channels and public events on the resiliency of the election system and the current work to mitigate cyber threats.

Communications Response

Best Practices

Be transparent but careful. Transparent communication builds trust, but in a cyber incident, you will have few facts at hand, especially at the outset. Public comments should demonstrate that you are taking the issue seriously, but avoid providing any details that may change as the investigation progresses, so you don't have to correct yourself down the line. Avoid speculation on the perpetrator of the incident.

Focus on actions you are taking to address the issue. To demonstrate that you are taking the issue seriously, you should talk about the steps you are taking to protect voter information and address any broader risks to the system.

Provide context. In an election-system incident, there will be a temptation for public speculation. Counter speculation with facts and context to reduce the risk of undermining public trust. Include metrics whenever possible.

Be visual. Cybersecurity can be challenging to understand depending on a person's technical background. The quickest way to get your message out is to pair it with a graphic. Connect with design teams who can provide you infographics and develop a library of graphics and photos you can draw from.

Use the right digital tools. Use social media to dispel rumors. When a cyber incident strikes, social media is now a go-to source of immediate information. In practice, this means using it selectively to counter misinformation and inaccuracies.

Learn from the incident. Use your and others' experiences to improve your cybersecurity practices and crisis plans.

Guidelines for Communicating with the Public

Focus your communications on your most important stakeholder—the public. You will be tempted to discuss the components of the incident. Instead, talk about what you are doing to address public needs or concerns in this given situation.

Speak plainly. Cybersecurity can be off-putting to nontechnical audiences. Use anecdotes and examples to demystify cybersecurity issues whenever possible.

Demonstrate transparency by communicating with the public on a regular basis. Establish a regular series of communications with the media and the public about the cybersecurity measures you are taking now, so that the first time they hear from you is not in a crisis.

Best Practices for Countering Misinformation

Establish the facts, and double-check them. You need to ensure that you are operating from a factual position before countering misinformation, so check your facts with multiple sources before citing them publicly. Ask all appropriate questions and put in the work before you speak to be certain that you do not accidentally provide misleading information.

Develop a simple, accurate, short counter-message. Develop a clear statement that contains only the facts. Avoid complex messages. You can provide additional nuance later.

Respond quickly. Misinformation can spread rapidly through social media and broadcast commentary. Your counter-message should be ready to disseminate as soon as possible.

Be transparent. Caveated, incomplete, or "no comment" responses can fuel conspiracy theories by making it appear your organization has something to hide. Demonstrating transparency can help to counter false claims. Opportunities to demonstrate transparency could include inviting reporters "behind the scenes" at a polling place.

Engage on all platforms. Misinformation can spread across multiple platforms, including social media and traditional media. To counter misinformation, deliver a clear, factual message on all available platforms.

Avoid repeating misinformation. Focus on providing accurate facts and do not repeat the false messages. For example, if false rumors circulate that lines at the polls are many hours long, avoid saying that rumors of long lines are circulating. Instead, your message should be that lines are short and moving quickly.

Communications Process

Maintaining a coordinated process is critical to effective and efficient communications planning and response to a cyber-related incident. For an incident affecting multiple states, this coordinated communications process outlines:

- Key stakeholders
- Phased planning and response
- Coordination functions
- Feedback loop to incorporate lessons learned

In this communications process, we assume that information and messaging coordination functions will be performed by cross-jurisdictional organizations that have played a similar role in past crises. Further, we recommend that new coordinating functions and mechanisms be created to execute information-sharing and communications.

We recommend that the EI-GCC—with support from other interested parties, such as the National Association of Secretaries of State (NASS), International Association of Government Officials (IGO), the U.S. Election Assistance Commission (EAC), the National Association of State Election Directors (NASED), and the National Governors Association (NGA)—establish a Cybersecurity Communications Response Group (CCRG).

This newly formed entity will provide the EI-GCC and its stakeholders with a communications coordination function that currently does not exist, allowing for collaborative, coordinated public message planning and execution if and when it is needed in the future.

Phase 1: Baseline Communications Activities

On a regular basis, the CCRG will provide updates to the public and other key stakeholders on current cyber threats and actions being taken to counter them. These baseline updates, whether part of a regular cadence or spurred by suspected nefarious activity, should be developed and coordinated with the expectation that they will be made public. Audiences and stakeholders are catalogued below with recommendations for actions that can be taken now to establish or maintain relationships with them.

Communicating with these groups on a regular basis, before something happens, is key to setting a baseline with critical audiences so that there is a level of understanding around the issue that allows mutual alignment on escalation and coordinated response. In order to provide this ongoing education, we recommend communicating early and often, in addition to when moments of interest (i.e., elections) arise. This baseline work could take the form of behind-the-scenes demonstrations and briefings for your audiences.

Stakeholders may include:

State / Local Comms. Counterparts

Law Enforcement

Federal / State Lawmakers

Media

Interested Parties

State and Local Communications Counterparts: Knowing your state and local counterparts is key to the planning and response actions discussed in later phases. The EI-GCC should maintain a "living list" of communications officials and accurate contact information, so these individuals can be reached on short notice for incident coordination and planning.

Law Enforcement: In the event of a cyber incident, federal, state, and/or local law enforcement will be involved in the response. Creating and maintaining relationships with key law enforcement officials and associated communicators in law enforcement agencies ensures more seamless coordination and information-sharing before, during, and after an incident.

Federal/State Lawmakers: Federal and state lawmakers play an important role in authorizing and overseeing election and cybersecurity measures. They also are likely to speak publicly about an election-related cyber incident, so communication with them is

critical before, during, and after an incident. Not only are lawmakers beneficiaries of a safe and secure elections system, but they have a vested interest in maintaining the public's trust in that system. Communicators should build relationships with key figures in Congress and statehouses, including their respective communications staffs, in advance.

Media: The media is a key information conduit to voters, providing news and commentary that shapes and defines public opinion and a belief in the election system's integrity. Establishing ongoing relationships with key reporters who cover both cybersecurity and election-related issues at the national, state, and local level will be important in shaping accurate coverage throughout all phases of cyber-related preparation and response. You should focus on two categories of media:

Traditional Media—Mainstream outlets and reporters;

Influencer Media—This category includes influential bloggers, outlets, and commentators, as well as outlets likely to reach them.

Interested Parties: You should develop relationships with voting advocacy and other third-party groups, because they play a role in maintaining the public's confidence in elections. Political parties an campaigns are a critical group with which you should develop a trusted relationship in advance. Third-party groups may also include vendors, researchers specializing in elections, technology service providers, or other industry service providers. We recommend as a next step that the CCRG develop an initial list of key groups, which should be maintained and updated by the team lead.
This list could include:

Political Parties and Campaigns

Election Groups

Think Tanks

Academics

Phase 2: Communications Planning, Activation, and Coordination

Cyber-related incidents rely on evolving investigations, making their scope and impact difficult to understand, particularly at the outset. This can make communications decision-making, coordination, and messaging even more important for reducing confusion.

Some incidents may be discovered as an attack or breach occurs, while most tend to be discovered after the fact—often after significant time has passed. The key to an effective response is not just coordination but also knowing with whom to coordinate. In any response, there are likely to be multiple voices speaking publicly, at both the national or field level.

In this phase, we assume an anomalous event has been identified, which activates a communications coordination scheme. It may be detected by a range of entities, such as a security researcher, state/local election official, law enforcement, or media.

When an incident occurs, many representatives from a variety of organizations will become involved. The section below outlines resources, coordination mechanisms, lines of coordination, and a checklist to be used in response to, or in advance of, a cyber-related incident.

Assembling Key Players

Note: *The U.S. Federal Government's National Response Framework outlines public information as an Emergency Support Function (ESF) and includes a framework for public information coordination and action around incidents that involve, or may involve, federal response. This process aligns with the ESF #15 Standard Operating Procedure.*

CCRG Roles & Responsibilities: The CCRG should establish the following roles for responding to a multistate cyber incident. These individual roles can be filled by specific people from a variety of interested parties, which may include, but are not limited to, NASS, NASED, IGO, EAC, and NGA.

Please note that as the EI-GCC builds on this Guide, updates should include a table with these roles assigned to individuals, along with their contact information.

Communications Director–On behalf of the EI-GCC, oversees the functional coordination resources, processes, and staff. Is responsible for overall operational direction and communications messaging development in cooperation and coordination with EI-GCC and interested parties. The communications director position can be filled by different people on a rotating basis; for example, the EI-GCC could designate a communications director to stand duty quarterly. The role should be filled by a senior communicator from the EI-GCC participants or other interested parties and have the relevant management, crisis, and media operations experience to understand not only their role but also the other roles outlined as part of the CCRG.

Affected Community Communications Representatives–Usually senior communicators from affected state or local jurisdictions representing a "field" perspective and providing relevant incident-related information to the coordination process. This may include a communicator from the governor's office and/or communicators from state and/or local elections offices.

Media Operations Director–Responsible for communication with reporters and for media monitoring on behalf of a multi-state communications coordinating body. Oversees near-term, "24-hour" communication operations, i.e., execution of communication plans.

Social Media Director–Responsible for online communications via ESCC web platforms, as well as coordination with interested parties' digital media teams in order to promote and cross-promote content.

Communication Plans Director–Responsible for forward-looking communication plans beyond the immediate "24-hour" period.

Congressional/Inter-governmental Affairs Liaison–Responsible for coordinating congressional/governmental briefings for members of Congress, state legislatures, or other elected officials with communications staff. Coordinate through the Affected Community Communications Representative, who is likely to be a member of the ESCC or interested parties' government affairs team.

Law Enforcement Affairs Liaison–Responsible for coordinating communications information with law enforcement and affiliated communicators.

Technical Liaison–Responsible for being the conduit of technical information between operational and communications teams. Ensures accuracy of technical data being released by communications team and serves as subject-matter expert for all such information.

Activation of the CCRG: The CCRG, while regularly communicating in Phase 1 during baseline operations, should plan for and exercise the activation of the CCRG in a crisis. Activation of the CCRG would be at the discretion of the Communications Director, with input from operational leads in response to a verified or potential incident. Additional information on the escalation process is in the Appendix available to election officials and can be obtained upon request from NASS, NASED, or the EAC

Generally speaking, this activation would be executed via a blast email to CCRG members with shareable background information on the incident, direction on the use of coordination mechanisms (discussed below), and next steps. For example, on discovery of a potential incident, the Communications Director would activate the CCRG by hosting an Election Sector Incident Communications Coordination Line call regarding the incident, thereby beginning the communications coordination process.

Election Sector Incident Communications Coordination Line (ESICCL): This bridge line is a standing conference call line that can be created to use for coordination before, during, or after a cyber-related incident. The CCRG will maintain a list of relevant contacts from federal, state, and local election offices in order to invite relevant parties to a call, should it be necessary. This resource does not currently exist and it would be incumbent upon the CCRG to coordinate the creation of this standing line at the outset.

Election Sector Information Center (ESIC): In the event of a multistate event, the CCRG should create a specific Information Center where communications activity is planned, coordinated, and executed real-time. This should include all the roles above and can reside in one physical location or it could be done virtually through online means. An ESIC would be the functional nerve center of all communications-related activity.

Using the Election Sector Incident Communications Coordination Line (ESICCL)

As the standing conference call line for election sector cyber-related incidents, the ESICCL can be a key coordination mechanism for communicators to share both operational data, as well as coordinate messaging and communications-related activity.

Upon the activation of the CCRG, the Communications Director will stand up the ESICCL and distribute the time and conference line to invited participants for an initial conference call. This call could include representatives from affected communities, as well as the CCRG roles listed above and any other CCRG participants or outside advisors with relevant subject-matter expertise.

The call agenda can follow a regular rhythm:

- Roll call
- Opening remarks by Communications Director for CCRG
- Brief operations summary (on-scene reps or operations)
- Summary of major communications plans and events
- Invitee comments
- Messaging coordination requirements outlined by EI-GCC Representative
- Conclusion and next steps

Standing up the ESIC

Should an event rise to the level where ongoing, real-time coordinated public information flow is necessary, the CRCG could stand up either an in-person or virtual ESIC where personnel could work together.

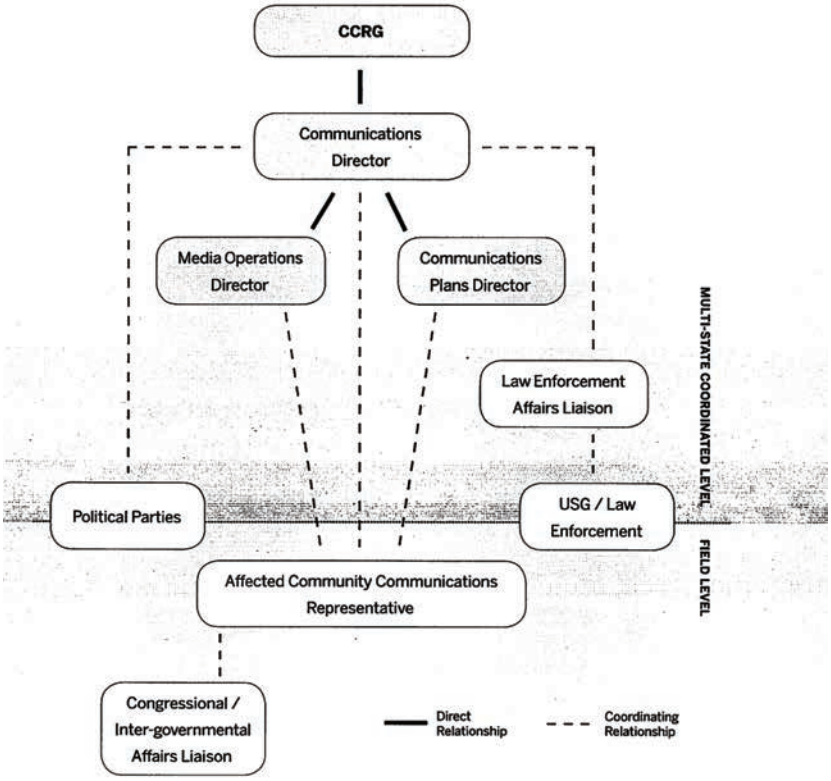
The ESIC would be stood up by the Communications Director, who would make a determination as to the critical personnel needed, as well as the location/online.

The CRCG, as part of steady-state planning, should identify both likely and convenient physical locations where an ESIC could reside should it be needed, as well as functional online collaboration tools to use in the event of a remote ESIC. In general, it is advisable to co-locate the ESIC with any space that is being used to coordinate operational response activity.

Current Coordination Processes

Should there be current coordination processes that are effective in sharing information, such as regular calls or email listservs, continue to use them—particularly prior to, or during the beginning phases of, activation. However, the scope and volume of an incident may make more direct communications, such as via the ESICCL or ESIC, more useful.

Lines of Coordination

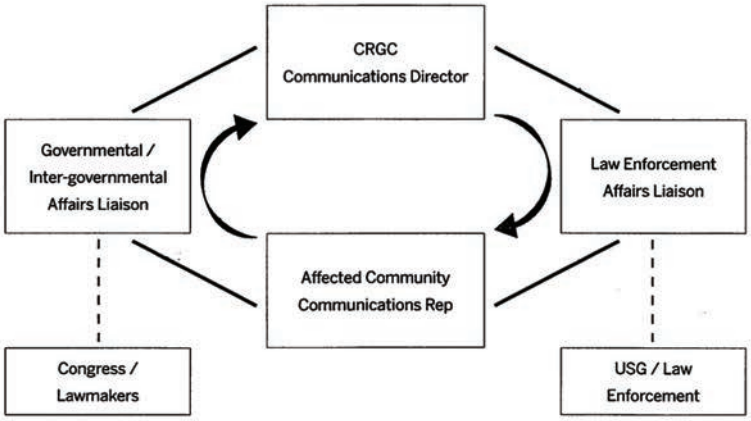


Phase 3: Message/Document Drafting, Coordination, and Distribution

Message/Document Drafting and Coordination

It is best to have some communications materials ahead of time; however, every incident is different and depends on a range of factors, so communicators will oftentimes have to adapt on the fly.

Messaging will need to be adapted, drafted, coordinated, and distributed quickly in order to effectively respond. In addition to the coordination resources, mechanisms, and processes described above, the diagram below shows how that loop may work practically, in and among the various parties who will be speaking publicly.

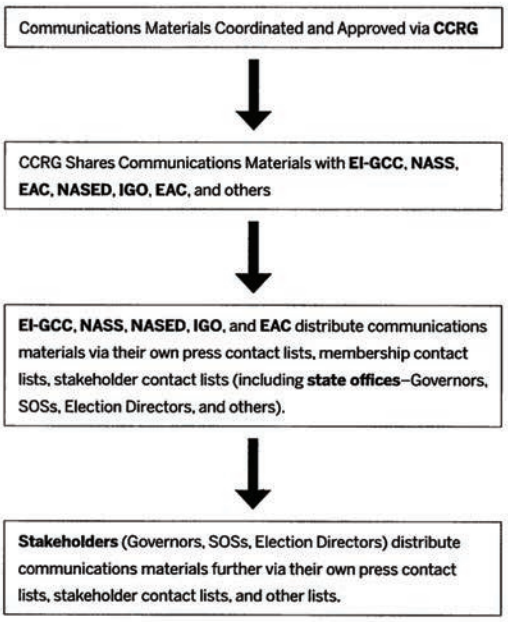


The CCRG staff will not necessarily retain authority to approve messages emanating from affected communities' communications staffs, nor vice versa; however, the CCRG staff can provide message guidance when needed or warranted. In addition, key inputs should be sought from Congressional/Inter-governmental Affairs and Law Enforcement Liaisons, and approval authority can be retained by those communicators with whom these liaisons work at their home agencies or organizations.

Distribution

Distribution of approved communications materials to the public and other stakeholders should leverage, and mirror, existing processes to the degree possible. The CCRG, by virtue of its makeup, with communications professionals from a variety of relevant organizations, should coordinate the messaging, but largely leave distribution to the organizational members.

A sample distribution process is illustrated below:



Phase 4: Evaluation and Feedback

Incorporating both real-time evaluation and feedback, as well as post-incident after-action reviews into your response is critical to both the response you are currently managing, and capturing lessons learned for the future.

Real-Time Evaluation

While capabilities and resources may differ greatly among affected communities, the CCRG could augment these by providing services that can assist the holistic communications response, including:

Media Monitoring–It is critical to understand how the media tone is shaping up. Media monitoring should be compiled at least daily, providing insight on tone and volume and identifying areas for further concentration or strategic/tactical communications changes.

Social Media Analysis–Similar to traditional media monitoring, social media listening tools and analysis can provide key insight into which messengers are driving conversation about the incident, as well as how voters are reacting to news and sharing information.

Call Center Analysis–If the affected community has a voter call center, it is important to track and analyze the questions and comments received. This information can be a key indicator of misinformation or provide insight into where efforts need to be expanded to get accurate information to voters.

Polling/Public Opinion Research–In order to gain more in-depth insights, polling or public opinion research can do much in terms of uncovering voter reactions to an election-related cyber incident, helping shape near and longer-term strategy.

After-Action Review and Report

Once an incident has concluded, it is important to review communications-related activities, discuss what worked and didn't work, and document those lessons to be incorporated into both steady-state and crisis planning.

Many of the coordination resources and mechanisms described above can be adapted for this purpose, for example the ESICCL call. The after-action process should analyze the incident from start to finish, examining the Plan-Prepare-Respond-Recover communications lifecycle of that incident.

Your after-action report should include:

A summary of the incident;

an overview of the operational response;

the communications objectives;

and by phase, with specificity:

- concern
- outcome
- recommendations

This after-action process will assist in building your communications response capability and coordination in a resilient process that can be more effectively utilized when facing future incidents.

Communications Coordination and Response Checklist

This checklist will help guide actions prior to, and through, the first several days of a multi-state election-related cyber incident.

There are five lists:

- **Before a cyber crisis**
- **Before a cyber crisis becomes public**
- **Multistate Election-Related Cyber Incident Assessment & Activation**
- **Coordination/Communications Outreach**
- **Products**

Before a cyber crisis

- ☐ Identify office protocol and a crisis communications team. (Should include IT).
- ☐ Create a list of terms with common nomenclature for use by all stakeholders.
- ☐ Set an internal communication plan with elections staff. (How often, when, and where will all staff meet? Information must travel up and down the chain of command with clear boundaries for disseminating information and interfacing with the public/media.)
- ☐ Ensure that all stakeholders can be reached in a crisis without access to networks or smart phones.
- ☐ Craft communications materials that can be used in a potential cyber incident. (For examples, elections officials may request sample materials from NASS, NASED, or the EAC.)
- ☐ Ensure that staff understand their role in a cyber incident. For those who do not have a specific role, ensure they understand why their work matters to the outside world and how they can continue doing their jobs while designated managers handle the cyber incident.
- ☐ Ensure that communications plans can be accessed and are regularly updated.

Before a cyber crisis becomes public

- ☐ Obtain technical briefing. (Assess and verify all information.)
- ☐ Decide whether to activate CCRG.
- ☐ Decide whether website can remain online. If you must disable it, launch a microsite (hosted on a different network) in its place.
- ☐ If email is potentially compromised, use an outside communications channel.
- ☐ Consult authorities, if needed.
- ☐ Meet internally in war room; set internal communication schedule.
- ☐ Determine CCRG roles and responsibilities, if you have not done so already.
- ☐ Assess stakeholders.
- ☐ Determine broad communications strategy.
- ☐ Prepare holding statement.
- ☐ Develop communications plan.
- ☐ Draft additional communications required to execute plan, including a communications rollout plan (includes communication with media, stakeholders, and employees).
- ☐ Establish plan for traditional and social media monitoring.
- ☐ Establish media response protocol.
- ☐ Notify affected employees, if necessary. It may be that only a small group of employees are informed initially. Communicate internally, as needed.
- ☐ Notify stakeholders (See list on reverse page), if appropriate, and galvanize support.

Multistate Election-Related Cyber Incident Assessment & Activation

- ☐ Notification to, and activation by CRCG, of a cyber-related incident or threat.
- ☐ Situation Assessment/Escalation.
  - ☐ **High-Intensity Incident**: Cyber-related incident that triggers reporting obligations, or one that is highly visible requiring response.
  - ☐ **Medium-Intensity Incident**: Cyber-related incident resulting in the loss or compromise of the data or systems, but no formal reporting obligations are triggered. There may be some awareness of the incident, however, spurring proactive communication.
  - ☐ **Low-Intensity Incident**: Cyber-related incident resulting in minor disruptions that may not be visible to public.
- ☐ If Major or Moderate, Media Operations Director and Communication Plans Director identified by Communications Director.
- ☐ Additional Relevant Personnel identified.
- ☐ Contact information for Relevant Personnel distributed.
- ☐ CRCG designates spokesperson, if applicable.
- ☐ Depending on assessment of situation, key messages determined based on specific scenario.

Coordination/Communications Outreach

- ☐ Communications Director activates ESICCL call.
- ☐ Incident Overview.
- ☐ Affected Communities Communications Representative Update.
- ☐ Initial Response Communications Plan.
  - ☐ Designate spokesperson based on type of incident, geography(ies) affected, and scope. In a Major Incident, the spokesperson role may include several people including a EI-GCC representative as well as an Affected Community spokesperson as well to share information at both a field and national level. In a Minor Incident, a single spokesperson may suffice, i.e. an Affected Community spokesperson.
  - ☐ Prep designated spokesperson for media engagement. This includes review of relevant facts and messaging as well as a peer review session, known as a "murder-board."
- ☐ Congressional/Inter-governmental Affairs Update.
- ☐ Congressional/Inter-governmental Affairs activity and plans.
- ☐ Law Enforcement Liaison Update.
- ☐ Law Enforcement Liaison activity and plans.
- ☐ Messaging Coordination outlined by Communications Director.
- ☐ Battle Rhythm (Daily Schedule).
- ☐ Conclusion & Next Steps.
- ☐ Communications Distribution & Rollout.
- ☐ ESIC activation, if necessary.

Products

- ☐ Staffing Plan with updates for Communications Director.
- ☐ Battle Rhythm (Daily Schedule).
- ☐ Staffing Matrix and Organization Chart.
- ☐ Communications Plan.
- ☐ Advisories.
- ☐ Press Releases.
- ☐ Traditional and Social Media Monitoring Reports.
- ☐ Regular/Daily update on response activities.
- ☐ Blog and Social Listening Updates.
- ☐ Talking Points.
- ☐ Website updates.
- ☐ Congressional/Inter-governmental Advisories, fact sheets, operations reports and briefing materials.
- ☐ Daily Communication Summary to include next day activity plans.

Conclusion

As we head into the next election cycle, we hope that this Guide provides additional tools to help the EI-GCC, and by extension election officials across the country, prepare for, and manage, this emerging and evolving cyber risk. As with all communications plans, we recommend that this one be regularly updated by the EI-GCC, as the council further develops and defines its role.

More information is available on different types of communications materials for responding to a cyber incident. Election officials seeking examples of these additional materials can request the communications materials appendix to this document from NASS, NASED, or the EAC.

Do you see a way to make this Playbook better?

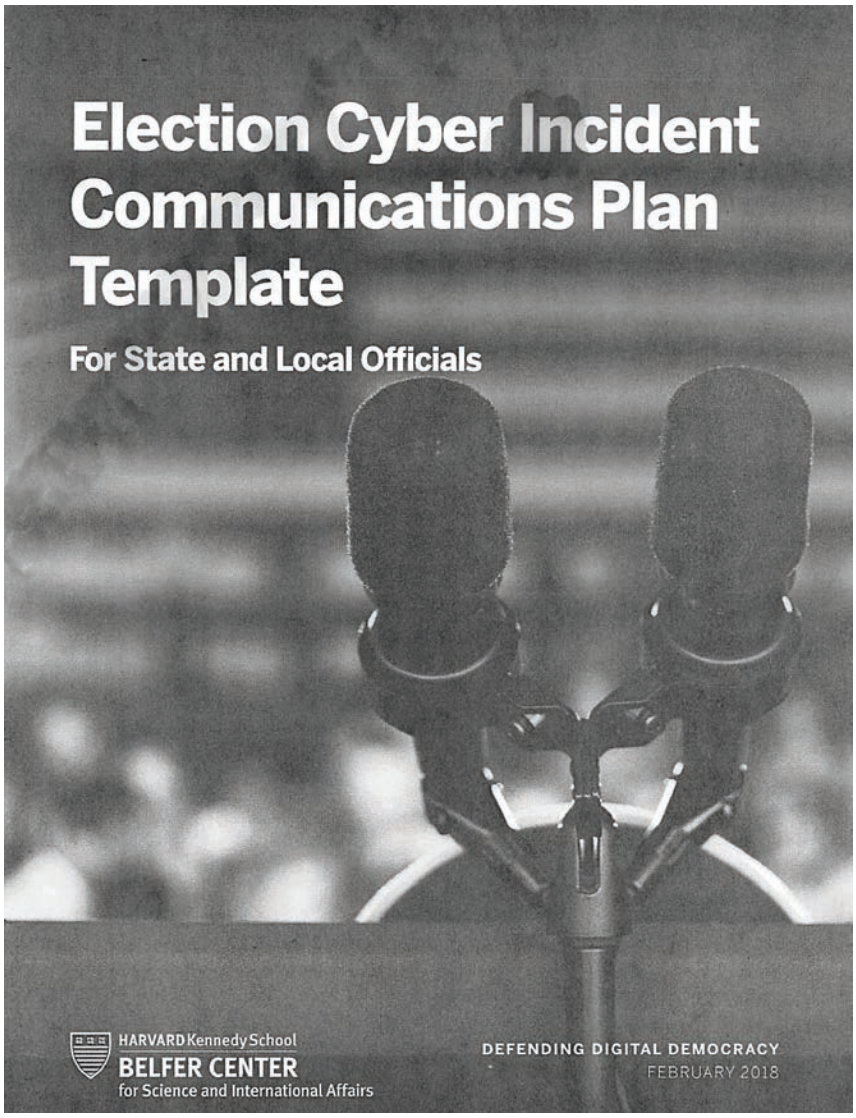
Are there new technologies or vulnerabilities we should address?

We want your feedback.

Please share your ideas, stories, and comments on Twitter @d3p using the hashtag #electionplaybook or email us at connect@d3p.org so we can continue to improve this resource as the digital environment changes.

Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 John F. Kennedy Street
Cambridge, MA 02138

www.belfercenter.org/D3P


Election Cyber Incident Communications Plan Template
For State and Local Officials
HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs
DEFENDING DIGITAL DEMOCRACY
FEBRUARY 2018

Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/D3P

Design & Layout by Andrew Facini

Cover photo: Microphones sit on a podium following Vice President Mike Pence's speech at an event at Dobbins Air Reserve Base in Marietta, Ga., Friday, June 9, 2017. (AP Photo/David Goldman)

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DEFENDING DIGITAL DEMOCRACY
FEBRUARY 2018

Election Cyber Incident Communications Plan Template

For State and Local Officials

Contents

Defending Digital Democracy: About Us

We established the Defending Digital Democracy Project (D3P) in July 2017 with one goal: to help secure democratic elections against cybersecurity threats and information operations.

There are two groups on the frontlines of defending democracy: (1) political campaigns, which enable citizens to pursue elected office; and (2) election officials, who ensure the election process is free and fair.

Last year, we set out to provide campaign and election professionals with practical guides to the most applicable cybersecurity best practices in advance of the 2018 midterm elections. In November 2017, we released "The Campaign Cybersecurity Playbook" for campaign professionals.

Now, we are releasing a set of three playbooks designed to be used together by election administrators: **"The State and Local Election Cybersecurity Playbook," "The Election Cyber Incident Communications Coordination Guide,"** and **"The Election Incident Communications Plan Template."** What follows is the Communications Plan Template.

D3P is a bipartisan team of cybersecurity and policy experts from the public and private sectors. To better understand the cyber threat and other challenges that election administrators face, our team spent four months interviewing state officials about their communications practices and how they would or would not apply in a cyber incident. We spoke with state and local election officials, as well as key national-level players and members of the Election Infrastructure Government Coordinating Council (EI-GCC).

These interviews exposed the range of challenges election officials confront in the cyber domain. One of the most significant needs we encountered was state and local officials' request for guidance on how to communicate in a cyber crisis, because they saw cybersecurity issues as unfamiliar territory. They asked specifically for help with developing a communications plan for a potential cyber incident in their jurisdiction.

This Plan Template document is primarily intended for use by state and local election officials as a basis for developing their own communications response plans, which include best practices for use in an election cyber incident. We are releasing the Template publicly, because election officials are among those best prepared and always looking for industry best practices, as well as practical checklists. This template will aid in that effort.

We hope this Plan Template becomes a starting point for state and local election officials to prepare for an election cyber incident.

Finally, we would like to thank the election officials around the country for whom we wrote this guide. You are the frontline defenders of democracy. We hope this effort helps make that tremendous responsibility a little easier.

Good luck,
The D3P Team

Authors and Contributors

This project was made possible by dozens of people who generously volunteered their time. Special thanks are due to **Siobhan Gorman**, who led the project and who, in addition to **Shannon Cortez**, wrote this plan.

We are also indebted to the people listed below who invested countless hours in reviewing drafts and providing input.

SENIOR ADVISORY GROUP

Eric Rosenbach, Co-Director, Belfer Center; Director, Defending Digital Democracy Project

Robby Mook, Co-Director, D3P

Matt Rhoades, Co-Director, D3P

Heather Adkins, Dir. of Information Security and Privacy, Google

Dmitri Alperovitch, Co-Founder and CTO, CrowdStrike

Siobhan Gorman, Director, Brunswick Group

Yasmin Green, Head of Research & Development, Jigsaw (Alphabet)

Stuart Holliday, CEO, Meridian International Center

Kent Lucken, Managing Director, Citibank

Debora Plunkett, former Director of Information Assurance, National Security Agency

Colin Reed, Senior Vice President, Definers Public Affairs

Suzanne Spaulding, Senior Advisor for Homeland Security, Center for Strategic and International Studies

Alex Stamos, Chief Security Officer, Facebook

CONTRIBUTORS

Lori Augino, Director of Elections, WA Office of the Sec. of State

Matt Chandler, Partner, Frontier Solutions

Caitlin Conley, Executive Director, D3P

Amy Cohen, Executive Director, National Association of State Election Directors

Shannon Cortez, Deputy Director of Elections, WA Office of the Secretary of State

Meredith Davis Tavera, D3P, Harvard Kennedy School

Karen Ejiofor, Staff Assistant, Belfer Center

Chris Farley, Associate, Albright Stonebridge Group

David Forsey, Policy Analyst, National Governors Association

Siobhan Gorman, Director, Brunswick Group

Eben Kaplan, Principal Consultant, CrowdStrike

Jane Khodos, Senior Director, Communications and Content, FS-ISAC

Matthew Masterson, Commissioner, Election Assistance Commission

Jeff McLeod, Division Director for Homeland Security and Public Safety, National Governors Association

Michelle Tassinari, Director/Legal Counsel, Elections Division, Office of the Secretary of the Commonwealth of Massachusetts

BELFER CENTER WEB & DESIGN TEAM

Arielle Dworkin, Digital Communications Manager, Belfer Center

Andrew Facini, Publications and Design Coordinator, Belfer Center

Acknowledgments

The D3P team would like to especially thank Heather Adkins of **Google**, Yasmin Green of **Jigsaw**, the **Hewlett Foundation**, the **Democracy Fund**, and the **Belfer Family**; without whom this Playbook would not have been possible. Additionally, we would like to thank the following organizations and offices for sharing their time with us through conversations, simulation participation, or field visits. Your perspectives were critical in shaping our approach to this document.

Department of Homeland Security (DHS)
National Association of State Election Directors (NASED)
National Association of Secretaries of State (NASS)
National Governors Association (NGA)
National Guard Bureau (NGB)

Election Officials from the Following States and Jurisdictions:

Atlantic County, New Jersey
Nevada County, California
Orange County, California
Santa Clara County, California
State of Colorado
Arapahoe County, Colorado
City and County of Denver, Colorado
State of Connecticut
Escambia County, Florida
Cook County, Illinois
State of Louisiana
State of Maryland
Caroline County, Maryland
Commonwealth of Massachusetts
State of Minnesota
State of Nevada
Clark County, Nevada
State of New Jersey
Mercer County, New Jersey
State of North Carolina
State of Ohio
State of Oregon
Multnomah County, Oregon
Commonwealth of Pennsylvania
State of Rhode Island
State of Tennessee
State of Vermont
Commonwealth of Virginia
State of West Virginia
Harrison County, West Virginia
State of Washington
State of Wisconsin

Executive Summary and Purpose

A cyber incident can span a wide spectrum of malicious cyber activity, and for the elections system, it could range from theft of voter registration data to disruption or manipulation of the vote tally. Given the growing cyber threats to elections globally and in the U.S., state and local elections officials are preparing for how to respond in a "cyber incident" on all fronts, including external communications.

To prepare for possible incidents, election officials have requested guidance on how to build their own communications plan for election-related cybersecurity incidents. This document provides a template and guidance to do so.

The potential for cyberattacks on our election system is an unfortunate reality of our time, and officials should recognize, and plan for, a possible incident. There has been growing interest in using cyber means to spy on or disrupt U.S. elections, dating back at least to 2008 and culminating in the high-profile cyber incidents in 2016.

That trend has rightly caused concern for state and local election officials administering and overseeing elections for all levels of government. In future cycles, the efforts to compromise elections may extend to state and local races. Every relevant agency, as part of their overall security strategy, should incorporate a cyber crisis communication plan.

When a cyber incident occurs, elections officials should be generally prepared to manage the crisis, because they have prepared ahead of time for other types of crises, such as a natural disaster. However, there are elements of a cyber incident that require additional preparation, because a cyber crisis is different from other situations in key ways:

> **High Degree of Uncertainty:** You will know very few facts when you first have to communicate about an incident, and you will need to demonstrate you are confidently and competently managing the incident with relatively little information.
>
> **Well-Sourced Journalism:** The journalists covering the cyber beat know technical and policy issues and are well sourced, so they may learn about details before you do.
>
> **Cross-Functional Impact:** Cyber incidents require coordination across a range of state agencies that may not normally work together.

Cross-Boundary Implications: Cyber incidents targeting elections systems can have effects that cascade across traditional jurisdictional boundaries.

Potential to Undermine Trust: A cyber incident has the potential to undermine public trust in the U.S. election system, so communicating in a way that avoids creating undue alarm is critical.

The Plan Template that follows outlines key components of a communications plan that state election officials can build out and tailor to the needs of their jurisdiction. It can also be used at the local level, particularly for large counties. This Plan Template is designed to be used in concert with the State and Local Election Cybersecurity Playbook and the Election Cyber Incident Communications Coordination Guide.

The sections that follow are suggestions only and should be retained, amended, or deleted based on the needs of your jurisdiction. The pages that follow will be in a template format, including bracketed text where the name of a jurisdiction, or other jurisdiction or situation-specific details, can be filled in. The template starts with the first component of a plan: how to use this communications plan. It then outlines best practices and key communications processes. An Appendix of additional communications materials is available to elections officials upon request from the National Association of Secretaries of State, the National Association of State Election Directors, or the U.S. Election Assistance Commission.

How to Use this Communications Plan

[STATE / LOCAL JURISDICTION'S] communications plan includes guidelines and template materials to help our election officials respond to an election-related cyber incident quickly and in a coordinated fashion during the first several days of a cybersecurity incident.

While every situation is unique, this plan provides a foundation on which election officials can build an appropriate response that addresses the incident with the goal of maintaining confidence in the election system.

This plan should be owned by one organization and updated at least annually.

Key components include:

Cyber Incident Best Practices: This section includes best practices for communicating with the media and other key stakeholders.

Communications Process Workflow: This component includes diagrams that outline who will manage crisis response, serve as spokesperson, and manage day-to-day crisis communications during an incident.

Response Checklist: This checklist broadly outlines steps that should be taken during the first several days after learning about a potential incident.

Establishing Baseline Communications: It is important to integrate cybersecurity into your jurisdiction's ongoing communication and set a public baseline understanding of the steps your jurisdiction it taking to mitigate exposure to cyber incidents. This section provides an example.

Scenario Planning and Materials: This section will include communications materials that could be used in different scenarios. [Additional scenario-planning materials are available to election officials and can be obtained upon request from the National Association of Secretaries of State, the National Association of State Election Directors, or the U.S. Election Assistance Commission.]

Cyber Crisis Communications Best Practices

The top priority in a cyber crisis will be to maintain public trust. The most effective way to achieve that goal is to respond confidently and quickly.

To lead confidently, election officials need to prepare, train for, and test responses ahead of time. In today's dynamic political and data environment, every official will likely have to respond to a cyber challenge at some point. Whether preparing for a cyber incident or another type of crisis, this plan can assist the state or local election official will develop a well-thought-out plan and response. That response will be central to preserving public trust.

Communications Coordination

Set guidelines for communicating with outside parties in an incident.

Elections officials should create a communications plan that provides escalation thresholds for reporting an incident internally and publicly. The guidelines should address who is responsible for communicating to key external stakeholders, such as the media and law enforcement. It should also spell out the timeframe for these communications and key individuals involved in communications response from the incident response team, such as public affairs, legal, and agency management.

Guidance on escalation decision processes is available Additional communications response materials are available to election officials in the Appendix and can be obtained upon request from the National Association of Secretaries of State, the National Association of State Election Directors, or the U.S. Election Assistance Commission.

Establish connections between the incident response team and communications officers.

Every situation will require collaboration and cooperation of multiple team members and groups. The relationships between, and credibility of, each player is vital to a successful post-incident recovery.

Encourage intra-state, cross-state, or cross-country communication and collaboration.

Key organizations to designate for regular communications include: Election Infrastructure Government Coordinating Council, the National Association of Secretaries of State, the U.S. Election Assistance Commission, the National Association of State Election Directors, the National Governors Association, the Department of Homeland Security, the Federal Bureau of Investigation, and other national organizations. Develop good working relationships between state and county registrars, clerks, and/or auditors.

Planning Ahead

Near-term Planning	Longer-term Planning
• **Determine internal roles and responsibilities.** Make sure there is a clear escalation process within `[JURISDICTION ELECTION AGENCY]` and the right teams are talking to one another in the event of a cyber incident. Designate an individual to be responsible for ensuring that this process is established and updated. • **Assess the current crisis communications plan** and analyze communications gaps and weaknesses. • **Plan your response to a cyber crisis in advance** with a communications plan, including a decision-making protocol and communications materials. • **Ensure cyber-incident response is part of the operational continuity plan.** Make sure there is a backup communications plan and system in place.	• **Conduct crisis simulation and table-top exercises,** coordinated with legal, technical, and outside advisors, including key senior leaders across `[JURISDICTION]`. Also consider a multistate drill, including officials from multiple states, counties, coordinated bodies and the federal government. • **Conduct stakeholder mapping and a reputational risk analysis** to understand your cyber risks, priority stakeholders, and how to reach them to address key concerns. • **Educate the media** through background meetings and public events on the resiliency of the election system, and the current work to mitigate cyber threats. • **Educate the public** through online channels and public events on the resiliency of the election system and the current work to mitigate cyber threats.

Communications Response

Best Practices

Be transparent but careful. Transparent communication builds trust, but in a cyber incident you will have few facts at hand, especially at the outset. Public comments should demonstrate that you are taking the issue seriously, but avoid providing any details that may change as the investigation progresses, so you don't have to correct yourself down the line. Avoid speculation on the perpetrator of the incident.

Coordinate with the Governor's Office beforehand and agree on if/how the Governor's Office should be involved or not. Election officials who want governors to remain silent in a cyber incident should seek agreement from the governor early on.

Focus on actions you are taking to address the issue. To demonstrate that you are taking the issue seriously, you should talk about the steps you are taking to protect voter information and address any broader risks to the system.

Provide context. In an election-system cyber incident, there will be a temptation for public speculation. Counter speculation with facts and context to reduce the risk of undermining public trust. Include metrics whenever possible.

Be visual. Cybersecurity can be challenging to understand depending on a person's technical background. The quickest way to get your message out is to pair it with a graphic. Connect with design teams who can provide you infographics and develop a library of graphics and photos you can draw from.

Use the right digital tools. Use social media to dispel rumors. When a cyber incident strikes, social media is now a go-to source of immediate information. In practice, this means using it selectively to counter misinformation andinaccuracies.

Learn from the incident. Use your and others' experiences to improve your cybersecurity practices and crisis plans. Conduct an after-action briefing to evaluate the response and suggest improvements.

Guidelines for Communicating with the Public

Make your communications about your most important stakeholder—the public. There will be a temptation to discuss the components of the incident. Instead, talk about what you are doing to address public needs or concerns in this specific situation.

Speak plainly. Cybersecurity can be off-putting to nontechnical audiences. Use anecdotes and examples to demystify relevant issues whenever possible.

Demonstrate transparency by communicating with the public on a regular basis. Establish a regular series of communications with the media and the public about the cybersecurity measures you are taking now, so that the first time they hear from you is not in a crisis.

Best Practices for Countering Misinformation

Establish the facts, and double-check them. You need to ensure you are operating from a factual position before countering misinformation, so check your facts with multiple sources before citing them publicly. Ask all appropriate questions and put in the work before you speak to ensure that you do not accidentally provide misleading information.

Develop a simple, accurate, short counter-message. Develop a clear statement that contains only the facts. Avoid complex messages. You can provide additional nuance later.

Respond quickly. Misinformation can spread rapidly through social media and broadcast commentary. Your counter-message should be ready to disseminate as soon as possible.

Be transparent. Caveated, incomplete, or "no comment" responses can fuel conspiracy theories by making it appear your organization has something to hide. Demonstrating transparency can help counter false claims. Opportunities to demonstrate transparency could include inviting reporters "behind the scenes" at a polling place.

Engage on all platforms. Misinformation can spread across multiple platforms, including social media and traditional media. To counter misinformation, deliver a clear, factual message on all available platforms.

Avoid repeating misinformation. Focus on providing the accurate facts and do not repeat the false messages. For example, if rumors circulate that lines at the polls are hours long, avoid saying that rumors of long lines are circulating. Instead, your message should be that lines are short and moving quickly.

State Election Communications Development & Approval Process

Even a rumor of online election meddling can trigger a communications crisis and sow distrust in the elections system. The good news is that much can be done ahead of time to prepare for such a crisis and get everyone on the same page. We cannot stress enough how much time this will save later in trying to determine how to respond.

Maintaining a coordinated process establishes effective and efficient communications planning and response to a cyber-related incident.

The communications process outlines:

Establishing a Cyber Incident Response Team (CIRT)

Establishing a Cyber Communications Response Team (CCRT)

Phased planning and response

Coordination functions

Feedback loop to incorporate lessons learned

Establishing a Cyber Incident Response Team

To manage a cyber incident effectively, the overall state response to the incident should integrate communications officials into the process. The following organizational structure will ensure that communications is part of the decision-making process.

Cyber Incident Response Team (CIRT) Organization

Cyber incident response should use, to the degree possible, the processes `[JURISDICTION]` already has to respond to other elections-related crises. It should make adjustments for the specific differences involving cyber meddling—particularly the key personnel involved and the potential for any incident to become high profile and raise questions about the integrity of the elections process as a whole.

The Chief Election Official and Director of Elections are responsible for consulting and activating `[JURISDICTION'S]` cyber incident response plan. You should have delegated executives who are backups and can decide whether to activate the plan. Each executive should have the necessary contact information and follow that sequence.

States may be able to suspend, delay, or postpone voting in an emergency situation, which may include a court order, legislative action, or the emergency powers of the Governor. At the local or regional level, lower courts may cancel, postpone, or extend Election Day polling place hours by issuing a court order.

`[INSERT HERE JURISDICTION'S POSITION ON OPTIONS THAT APPLY IN THE EVENT THAT A CYBER INCIDENT DISRUPTS THE ELECTION PROCESS OR OUTCOME IN YOUR JURISDICTION.]`

This table should be updated regularly as part of the annual plan review.

[Note: the table below represents a starting point and should be adapted to your organizational structure.]

Position	Designated Individual and Contact Information	Designated Backup and Contact Information
Chief Election Official		
Director of Elections		
Communications Director		
Chief Financial Officer		
Chief Information Officer		
Director of Operations and IT		
Human Resources Manager		
Government & Community Relations Director		
Attorney General		

Establishing a Cyber Communications Response Team (CCRT)

Your Cyber Communications Response Team will support your [Director of Communications] assigned to the CIRT. Here are the steps you can take to ensure your Cyber Communications Response Team has the right people at the table.

Note: The U.S. Federal Government's National Response Framework outlines public information as an Emergency Support Function (ESF) and includes a framework for public information coordination and action around incidents that involve, or may involve, federal response. This process aligns with the ESF #15 Standard Operating Procedure.

`[JURISDICTION]` should establish the following roles for responding to a state-level cyber incident:

Note: Counties should adapt accordingly for their structure. Depending on a jurisdiction's organizational structure, you may choose not to include the Chief Election Official, Director of Elections, and Chief Information Officer on the Cyber Communications Response Team.

Chief Election Official—Responsible for coordinating communications information with local elected officials and administrators in `[JURISDICTION]`.

Director of Elections—Responsible for coordinating communication information with local elected officials and administrators in `[JURISDICTION]`.

Jurisdiction Local IT Director/CIO—Responsible for the `[JURISDICTION]` IT systems and the security of the systems.

Communications Director—Oversees the functional coordination resources, processes, and staff for communications in `[JURISDICTION]`. Is responsible for overall operational direction and communications messaging development in cooperation and coordination with key internal and external stakeholders.

Affected Local Elections Administrators—Usually local auditors / clerks or other officials from affected local jurisdictions representing a "field" perspective and providing relevant incident-related information to the coordination process.

Media Operations Director—Responsible for communication with media and media monitoring on behalf of national-level communications coordinating body. Oversees near-term "24-hour" communication operations, i.e., execution of communication plans.

Communication Plans Director—Responsible for forward-looking communication plans beyond the immediate "24-hour" period.

Legislative/Inter-Governmental Affairs Liaison—Responsible for coordinating governmental briefings for members of state legislatures, county commissioners or other elected officials. Coordinate through the Communications Director.

Law Enforcement Affairs Liaison—Responsible for coordinating communications information with law enforcement and affiliated communicators.

Technical Liaison—Responsible for being the conduit of technical information between operational and communications teams. Ensures accuracy of technical data being released by communications team and serves as subject-matter expert for all such information.

Cyber Communications Response Team List

Position	Designated Individual	Designated Backup
[Chief Election Official]		
[Director of Elections]		
[Jurisdiction IT Director/CIO]		
Communications Director		
Affected County Elections Administrators		
Media Operations Director		
Communications Plans Director		
State Homeland Security Advisor		
Legislative/Inter-governmental Affairs Liaison		
Technical Liaison		

Incident Communications Coordination Line (ICCL): This bridge line is a standing conference call line that can be created for coordination before, during, or after a cyber-related incident. The Communications Response Team will maintain a list of relevant contacts from federal, state, and local election offices (and officers) to invite relevant parties to a call, should it be necessary.

`[JURISDICTION SHOULD INSERT BRIDGE LINE DETAILS HERE]`

Developing a Response Process

The following steps will guide you as you start up a Cyber Communications Response Team and develop a process for drafting and approving messages.

Step 1: Decide on team. Select the individuals who will fill the roles previously listed. Outline their roles and identify the decisions around messaging and communication that they can make in real time.

Step 2: Security alignment. With your IT or security team, take inventory of your data assets and potential risks, and conduct an impact assessment. You should understand the attacks to which you are most vulnerable. You should also understand how security tactics are tied to the way your elections office manages risk. Your IT team's early monitoring and detection functions should be aligned to the agency's most critical assets, such as elections results servers. Establish who will be the liaison on the IT team to the CCRT.

Step 3: Disclosure alignment. Determine and document exactly what you are obligated to disclose. Develop a decision-making process to assess the public posture—proactive or reactive—you will take in a given situation. Take into account both legal implications and public opinion.

Step 4: Stakeholder analysis. Assess and prioritize your key stakeholders, based on their influence on voters, because public opinion can turn very quickly during a cybersecurity crisis. Establish ongoing relationships with these stakeholders BEFORE a crisis hits. Your stakeholders may include:

Voters

Federal, state, and local elections communications counterparts

Law enforcement

State and federal lawmakers, including the Governor's Office

Media (cybersecurity and election/political beat reporters)

Political parties and campaigns

Third-Party advocacy groups

Step 5: Select a spokesperson or spokespeople. Establish ahead of time who will speak for `[JURISDICTION]` in a cyber incident, and make sure that they have received media training. You may choose different spokespeople for different audiences. Your head of IT might be best equipped to post a response on a vendor site or address hardware concerns, while the Chief Election Official, the director of elections, or your Chief Information Security Officer or Public Information Officer might be the best person to speak to the media. Consider factors such as who has the best communication skills, prior experience with the media, authority in the agency, and relationships with stakeholders.

Step 6: Establish a drafting and approval process for key messages and include diagrams of this process in your communications plan. This process will be specific to `[JURISDICTION'S]` Cyber Communications Response Team structure but will likely follow this basic outline, tailored to your organizational structure:

Step 7: Decide what baseline information you can communicate now. Establish a baseline understanding among key stakeholders of `[STATE's]` work to implement cybersecurity best practices well ahead of the next election. In the event of a cyber incident, this effort will position `[STATE]` to make the case that `[STATE]` has been implementing best practices, but unfortunately cyber incidents do still sometimes occur.

Step 8: Establish a feedback loop. Establish a means—both during and after an incident—to incorporate feedback from voters and other key stakeholders into your response. During an incident, this work could take the form of media and social media monitoring as well as polling. After an incident, you should conduct an after-action report and ensure that lessons learned are incorporated into this Cyber Communications Plan Template Your after-action report should include:

A summary of the incident (keeping in mind it could be subject to public disclosure);

an overview of the operational response;

the communications objectives;

and by phase, with specificity:

- concern
- outcome
- recommendations

Activation of the Cyber Communications Response Team (CCRT)

Cyber-related incidents vary in size and severity, which makes it important to have a process to ensure the appropriate steps are calibrated to the significance of the incident. All incidents can be categorized under one of the following severity levels:

1. **Low**: Cyber incident that involves no PII and/or minor system disruptions that will likely not be visible to the public or affect the elections process.
2. **Medium**: Cyber incident resulting in the loss or compromise of voter data or VR systems, but formal notification obligations may not be triggered. The issue begins to become public.
3. **High**: Cyber incident that triggers U.S. or international reporting obligations, affects a large amount of voter information, and/or is destructive to election operations.

In a medium-intensity incident, `[CHIEF ELECTION OFFICIAL]` will need to make a judgment call about whether to activate the CCRT, but if the incident is likely to become public and raise questions about trust in the election systems, `[CHIEF ELECTION OFFICIAL]` should err on the side of activation. You can always deactivate if the intensity declines. Once activated, `[CHIEF ELECTION OFFICIAL]` along with `[DIRECTOR OF ELECTIONS]`, will decide which level applies, based on an initial assessment. Once `[CHIEF ELECTION OFFICIAL]` activates the CCRT, all key response team members will be notified of the activation `[INSERT STATE'S METHOD OF REACHING TEAM MEMBERS]`.

Coordination Mechanisms

Using the Incident Communications Coordination Line (ICCL)

As the standing conference call line for cyber-related incidents, the ICCL can be a key coordination mechanism for communicators to share both operational data, as well as coordinate messaging and communications-related activity.

Upon activation of the Cyber Communications Response Team, the `[COMMUNICATIONS DIRECTOR]` will stand up the ICCL and distribute the time and conference line to invited participants for an initial conference call. This call could include representatives from affected communities, as well as the CCRT roles listed above and any other CCRT participants or outside advisors with relevant subject-matter expertise.

The call agenda can follow a regular rhythm:

- Roll call
- Opening remarks by `[COMMUNICATIONS DIRECTOR]`
- Brief operations summary (on-scene reps or operations)
- Summary of major communications plans and events
- Invitee comments
- Messaging coordination requirements outlined by national-level coordinating body representative
- Conclusion and next steps

If this incident has the potential to escalate to an event that crosses state lines, please contact the Cyber Communications Response Group at the Election Infrastructure Government Coordinating Council. `[INSERT CONTACT DETAILS FOR CCRG REPRESENTATIVE]` More information on the CCRG can be found in the Election Cyber Incident Communications Coordination Guide.

Should there be current coordination processes that are effective in sharing and coordinating information, such as regular calls, email listservs, continue to use them—particularly prior to, or the beginning phases of, activation. However, the scope and volume of an incident may make more direct communications, such as via the ICCL or a War Room, more useful.

Communications Process for a Cyber Incident

If a cyber crisis happens, it will demand its own communications plan. The steps below will help you assess the situation and take basic actions while you develop a more detailed communications plan. Each situation must be fully assessed on its own merits before a particular strategy is executed. The following are general guidelines:

Step 1: Activate the CCRT and obtain a technical briefing from the CIO or technical liaison.

Step 2: Only if absolutely necessary, and in consultation with IT specialists, decide if you need to disable agency website and launch a microsite outside of the agency's network. This will be a decision for `[JURISDICTION ELECTIONS DIRECTOR/LOCAL COUNTY AUDITOR OR CLERK]`. Notify key staff members. If website remains active, a message on the website may need to be posted.

Step 3: If necessary, contact law enforcement or federal authorities.

Step 4: If media are calling or showing up at the office, CCRT responds to reporters. If needed, you can issue a holding statement.
[Additional communications response materials are available to elections officials on request in the appendix to this document and can be obtained upon request from the National Association of Secretaries of State, the National Association of State Election Directors, or the U.S. Election Assistance Commission.]

Step 5: Notify key people: Chief Election Official, State Elections Director, Assistant Election Officials, Deputy Election Officials, IT Team, Communications Team, Elections Team.

Step 6: Inform entire agency of developing crisis, agency response, and agency policies that apply.

Step 7: Inform stakeholders / Legislature / Auditors.

Step 8: If you have not done so already, consider whether you need to inform the media/public about the incident. Make sure you inform the media only of confirmed facts that you are confident will not change (very few facts will fall into this category).

Step 9: Begin monitoring media coverage.

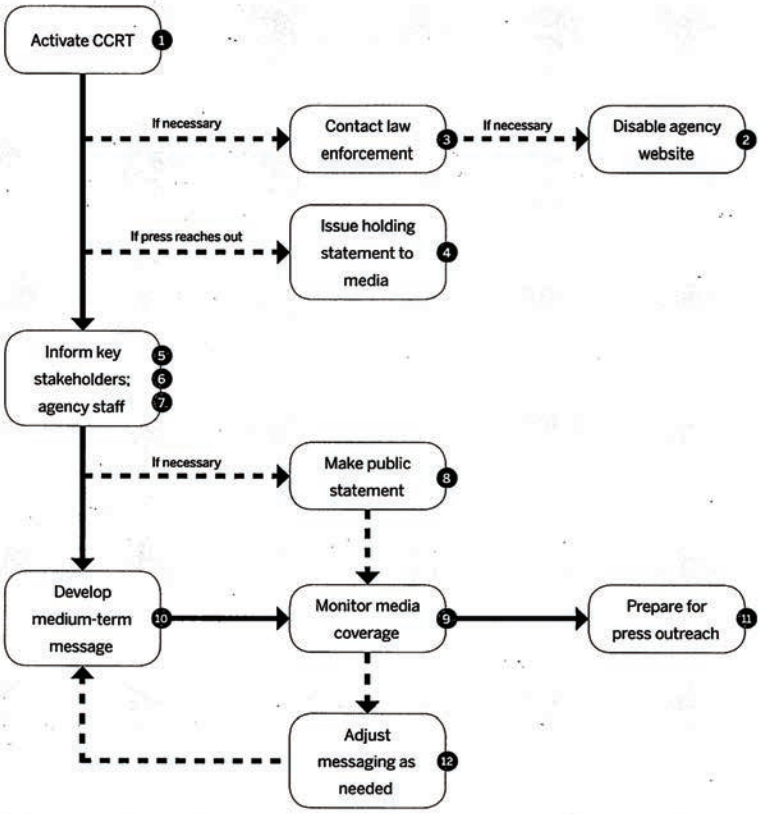
Step 10: Develop medium-term message.

Step 11: Prepare for press outreach/briefing and media schedule.

Step 12: Develop feedback loop from media monitoring or polling and incoming queries from media to determine if you need to recalibrate messages.

Communications Process for a Cyber Incident

Numbers below correspond to steps outlined in prior page



Communications Coordination & Response Checklist

Elections Crisis Communications Checklist

A cyber crisis has the potential to cast a negative light on the [CHIEF ELECTION OFFICIAL] or a local county elections office—as well as to undermine faith in the elections system. If you are uncertain whether a situation could escalate into a crisis, err on the side of standing up response teams, because you can always stand down if the incident does not escalate. (Consult [JURISDICTION'S]—Continuity of Operations Plan—in crises that impact operations.)

The checklists below can be adapted to your jurisdiction's processes. They provide guidance on actions to be taken in the lead up to, and days following, a cyber incident.

Action: Before a cyber crisis

- ☐ Identify office protocol and a crisis communications team. (Should include IT).
- ☐ Create a list of terms with common nomenclature for use by all stakeholders.
- ☐ Set an internal communication plan with elections staff. (How often, when, and where will all staff meet? Information must travel up and down the chain of command with clear boundaries for dissemination and interfacing with the public/media.)
- ☐ Ensure that all stakeholders can be reached in a crisis without access to the [CHIEF ELECTION OFFICIAL] network or smart phones.
- ☐ Craft communications materials that can be used in a potential cyber incident. For examples, elections officials may request sample materials from the National Association of Secretaries of State, the National Association of State Election Directors, or the U.S. Election Assistance Commission.)
- ☐ Ensure that staff understand their role in a cyber incident. For those who do not have a specific task to carry out, reassure them that their work is important and inform them how they can continue doing their jobs while designated managers handle the cyber incident.
- ☐ Ensure that communications plans can be accessed and are regularly updated.

Action: Before a cyber crisis becomes public

- ☐ Obtain technical briefing. (Assess and verify all information.)
- ☐ Decide whether to activate CCRT.
- ☐ Decide whether website can remain online. If you must disable it, launch a microsite (hosted on a different network) in its place.
- ☐ If email is potentially compromised, use an outside communications channel
- ☐ Consult authorities, if needed.
- ☐ Meet internally in war room; set internal communication schedule.
- ☐ Determine CCRT roles and responsibilities, if you have not already done so.
- ☐ Assess stakeholders.
- ☐ Determine broad communications strategy.
- ☐ Prepare holding statement.
- ☐ Develop communications plan.
- ☐ Draft additional communications required to execute plan, including a communications rollout plan (includes communication with media, stakeholders and employees).
- ☐ Establish plan for traditional and social media monitoring.
- ☐ Establish media response protocol.
- ☐ Notify `[CHIEF ELECTION OFFICIAL]` employees, if necessary. It may be that only a small group of employees are informed initially. Communicate internally, as needed.
- ☐ Notify stakeholders (See list on next page), if appropriate, and galvanize support.

Action: Once a cyber crisis becomes public

- ☐ Fact check: Make sure communications materials reflect current facts.
- ☐ Execute rollout plan, including informing media, if appropriate.
- ☐ Determine if microsite/web page is needed.
- ☐ Record an office greeting for phone system, if necessary.
- ☐ Maintain a record of inbound media inquiries and responses.
  `[ADD BULLETS ON FEEDBACK INFO FORM COVERAGE, CONVERSATIONS WITH REPORTERS AND OTHER DATA ON EXTERNAL REACTION]`
- ☐ Begin media (social and traditional) monitoring.
- ☐ Review and revise messaging, as needed, based on feedback.

General Media Inquiries Checklist

Gather basic facts:

- ☐ Story topic/angle/deadline
- ☐ Platform (blog, newspaper, television, radio, etc.) plus request content and images
- ☐ Other potential interview subjects
- ☐ Remember: Only designated spokespeople should speak or provide content.
- ☐ Remember: You have rights when you communicate with journalists, especially when asked about technical details you wouldn't be expected to know. "Let me see what I can find out for you" is always an option for a response. This response may mean that you return to the reporter without any additional information. You are not obligated to provide details.
- ☐ Remember: Reporters are under pressure from their editors and may shift the pressure to you. Do not speculate to fill gaps for them.

Notify key people:

- ☐ Meet internally.
- ☐ Craft media plan. Includes internal plans for staff and stakeholder communications.

- ☐ Designate key spokespeople and content providers. Assign tasks.
- ☐ Assist in crafting messaging. Reflect key audiences, people affected now, and those who will be affected in the future.
  - ☐ Voters
  - ☐ Counties
  - ☐ Candidates
  - ☐ Campaigns
  - ☐ Media
  - ☐ Other government offices
  - ☐ Vendors
  - ☐ General public
  - ☐ SOS employees and their families (if necessary)
- ☐ Demonstrate leadership by describing the steps you are taking to address this cyber incident. Consider contacting stakeholders who may be affected, especially if you think they may dislike or disagree with your messages.

Key Messages for Baseline Communications

You need to set a baseline understanding for the public that your [JURISDICTION] is taking cybersecurity seriously, and integrating best practices throughout the elections process. Below [are a few/is one example/s] of these baseline communications. In addition to a standing website message, develop key messages for [JURISDICTION'S] cyber preparedness activities and integrate them into current web content and future public remarks by [JURISDICTION'S] elections officials.

Below is one example of baseline communications. For your state, add relevant additional communications.

Sample State Website Message Emphasizing Cybersecurity

Note: Counties can modify to fit their jurisdiction.

Welcome to [STATE] State Elections. We are honored to serve you, the voters of [STATE]. Our mission is to ensure accessible, fair, and accurate elections.

Our office facilitates federal, state, and local elections conducted by all [X NUMBER OF] county election departments. We maintain voting equipment and software integrity, provide training and certification for election administrators, and support the statewide voter registration database.

Through educational programs and materials, we help all eligible [STATE] residents register to vote and cast an informed ballot. This website is one of many ways we provide information about [STATE'S] unique election system, our [INSERT DETAIL ON SYSTEM THAT SETS IT APART]. It provides [STATE] voters the power of citizen legislators, and the special services available to military voters, college students, voters with disabilities, and minority language communities.

We're proud that [STATE] is at the forefront of elections by embracing technology and innovation to better serve voters. Some of our achievements include:

[INSERT COMBINATION OF ACCOMPLISHMENTS ON TECHNOLOGY AND SECURITY:]

Second state to provide online voter registration

First to provide voter registration via Facebook

Ranked second for election administration in 2010 by the PEW Election Performance Index

Annual security audit of election equipment

Paper backup for electronic voting to provide auditable trail of voting records

Daily review of change log to identify unusual activity

One of first states to work with Homeland Security to provide cyber hygiene security scans and risk and vulnerability assessments

[STATE] State Elections is passionate about bringing access and transparency to the elections process. I hope you register and vote in our great state!

[CHIEF ELECTION OFFICIAL OR STATE ELECTIONS DIRECTOR]

Conclusion

As we head into the next election cycle, we hope that this Plan Template provides a running start for elections officials who are seeking to develop a cybersecurity communications response plan. We hope the guidance and format of this template helps officials prepare for, and manage, this emerging and evolving cyber risk to our elections process. As with all communications plans, we recommend that you regularly update your plan to account for changes in agency structures and personnel.

More information is available on the type of information communications materials should include. Election officials seeking examples of additional communications materials, can request the communications materials appendix to this document from NASS, NASED, or the EAC.

Do you see a way to make this Playbook better?

Are there new technologies or vulnerabilities we should address?

We want your feedback.

Please share your ideas, stories, and comments on Twitter @d3p using the hashtag #CyberPlaybook or email us at connect@d3p.org so we can continue to improve this resource as the digital environment changes.

Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 John F. Kennedy Street
Cambridge, MA 02138

www.belfercenter.org/D3P