DEFENDING DIGITAL DEMOCRACY PROJECT

Beyond 2020

Policy Recommendations for the Future of Election Security

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

REPORT
FEBRUARY 2021

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 and layout by Andrew Facini

DEFENDING DIGITAL DEMOCRACY PROJECT

Beyond 2020

Policy Recommendations for the Future of Election Security

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

REPORT
FEBRUARY 2021

Acknowledgments

The Defending Digital Democracy Project (D3P) would like to thank the following thought leaders and experts for sharing their time and insights as D3P reflected on the election ecosystem. **The varied perspectives of these experts greatly informed this report; however, the statements and recommendations are solely those of the authors and collective experience of D3P.**

- **Lori Augino**, Director of Elections, Washington Office of the Secretary of State
- **Karen Brinson Bell,** Executive Director, North Carolina State Board of Elections
- **Amy Cohen**, Executive Director, National Association of State Election Directors
- **Jeff Fields**, Member, U.S. Intel Community, Fellow, Belfer Cyber and Intelligence Projects
- **Mike Garcia**, Senior Advisor for Election Security, Center for Internet Security
- **Siobhan Gorman**, D3P Senior Advisor, Director, Brunswick Group
- **Thomas Hicks,** Commissioner, U.S. Election Assistance Commission
- **Juliette Kayyem**, Senior Belfer Lecturer in International Security, former Assistant Secretary, Intergovernmental Affairs, Department of Homeland Security
- **Ryan Macias**, former Acting Director, Voting Systems Testing and Certification Program, Election Assistance Commission
- **Alysoun McLaughlin**, Deputy Election Director, Montgomery County, MD
- **Sam Oliker-Friedland**, Chief Counsel, Center for Secure and Modern Elections
- **Tammy Patrick**, Senior Advisor, Elections Program, Democracy Fund, former Commissioner, Presidential Commission on Election Administration
- **Debora Plunkett**, D3P Senior Fellow and Senior Advisor, Belfer Cyber Senior Fellow, Former Director of Information Assurance, National Security Agency
- **Suzanne Spaulding,** D3P Senior Advisor, Senior Adviser, Homeland Security and Director, Defending Democratic Institutions Project, Center for Strategic and International Studies, former under secretary, Department of Homeland Security
- **Shane Schoeller**, County Clerk, Greene County, MO
- **Brian Scully,** Chief, Countering Foreign Influence Task Force, Cybersecurity and Infrastructure Security Agency
- **Ben Spear,** Director, Election Infrastructure ISAC, Center for Internet Security
- **Charles Stewart III,** D3P Senior Advisor, Kenan Sahin Distinguished Professor, MIT
- **Aaron Wilson**, Senior Director for Election Security, Center for Internet Security

We would also like to thank our colleagues, fellows, and students for their authorship, expertise, and support in bringing this report to fruition:

- **Austin Boral** is a current graduate student at the Harvard Kennedy School and Harvard Business School
- **Amina Edwards** is a current non-resident fellow with the Belfer Center for Science and International Affairs at HKS and former Harvard Business School graduate student
- **Stefani Jones** is a current Harvard Kennedy School graduate student and a Belfer Center Student Fellow
- **Kunal Kothari** is a former Harvard Kennedy School graduate student

- **Eric Rosenbach**, Co-director of the Belfer Center for Science and International Affairs at HKS, Director and Co-founder, D3P, Lecturer in Public Policy at HKS
- **Robby Mook**, D3P Co-Founder, Senior Fellow and Senior Advisor, Adjunct Lecturer at HKS
- **Maria Barsallo Lynch**, Executive Director of the Defending Digital Democracy Project

The Belfer Center for Science and International Affairs is the hub of Harvard Kennedy School's research, teaching, and training in international security and diplomacy, environmental and resource issues, and science and technology policy. The Defending Digital Democracy Project (D3P) identifies and recommends strategies and tools to protect democratic processes and systems from cyber and information attacks.

Table of Contents

Figures:

Voters mark their ballots during early voting at the Park Slope Armory in Brooklyn, Tuesday, Oct. 27, 2020.

AP Photo/Mary Altaffer

Executive Summary

The 2020 election presents a paradox. Despite dramatic changes to the election process due to the COVID-19 pandemic and increasingly complex threats since the 2016 election, 2020 is widely regarded as "the most secure [election] in American history."[1] Operationally, it was also one of the smoothest.[2] State and local election officials overcame unprecedented challenges and scarce resources to administer an election with fewer incidents of cyber compromises, technical failures or long lines than anticipated. After Election Day, recount procedures functioned as designed. Yet, amidst these successes, officials from both parties faced a barrage of mis- and disinformation about the election process that served to undermine confidence in the result. **Though the election security ecosystem survived the triple threat of cybersecurity, physical security, and mis- and disinformation in 2020, this success will prove to be hard to replicate in future election cycles without proper investment and reinforcement.**

D3P has identified four overarching challenges policymakers and election officials at the state and federal levels must address:

1. Many states do not have a coherent or consistent policy to protect local IT infrastructure and election systems, and lack the necessary funding to make needed improvements;
2. Although federal support was greatly enhanced since 2016, it is still inconsistent and spread across agencies;
3. Strategies and structures to confront mis- and disinformation are fragmented and insufficient at the state and federal levels, and fail to hold social media platforms sufficiently accountable for protecting election integrity;

1 "Joint Statement from Elections Infrastructure Government Coordinating Council & the Election Infrastructure Sector Coordinating Executive Committees." *Cybersecurity and Infrastructure Security Agency,* 12 November 2020, https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election.

2 Cassidy, Christina, Izaguirre, Anthony and Smyth, Julie Carr. "States Cite Smooth Election, despite Trump's Baseless Claims." *AP News*, 11 November 2020, https://apnews.com/article/election-2020-donald-trump-virus-outbreak-general-elections-elections-4060823b211ce91959b26f46efb73636.

4. Training and support for election officials remains inconsistent and hard to access.

This report highlights D3P's key recommendations for how these challenges can be addressed by state and federal legislators and policymakers. We believe these recommendations deserve serious consideration to create a more sustainable election ecosystem and stay ahead of challenges yet to come.

1. **Strengthen statewide cybersecurity coordination and funding:** It is ultimately the responsibility of state legislatures and executives to provide election officials with sufficient guidance, funding, and authorizations to run elections smoothly and sustainably. State leaders play an especially critical role in ensuring IT security—either by directly designing, managing, and implementing IT and security systems for local election officials, or by setting standards and collaborating to meet them. Centralizing security efforts not only bolsters statewide resilience against cyber attacks, but also lowers procurement costs and ensures security standards are met in smaller jurisdictions that lack the resources to procure and manage their own infrastructure.

2. **Streamline federal government support:** Congress is responsible for organizing the federal government to most efficiently deliver agency support to states, while channeling public funding towards long-term, capital intensive needs. There has been, and will continue to be, a robust debate over whether federal funding for elections should come with stipulations for how it can be used. However, Congress' first priority must be resourcing elections at a consistent, sustainable level and giving federal agencies the authorization and funding they need to better support states and localities—especially small and mid-sized jurisdictions.

3. **Increase trust in election integrity:** There is a shared responsibility between election officials, state and federal officeholders, the private sector, and civil society organizations to bolster and maintain trust in elections. The 2020 election saw an unprecedented rate of domestic election mis- and disinformation, as well as historic interest in the election and nationwide voter turnout. As citizens become increasingly interested in the process of election

administration and security—and as mis- and disinformation continues to spread—governments must be trusted sources of information who can credibly respond to concerns and rebut incorrect information. Dedicated, direct collaboration with private sector entities and civil society organizations can help bridge the gap and offer channels for swift response.

4. **Invest in election security talent:** Another shared responsibility of the public and private sectors is investing in election security talent across all levels of government and civil society through pipeline programs that supply talented personnel to election departments. Election administration—and particularly election cybersecurity—requires a diverse talent pool of well-trained election officials with the capacity to accommodate significant changes (e.g., large increases in early voting, surges in voter interest around general and primary elections, changing methods of vote-casting, increasing rates of non-English speakers). Through academic partnerships and intergovernmental fellowships, elected officials can actively invest in developing the next generation of election security talent. Ensuring a stable and well-prepared workforce—that renews itself with young, diverse, and digitally literate talent—is a critical component of the system's continued resilience.

Summary of Recommendations

1. **Strengthen statewide cybersecurity coordination and funding**
2. **Streamline federal government support**
3. **Increase trust in election integrity**
4. **Invest in election security talent**

	State Government Leaders	Federal Government Leaders
Organizational	☐ Fortify statewide cyber defense by consolidating IT infrastructure and setting security standards at the state level **(1a)**	☐ Improve federal cross-sector coordination for effectively responding to mis- and disinformation **(3b)**
Operational	☐ Expand proactive state communications efforts and civil society partnerships to improve public understanding of election processes and results **(3a)** ☐ Partner with accredited institutions to develop and expand cross-sector cybersecurity and election administration certification programs **(4a)**	☐ Strengthen the Cybersecurity and Infrastructure Security Agency's (CISA) authority to defend election infrastructure and support election administrators as an interagency coordinator **(2a)** ☐ Strengthen the Election Assistance Commission's (EAC) authority to improve voter experience and support election administrators as an intergovernmental clearinghouse for non-infrastructure best practices **(2b)** ☐ Establish an election fellows program to support state and local jurisdictions during election cycles, like Presidential Innovation Fellows or United States Digital Service **(4b)**
Fiscal	☐ Regularize local election appropriations and revise fee structures to ensure timely, equitable distribution of election administration and modernization costs **(1b)**	☐ Expand proactive funding avenues for state and local jurisdictions to modernize election infrastructure **(2c)**
Legal		☐ Increase transparency and accountability of those who traffic election-related disinformation by empowering states to take legal action **(3c)**

Recommendations

Article I, Section 4 of the Constitution empowers states with the authority to regulate and run their own elections.[3] Today, this responsibility is distributed across more than 10,000 jurisdictions at all levels of state government—each with distinct challenges, funding structures, and common characteristics. This is how the United States has run elections for over two centuries.[4] Yet as threats to election security have grown increasingly complex in the last two decades, public dialogue about the issue has pivoted from state to *federal* funding and policy. This shift was in part driven by the nationalization of media and the decline of local news, as well as the rise of foreign, cyber-based threats that only federal agencies have the capabilities and authorities to address.[5] As public dialogue shifts and threats to elections evolve, the roles and responsibilities of government stakeholders—particularly between the federal and state levels—becomes more difficult to delineate.

Much of the progress made in 2020 was the result of temporary fixes and one-off support that election officials cannot necessarily count on in 2022 or 2024. This included hundreds of millions of dollars in private philanthropic donations to state and local election officials and a record number of volunteers.[6] Federal agencies made elections a top priority and 'did what needed to be done,' stretching their mandates to fill operational voids.[7] Nationwide capabilities to respond to persistent cyber, information, and operational threats significantly improved since 2016, but require additional reinforcement to be sustainable.[8]

3 *U.S. Constitution*. ArtI.S4.C1.1.1.1.1 Role of the States in Regulating Federal Elections. https://constitution.congress.gov/browse/essay/artI-S4-C1-1-1-1-1/ALDE_00001036/#:~:text=Article%20I%2C%20Section%204%2C%20Clause,the%20Places%20of%20chusing%20Senators.

4 "Election Administration at State and Local Levels." *National Conference of State Legislatures*, 3 February 2020, https://www.ncsl.org/research/elections-and-campaigns/election-administration-at-state-and-local-levels.aspx.

5 Hopkins, Dan. "All Politics Is National Because All Media Is National." *FiveThirtyEight*, 6 June 2018, https://fivethirtyeight.com/features/all-politics-is-national-because-all-media-is-national/.

6 Sprunt, Barbara. "Poll Worker Numbers Have Many Election Officials Breathing Sigh of Relief." *NPR News*, 29 October 2020, https://www.npr.org/2020/10/29/928225412/on-poll-workers-many-election-officials-breathe-sigh-of-relief.

7 Collier, Kevin. "Despite Trump's claims, federal agencies foresee a secure election." *NBC News*, 9 October 2020, https://www.nbcnews.com/news/us-news/despite-trump-s-claims-federal-agencies-foresee-secure-election-n1242795.

8 Johnson, Derek B. "Experts tout election security gains since 2016." *Federal Computer Week*, 28 August 2020, https://fcw.com/articles/2020/08/28/johnson-election-security-congress.aspx.

D3P's past work and recent conversations with election professionals at the local, state, and federal levels, demonstrate the tradeoffs of increasing collaboration between state and federal governments. Through the following recommendations, we have taken pains to respect state sovereignty in the election process by focusing on what states and the federal government can each uniquely do to better secure elections.

1. Strengthen statewide cybersecurity coordination and funding

CHALLENGE:

Many states do not have a coherent or consistent policy to protect local IT infrastructure and election systems, and lack the necessary funding to make needed improvements. The devolved nature of election administration—which many states delegate to counties, cities, and localities—is ultimately a strength, because it makes the election ecosystem more robust against attacks.[9] However, decentralized information technology (IT) infrastructure can be a weakness if states lack clear standards and local jurisdictions don't have the expertise and resources needed to properly secure systems. While some states have chosen to centralize their IT infrastructure, others have yet to decide on any clear policy at all—leaving localities in limbo and their systems unsecured. In addition, insufficient and inconsistent funding for local security enhancements and operational needs remains a challenge. After one-off, ad hoc appropriations from the Help America Vote Act of 2002 (HAVA) ran out, many state and local election officials relied on hundreds of millions of dollars in private funding to support the logistics of mail and in-person voting in 2020.[10] Although election officials received $400 million in federal appropriations to cope with adjustments due to COVID-19, most states still lack a dedicated funding stream to continue updating and enhancing election technology on an ongoing basis.[11]

(1a) Fortify statewide cyber defense by consolidating IT infrastructure and setting security standards at the state level. As threats to election infrastructure grow increasingly sophisticated and the consequences of successful attacks become even more dire, most local jurisdictions simply cannot afford to maintain and secure their own IT systems. At the same time, states and their localities have grown increasingly intertwined from a cybersecurity perspective (e.g., through voter registration databases, electronic pollbooks, election night reporting systems) making election

9 Pastor, Robert A. "The United States Administration of Elections: Decentralized, Pre-modern and Contented." *The Electoral Knowledge Network*, https://aceproject.org/ace-en/topics/em/annex/electoral-management-case-studies/the-united-states-decentralized-to-the-point-of.

10 Sherer, Michael. "Mark Zuckerberg and Priscilla Chan donate $100 million more to election administrators, despite conservative pushback." *The Washington Post*, 13 October 2020. https://www.washingtonpost.com/politics/zuckerberg-chan-elections-facebook/2020/10/12/0e07de94-0cba-11eb-8074-0e943a91bf08_story.html.

11 Wiersema, Alisa. "States' election funding requests indicate numerous anticipated hurdles." *ABC News*, 25 April 2020, https://abcnews.go.com/Politics/states-election-funding-requests-numerous-anticipated-hurdles/story?id=70275211.

systems' security only as strong as their weakest link. However, small changes can significantly enhance security.

- **Develop a cohesive IT strategy**: In states that still lack clear guidance or governance for IT systems, state election authorities, governors, and state legislators can put policies in place to answer three questions: *(1) what are the optimal IT setup and standards for local jurisdictions and who is accountable for putting them in place? (2) who is responsible for funding and monitoring this setup to ensure standards stay in place? and (3) how are state leaders and employees addressing cyber incidents and building an ongoing culture of security?* The issue of autonomy can be just as sensitive between states and localities as it is between states and the federal government; however, many municipalities welcome the ability to outsource IT as long as they retain control of election administration. Some states, like Michigan, chose to consolidate their cybersecurity governance at the state level—others may choose to take a more hybrid approach where duties are split between the state and counties (*Figure A*). Regardless, state executive and legislative branches should ensure there is a coherent standard and strategy—and that resources (i.e., talent and funding) are available to implement and sustain it.

FIGURE A:

Michigan's 2011 and 2015 Cyber Initiative state plans present a helpful example of how states can migrate localities to a consolidated backbone without eroding local control. The following excerpts are synthesized from CISA's comprehensive case study:[12]

- **Strategy and Planning**: Based on the Governor's overarching strategy to address cyber risks, the Department of Technology Management and Budget (DTMB) Director/Chief Information Officer (CIO) developed a statewide strategic information technology (IT) plan. This plan set direction for how the state government would use and secure technology, while establishing a formal governance structure for execution.
- **Budget and Acquisition**: The governance structure put the CIO and State Budget Office in charge of evaluating IT and cyber-related spending requests across state agencies and making recommendations to the legislature for approval. Meanwhile, the CSO was made responsible for the state's IT acquisition approach for evaluating and managing risks associated with proposed IT acquisitions across agencies.
- **Risk Identification and Mitigation**: Michigan then merged its cyber and physical security teams under a single role, the CSO, which sets policies and standards to govern information security across state government systems. The CSO's office actively worked with state agencies to assess and manage cybersecurity risks in system development, while using a shared service model to support local municipalities that cannot fully fund their own.
- **Incident Response**: The state then worked with federal and state governments, private industry, and others to create a Cyber Disruption Response Plan (CDRP) to guide preparation for and response to cyber incidents across public and private organizations. The state tailored existing emergency management response and recovery approaches and structures to cyber incidents, using a five-level threat matrix to move cyber incidents through escalation and de-escalation of the incident across the DTMB and the Emergency Management and Homeland Security Division.
- **Information Sharing**: Michigan remains intentional in its formal and informal information sharing mechanisms at strategic, operational, and tactical levels. The CSO participates in cross-state information sharing bodies, such as the Multi-State Information Sharing and Analysis Center (MS-ISAC) and National Association of State Chief Information Officers (NASCIO).

12 "Cybersecurity Governance in the State of Michigan." *Cybersecurity and Infrastructure Security Agency*, December 2017, https://www.cisa.gov/sites/default/files/publications/Michigan_Cyber_Governance_Case_Study_508.pdf.

- **Transition to the .gov top-level domain (TLD)**: In many cases, election systems are not walled off from other government systems, which can offer an additional attack surface for malicious actors seeking to disrupt elections through tactics such as ransomware. Using local domains also leaves voters vulnerable to social engineering through forged email addresses and spoofed domains, which can be used to harvest personal data, spread malware, and disseminate false or inflammatory information.[13] With federal support from the December 2020 DOTGOV Online Trust in Government Act, localities can proactively bolster their cyber defense by transitioning IT infrastructure at the county and state levels—including election websites, email addresses, and online voter-registration portals—to .gov addresses.[14]

(1b) Regularize local election appropriations and revise fee structures to ensure timely, equitable distribution of election administration and modernization costs. Local election offices are constrained to operate under state rules, and yet in most states, there is no well-defined way of allocating the cost of operating local elections. Meanwhile, the federal government's role in helping to pay for elections remains unclear—leaving states to reckon with chronic under-funding.

- **Allocate state funding more consistently**: The Help America Vote Act's (HAVA) ad hoc appropriations have been too reactive and inconsistent to give states the support they need for long-term planning and modernization. Rather than depending on the federal government for this support, state legislatures can bridge the gap in 2021 by assessing their own costs to secure elections and funding elections on a regular basis. This assessment should also acknowledge the critical capacity officials require to execute activities that support and protect their core mission of election administration (e.g., hiring additional personnel to monitor, report, and respond to mis- and disinformation).

13 Miller, Maggie. "Krebs emphasizes security of election as senators butt heads." *The Hill*, 16 December 2020, https://thehill.com/policy/cybersecurity/530532-krebs-doubles-down-on-asserting-the-security-of-the-election-as-senators.

14 Freed, Benjamin. "Stimulus bill includes .gov bill to help states and localities move domains." *StateScoop*, 21 December 2020, https://statescoop.com/stimulus-bill-includes-gov-bill-domains/.

- **Allocate state funding more equitably**: For many states, the cost of election administration is not fairly distributed across jurisdictions or levels of government, leaving some offices with access to more resources than others. Some states bear the full cost of election security and administration centrally for all contests (e.g., Alaska, Delaware); others bear the full cost only for state elections or ballot initiatives (e.g., Colorado, Louisiana); others allow local jurisdictions to cover costs and reimburse for certain components (e.g., Kentucky, Rhode Island).[15] In many states, these payment models underestimate the costs of election administration for local jurisdictions and overestimate anticipated funding from federal sources. These models also do not account for the long-term investments required to maintain and modernize election infrastructure, compounding the challenges of inconsistent federal funding. States can learn from each other to introduce and expand renewable revenue streams to support election administration. For example, Washington's 'real estate-based' reimbursement approach ensures that costs are covered according to the share of federal, state, and local elections represented on the ballot (e.g., if X% of a given ballot is filled by federal contests, the federal government covers X% of costs).

15 Owens Hubler, Katy and Underhill, Wendy. "Election Costs: Who Pays and With Which Funds?" *National Conference on State Legislatures*, 11 March 2018, https://www.ncsl.org/research/elections-and-campaigns/election-costs-who-pays-and-with-which-funds.aspx.

2. Streamline federal government support

CHALLENGE:

Although federal support was greatly enhanced since 2016, it is still inconsistent and spread across agencies. In 2002, the Election Assistance Commission (EAC) was established by HAVA as a 'one-stop-shop' for recommended best practices, data about elections, and independent certification of voting systems. However, insufficient funding since its inception forced the EAC to take a back seat to other agencies and entities in coordinating and delivering this support. During the 2020 election cycle, The Cybersecurity Infrastructure and Security Agency's (CISA) Election Security Initiative (ESI) at DHS filled the void, serving as a hub for federal interagency coordination and cybersecurity support to states.[16] CISA quickly grew "from a backwater agency that was largely unknown outside Washington to the main federal government liaison to a nationwide ecosystem of officials running the elections."[17]

In establishing CISA as a dedicated agency, the Trump administration successfully built on the Obama administration's blueprint for defending state election systems as "critical infrastructure."[18] This move enabled the federal government to provide cybersecurity assistance to state and local election officials and "[enjoy] all the benefits and protections of critical infrastructure that the U.S. government has to offer"—however, redundancies in the roles and responsibilities of the EAC and ESI remain.[19] Election officials still occasionally have to navigate the federal bureaucracy to get the full benefit of support from other agencies like the Department of Defense (DoD), Federal Bureau of Investigation (FBI), and Center for Disease Control (CDC), to name a few. Meanwhile, declining federal funding for the EAC has hindered its ability to execute its mission and expand its reach to small and mid-sized jurisdictions.

16 Goldstein, Phil. CISA, Working with Partners, Kept the 2020 Election Secure and Free from Interference." FedTech Magazine, 11 November 2020, https://fedtechmagazine.com/article/2020/11/cisa-working-partners-kept-2020-election-secure-and-free-interference.

17 Marks, Joseph. "DHS plans largest operation to secure U.S. election against hacking." The Washington Post, 30 October 2020, https://www.washingtonpost.com/nation/2020/10/30/dhs-is-planning-largest-ever-operation-secure-us-election-against-hacking/.

18 "Congress Passes Legislation Standing Up Cybersecurity Agency in DHS." Department of Homeland Security, 18 November 2020, https://www.dhs.gov/news/2018/11/13/congress-passes-legislation-standing-cybersecurity-agency-dhs.

19 Johnson, Jeh. "Statement by Secretary Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector." Department of Homeland Security, 21 September 2018, www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

(2a) Strengthen the Cybersecurity and Infrastructure Security Agency's (CISA) authority to defend election infrastructure and support election administrators as an interagency coordinator. In an ideal world, Congress would consolidate all federal support for elections into a single entity. However, the most realistic option at this time is for Congress to build on what's working and clarify EAC and CISA's roles so that states have clarity on where to get support. This will allow the two entities to institutionalize and expand best practices coming out of 2020.

Broadly speaking, CISA should be more clearly authorized to convene interagency collaboration and organize federal support for election infrastructure and cyber-related matters. Meanwhile, the EAC should focus on expanding its role as a national clearinghouse of resources for election officials and take the lead on developing new resources of non-infrastructure best practices for election officials, such as how state and local officials can best educate voters and manage mis- and disinformation. The following recommendations (*2a* and *2b*) present a clear delineation between CISA, which is mandated "to enhance the security and resilience of election infrastructure" by supporting election administration with cyber-related responsibilities (e.g., cybersecurity assessments, detection and prevention), and the EAC, which is mandated to improve voter experience by supporting election administrators with non-infrastructure responsibilities (e.g., ballot design, training, public engagement).[20]

- **Consolidate infrastructure-related responsibilities within CISA's ESI**: As the nation's risk advisor, CISA plays a critical role in securing election technology and infrastructure, which DHS defines as (1) voter registration databases and associated IT systems; (2) IT infrastructure and systems used to manage elections; (3) voting systems and associated infrastructure; (4) storage facilities for election and voting system infrastructure; and (5) polling places (including early voting locations).[21] Currently, the EAC's voting system testing and certification program only tests and certifies hardware and

20 "CISA Strategic Intent," Cybersecurity and Infrastructure Security Agency, August 2019, https://www.cisa.gov/sites/default/files/publications/cisa_strategic_intent_s508c.pdf.

21 "Election Security." Department of Homeland Security, 14 July 2020, https://www.dhs.gov/topic/election-security.

software from one of these five areas—voting systems.[22] Shifting these responsibilities to CISA will leverage the agency's technical expertise, tools, cybersecurity services, and testing suite (e.g., penetration testing, reliability testing, source code review, supply chain validation) to improve the efficacy, efficiency, and frequency of testing for all election technology.[23] This shift will also remove any barriers to sharing critical information through greater access to law enforcement and the intelligence community and routine access to Sensitive Compartmented Information Facilities (SCIFs), which allow election officials to get a more holistic view of emerging threats and adversarial operations.

- **Authorize CISA to lead interagency coordination on election security**: Over the course of the 2020 election cycle, ESI's responsibilities evolved to meet the needs of state and local election officials, as well as their federal agency counterparts at the DoD, FBI, CDC, and United States Postal Service (USPS), among others. Their core programs—including CISA's Tabletop Exercise Package (CTEP), and Federal Virtual Training Environment (FedVTE)—provided critical information and support to election officials across the country. Meanwhile, the agency's core coordinating initiatives —including the Election Infrastructure Government Coordinating Council (GCC), the Election Infrastructure Sector Coordinating Council (SCC) and the Election Day war room—provided critical lines of communication across intelligence agencies, election officials and elected officials in D.C. and beyond. However, CISA's success as an interagency coordinator depended on informal relationships established by ESI. To extend these core coordinating initiatives, Congress can revise the Cybersecurity and Infrastructure Security Agency Act of 2018 to formally include this convening mandate, which will help ESI institutionalize all the best practices from 2020. If these authorizations are not clarified, Congress risks a substantive backslide in federal support for election infrastructure and cybersecurity.

22 State Requirements and the U.S. Election Assistance Commission Voting System Testing and Certification Program. The U.S. Election Assistance Commission, 4 September 2020, https://www.eac.gov/sites/default/files/TestingCertification/State_Requirements_for_Certification09042020.pdf.

23 "Voluntary Voting System Guidelines." U.S. Election Assistance Commission. https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines.

- **Establish a CISA Center of Excellence to incubate election technologies and expand shared services**: Last year's National Defense Authorization Act (NDAA) gave CISA the authority to develop shared services that can be utilized across all federal agencies, as well as state and local governments.[24] The Biden administration's recent American Rescue Plan proposed a $9 billion investment to expand CISA's "new IT and cybersecurity shared services… [and] complete modernization projects at federal agencies."[25] Building on this momentum, establishing a CISA Center of Excellence (COE) can elevate DHS' cyber agency as a one-stop shop for guiding state and local election officials through testing, vulnerability assessments, and recommended mitigations to help them prioritize ongoing efforts and implement necessary resiliency measures where applicable.

  The COE can also emulate DoD's Defense Innovation Unit (DIU) and Joint Artificial Intelligence Center (JAIC) by incubating and piloting new tools through related service offerings, which could also be shared across federal agencies. These 'center of excellence' approaches connect organizations across the DoD with leading technologists and companies across the country "to rapidly prototype and field advanced commercial solutions that address national security challenges."[26] While the House already called for a similar Center of Excellence in Election Systems in the Election Technology Research Act of 2020 (H.R. 4990), housing this initiative within CISA would help fulfill its mandate to defend election infrastructure.[27] In November 2020, the DoD, DIU, and DHS signed a memorandum of understanding to collaborate on a range of cybersecurity initiatives to advance CISA mission-specific needs ranging from network and infrastructure security, to blockchain, to digital risk management.[28]

24 Starks, Tim. "A look inside Congress' biggest cyber bill ever." CyberScoop, 7 December 2020, https://www.cyberscoop.com/congress-solarium-commission-defense-authorization-ndaa/.

25 Boyd, Aaron. "Biden-Harris Admin Proposes $10B in New IT and Cyber Funding for Federal Agencies." Nextgov, 15 January 2021, https://www.nextgov.com/it-modernization/2021/01/biden-harris-admin-proposes-10b-new-it-and-cyber-funding-federal-agencies/171446/.

26 "Joint Artificial Intelligence Center." Chief Information Officer, U.S. Department of Defense, https://dodcio.defense.gov/About-DoD-CIO/Organization/JAIC/.

27 Election Technology Research Act of 2020. H.R.4990, 116th Congress, 17 September 2020, https://www.congress.gov/bill/116th-congress/house-bill/4990. 2019/2020.

28 Vergun, David. "DHS Collaborating on Innovative Cybersecurity Solutions." *U.S. Department of Defense News*, 17 December 2020, https://www.defense.gov/Explore/News/Article/Article/2449534/dod-dhs-collaborating-on-innovative-cybersecurity-solutions/.

CISA's COE can build on this collaboration to elevate election security technologies—such as blockchain, cloud security, and artificial intelligence for voter fraud and interference monitoring—in partnership with state and local jurisdictions.

FIGURE B:

The following allocation of roles and responsibilities is inspired by a bipartisan group of 17 secretaries of state. In a recent letter to Senate and House leadership, the group calls on Congress to bolster funding for the EAC in support of a wide range of election-related responsibilities.[29] The below division reflects D3P's vision for how new and existing responsibilities can be distributed between the EAC and CISA's ESI to streamline federal support and increase specialization.

EAC Responsibilities

- Serve as a national clearinghouse of information on election administration (e.g. *distribute* digital, technology and cyber resources; *develop* resources like poll worker training, communicating trusted election information, etc.)
- Develop guidance to meet HAVA requirements, audit the use of HAVA funds, submit an annual report to Congress, and testify periodically about HAVA progress and related issues
- Develop and deliver recommendations, tools, and support to election officials—including guidance on voter deadlines and registration, model legislation, best practices for voting methods, template communications strategies and response plans for mis- and disinformation, etc.
- Retain a design team to support states in developing voting materials and voter education content
- Maintain the national mail voter registration form developed in accordance with the National Voter Registration Act of 1993
- Hold public meetings and hearings to inform the public about the EAC's progress and activities

29 Brandon Moseley. "Merrill, 16 Other Secretaries of State Support Funding for Election Assistance Commission." *Alabama Political Reporter*, 8 December 2020, https://www.alreporter.com/2020/12/18/merrill-16-other-secretaries-of-state-support-funding-for-election-assistance-commission/.

CISA Responsibilities

- Serve as an interagency coordinator for election security across federal entities (e.g., FBI, ODNI*, EAC, USPS, CDC) and private sector entities (e.g., social media platforms) through initiatives such as the Countering Foreign Influence Task Force (CFITF), the Cyber Information Sharing and Collaboration Program (CISCP), and the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)
- Operate a modern election technology testing and certification program for all components of election infrastructure—including penetration testing, reliability testing, source code review, supply chain validation, etc.
- Establish a team dedicated to recommend improvements to the voluntary voting systems guidelines (VVSG) and to create best practices and guidelines for election technologies
- Develop and deliver infrastructure and cyber-related tools and support to state and local officials—including programs such as Crossfeed, Rumor Control, the Continuous Diagnostics and Mitigation (CDM) program, the Enhanced Cybersecurity Services (ECS) program, and critical product evaluations (CPE)
- Implement a robust personnel training program available to all election officials nationwide—including CTEP and FedVTE

** Office of the Director of National Intelligence*

(2b) Strengthen the Election Assistance Commission's (EAC) authority to improve voter experience and support election administrators as an intergovernmental clearinghouse for non-infrastructure best practices. Congress can further clarify the division of labor between CISA and the EAC by changing and enhancing the EAC's role in the following ways:

- **Expand funding to support intergovernmental engagement as a clearinghouse**: Since 2010, the EAC's budget has been cut in half, severely limiting its ability to support state and local jurisdictions. Their enacted fiscal year 2021 appropriation of $19.1 million for operating expenses represents an increase of $3.9 million above the prior level, but still does not allow the EAC to hire experts or develop materials and training required to provide states the

guidance and support 17 secretaries of state recently requested.[30] However, we recommend that the cyber and infrastructure-related initiatives in their letter should be shifted to CISA (*Figure B*).[31]

- **Retain a design team to support officials in developing voting materials and voter education content that mitigates the effects of mis- and disinformation**: As ballots, voter education materials, and voter registration forms have become increasingly complex, state and local election officials can benefit from more guidance and support to improve voter experience and reduce confusion. Although the 2020 election saw substantially lower rates of rejected ballots relative to previous general and primary elections—thanks in large part to the voter education and awareness campaigns led by civil society organizations—the total number of rejected mailed and absentee ballots increased in several states.[32] While the EAC's last government-sponsored report on ballot design and delivery was conducted in 2007, civil society organizations such as the Center for Civic Design[33] and U.S. Digital Response have bridged the gap by publishing their own best practice guides. Moving forward, the EAC should contract an election design and delivery team that, by request, can offer states suggestions on how they can improve the design of voter registration forms, ballots, and instructional materials to reduce spoiled or rejected registration applications and votes.

- **Invest in expanding state and local communications capabilities**: Election officials and civil servants at the state and local level must invest heavily in proactive constituent and stakeholder communications to ensure that correct election information is disseminated to all communities, particularly those that may be distrustful of mainstream media or government sources. In D3P's own work

30 Buble, Courtney. White House Budget Gives Election Agency More Funding, But Expert Says It's Not Enough." *Government Executive*, 11 February 2020, https://www.govexec.com/management/2020/02/white-house-budget-gives-election-agency-more-funding-expert-says-its-not-enough/163045/.

31 Brandon Moseley. "Merrill, 16 Other Secretaries of State Support Funding for Election Assistance Commission." *Alabama Political Reporter*, 8 December 2020, https://www.alreporter.com/2020/12/18/merrill-16-other-secretaries-of-state-support-funding-for-election-assistance-commission/.

32 Fessler, Pam. "A 2020 Surprise: Fewer Absentee Ballot Rejections Than Expected." *NPR News*, 31 December 2020, https://www.npr.org/2020/12/31/951249068/a-2020-surprise-fewer-absentee-ballots-rejections-than-expected.

33 "Field Guides to Ensuring Voter Intent." *Center for Civic Design*. https://civicdesign.org/fieldguides/.

training local election officials in 2020, we saw tremendous interest in materials and training to help them develop realistic communication strategies and we continue to hear the expressed need for further communications training and support. Through additional funding and authorization, Congress can also bolster EAC's ability to provide communications strategies and tools for election officials and offices through capability building (e.g., media training, communications workshops) and best practices (e.g., templates for communications response plans to help election officials counter mis- and disinformation). However, CISA would continue its ongoing efforts to identify and address mis- and disinformation campaigns through initiatives such as the Countering Foreign Influence Task Force (CFITF) and its collaboration with EI-ISAC and officials in reporting such incidents.

(2c) Expand proactive funding avenues for state and local jurisdictions to modernize election infrastructure. Since HAVA provided over $4 billion in direct support for states to update voting infrastructure in 2002, the federal government has provided funding for elections on an ad hoc basis, including $1.2 billion since the 2018 midterms—$400 million of which was from the CARES Act as a result of the COVID-19 pandemic.[34] While estimates vary, consensus indicates that getting jurisdictions 'caught up' on needed security, technology, and audits will cost approximately $2 billion over the next four years.[35]

- **Allocate federal funding more consistently**: Moving forward, Congress must provide funding to states on an ongoing, predictable basis—much like it does for other critical infrastructure such as electrical grids, interstate highways, and government facilities. This will allow states to better plan upgrades and adapt their own budgets accordingly. Though states are ultimately responsible for running and managing elections, increased reliance on technology and sophisticated security practices make consistent federal

34 "2020 CARES Act Grants." *U.S. Election Assistance Commission*. https://www.eac.gov/payments-and-grants/2020-cares-act-grants.

35 Norden, Lawrence and Cortes, Edgardo. "What Does Election Security Cost?" *Brennan Center for Justice*, 15 August 2019, https://www.brennancenter.org/our-work/analysis-opinion/what-does-election-security-cost.

funding critical to ensuring a baseline level of national security. This reliance is further reinforced by the federal government's vested interest in each state's success. As the 2020 contest demonstrated, real or perceived problems with any state's election administration can cast doubt on federal election results and severely undermine public trust in elections at large.

- **Introduce federal innovation block grants**: The U.S. electoral system's highly decentralized network of more than 10,000 distinct jurisdictions offers "laboratories of democracy" through which election administration and security practices have been developed and deployed over the course of several decades.[36] However, state and local governments are struggling to fund the maintenance of their existing election infrastructure, let alone incentivize or scale innovation. Existing programs at the Department of Education, the Economic Development Agency, and the Department of Energy demonstrate that the federal government is capable of recognizing and encouraging state-led innovation through block grants (*Figure C*). A specific focus on recognizing and scaling best practices—such as replacing paperless voting systems, expanding online voter registration, and conducting post-election audits—can also allow election officials to identify and scale solutions to issues that they face every day. These innovation block grants could be offered through CISA, building on DHS' preparedness grants program and the Science & Technology team's contracting mechanisms.

36 "Election Administration at State and Local Levels." *National Conference of State Legislators*. 3 February 2020, https://www.ncsl.org/research/elections-and-campaigns/election-administration-at-state-and-local-levels.aspx.

FIGURE C:

The federal government can look towards a number of agencies for successful examples of how federal dollars have enabled state-specific innovation through public and private sector involvement:

The U.S. **Department of Education (ED)** oversees the Education Innovation and Research program (formerly known as the Investing in Innovation Fund), which supports local educational agencies and nonprofit organizations to expand innovative practices that have a demonstrated impact on mission-specific needs such as "improving student achievement or student growth, closing achievement gaps, decreasing dropout rates, increasing high school graduation rates, or increasing college enrollment and completion rates."[37] As of November 2019, the program awarded nearly 250 grants totaling $1.7 billion since it was established by the American Recovery and Reinvestment Act of 2009.[38]

The U.S. **Economic Development Agency (EDA)** oversees the "Build to Scale" program (formerly known as Regional Innovation Strategies), which aims to expand technology-based economic development initiatives that advance mission-specific needs such as "accelerating high quality job growth, creating more economic opportunities, and supporting the future of the next generation of industry leading companies."[39] The program has awarded $100 million in grants across six national competitions, matched by over $115 million in community dollars across 224 projects since it was established by the America COMPETES Reauthorization Act of 2010.[40]

The U.S. **Department of Energy (DOE)** oversees the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs, which aim to help small businesses conduct R&D projects that meet specific DOE mission-specific needs such as energy production, energy use, and environmental management. As of January 2020, these programs awarded 158 grants totaling $32 million to 118 small businesses in 32 states.[41]

37 "Investing in Innovation Fund (i3)." *U.S. Department of Education*, 21 June 2017, https://www2.ed.gov/programs/innovation/index.html.

38 Campbell, Neil and Quirk, Abby. "Lessons Learned From the Investing in Innovation Program," *Center for American Progress*. 5 November 2019, https://www.americanprogress.org/issues/education-k-12/reports/2019/11/05/476831/lessons-learned-investing-innovation-program/.

39 "About Office of Innovation and Entrepreneurship," *U.S. Economic Development Agency*, https://www.eda.gov/oie/.

40 United States, Congress. Public Law 111-358. *U.S. Government Publishing Office*, https://www.congress.gov/111/plaws/publ358/PLAW-111publ358.pdf.

41 "Department of Energy Announces $32 Million for Small Business Research and Development Grants," *U.S. Department of Energy*, 6 January 2020, www.energy.gov/articles/department-energy-announces-32-million-small-business-research-and-development-grants.

3. Increase trust in election integrity

CHALLENGE:

Strategies and structures to confront mis- and disinformation are fragmented and insufficient at the state and federal levels, and fail to hold social media platforms sufficiently accountable for protecting election integrity. Though election officials expected widespread mis- and disinformation from both foreign and domestic malicious actors—including state-sponsored efforts from Russia and Iran—domestic sources played a bigger role in sowing distrust in the 2020 election. Election officials were inundated by calls and threats regarding false claims of voter fraud both before and notably for many weeks after the election.[42] On the final day of the 2020 election cycle, these threats culminated with an attack on the U.S. Capitol as Congress counted Electoral College votes—a visible manifestation of disinformation moving beyond the digital world, and a dramatic reminder that this challenge must be tackled proactively rather than reactively.

In responding to mis- and disinformation, federal agencies collaborated with civil society organizations, private sector organizations, and election officials, as demonstrated by ESI's Rumor Control initiative and the Elections Infrastructure Information Sharing and Analysis Center's (EI-ISAC) cross-sector coordination. However, many of the collaborative efforts established to track and report issues for this election were hastily set up—and it's unclear whether they will extend beyond the 2020 election cycle.[43] Although leading social media platforms such as Twitter and Facebook introduced new policies and processes in 2020 to support election officials with addressing mis- and disinformation and collaborated with government entities to monitor and mitigate disinformation on a limited basis, they also hindered information sharing with national security stakeholders and election officials through siloed, opaque communication.[44]

42 Helderman, Rosalind S., et al. "Despite Trump's Intense Hunt for Voter Fraud, Officials in Key States Have so Far Identified Just a Small Number of Possible Cases." *The Washington Post*, 23 December 2020, https://www.washingtonpost.com/politics/voter-fraud-investigations-2020/2020/12/22/bdbe541c-42de-11eb-b0e4-0f182923a025_story.html.

43 Miller, Maggie. "New federal cybersecurity lead says 'rumor control' site will remain up through January." *The Hill*, 3 December 2020, https://thehill.com/policy/cybersecurity/528675-new-federal-cybersecurity-lead-says-rumor-control-site-will-remain-up.

44 Isaac, Mike and Conger, Kate. "Google, Facebook and Others Broaden Group to Secure U.S. Election." *The New York Times*, 12 August 2020, https://www.nytimes.com/2020/08/12/technology/google-facebook-coalition-us-election.html.

(3a) Expand proactive state communications efforts and civil society partnerships to improve public understanding of election processes and results.

- **Leverage authority and convening power of Chief Election Officials to build trust**: As they hold the responsibility to run elections, states must play a lead role in fighting disinformation. Voters need both visible and trusted sources of information, as well as proactive education efforts on election security and spotting misinformation. Chief Election Officials (e.g., Secretaries of State, State Election Directors) are well-positioned to lead such an effort, lending bipartisan credibility and, in turn, raising the profile of their work. State and local leaders can establish a commission of local election officials to engage stakeholders from across civil society and academia, social media platforms, government agencies, and elected officials to develop efforts and recommendations for countering disinformation. Many of these stakeholders have already collaborated with election professionals to advance their work individually and collectively in establishing themselves as voices of authority—these partnerships helped disseminate critical voter education, counter mis- and disinformation, and verify accurate information on election processes and results more widely in the 2020 general election. This recommendation builds on these efforts with an aim to continue elevating all election officials as trusted conduits of information to wider audiences than communications teams and smaller jurisdictions could traditionally reach on their own. Congress can also financially support the commission to identify and elevate best practices for combatting historic rates of mis- and disinformation, and to conduct a post mortem on the repercussions of mis- and disinformation throughout the 2020 election cycle.

- **Expand access to public spaces for civic purposes**: From 2000 to 2015, an estimated $12 billion in public money was spent to subsidize the costs of building privately-owned stadiums.[45] This amount excludes the $4 billion in taxpayer subsidies to provide loans (in

45 Heller, Chris. "The Impossible Fight Against America's Stadiums." *Pacific Standard*, 5 September 2017, https://psmag.com/economics/the-shady-money-behind-americas-sports-stadiums.

the form of tax-exempt municipal bonds) for these projects—as well as other funds used to support similarly large venues (e.g., concert halls).[46] Public investment can produce tangible benefits, such as job creation and tax revenue, as well as intangible ones, such as increased quality of life and "civic pride."[47] State and local governments can partner with private civic spaces (e.g., stadiums, museums, libraries, concert venues) to make them available for election purposes (e.g., voting, vote counting). This approach invites citizens into the civic process, bolstering exisiting efforts by election officials to increase transparency and trust in the election process, and lowers barriers to entry for voting.

(3b) Improve federal cross-sector coordination for effectively responding to mis- and disinformation.

- **Expand CISA's ability to counter information operations**: During the 2020 election, CISA filled a critical gap in federal efforts to combat election mis- and disinformation. CISA is well positioned to lead this work for future cycles at the federal level, and should be given the authority to do so—particularly because of the agency's role in facilitating information sharing from election professionals across national security entities. CISA should expand its efforts to facilitate coordination between election officials and social media companies, amplifying jurisdictions' pages and websites as a source of truth for fact-checks and content flags, and working to exempt them from content moderation intended for political entities—a role that has often been filled by individual leaders or informal collaborations between government and civil society groups.
- **Reinforce the EI-ISAC as a cross-sector clearinghouse for election disinformation reporting and risk mitigation**: Established in 2018 and funded by CISA, EI-ISAC's mission is to "improve the overall cybersecurity posture of SLTT (state, local, tribal, and

46 Kuriloff, Aaron, and Darrell Preston. "In Stadium Building Spree, U.S. Taxpayers Lose $4 Billion." *Bloomberg*, 14 September 2012, https://www.bloomberg.com/news/articles/2012-09-05/in-stadium-building-spree-u-s-taxpayers-lose-4-billion.

47 Diedrich, Christoper. "Homefield Economics: The Public Financing of Stadiums." PolicyMatters, vol. Volume 4, Number 2, Spring 2007, https://www.faegredrinker.com/webfiles/Homefield%20Economics.pdf.

territorial) election offices, through collaboration and information sharing among members, the U.S. Department of Homeland Security and other federal partners, and private sector partners."[48] However, EI-ISAC and its parent organization—the Center for Internet Security (CIS)—lack the necessary 'carrots and sticks' to incentivize cooperation from private sector stakeholders (e.g., social media firms). With CISA's support, expanding EI-ISAC's authority and capability as the central mechanism for incident reporting would reinforce the need for partners across all sectors and levels of government to collaborate on issues of mis- and disinformation—especially at the state and local level.

(3c) Increase transparency and accountability of those who traffic election-related disinformation by empowering states to take legal action. In 2018, the Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA) carved out a new exception to Section 230—one of the most impactful clauses of the Communications Decency Act of 1996. Section 230 states that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[49] This protects websites that host speech from laws that might otherwise be used to hold them legally responsible for what their users say or do online and offline—and in turn, subverts the cost-benefit analysis of actively mitigating mis- and disinformation.[50] Just as FOSTA holds social media firms accountable to fighting sex trafficking by reducing their legal protections, a new carve out of Section 230 can hold platforms accountable to fighting election-related disinformation during election season. This statute could narrowly permit states' chief election officials to sue social media firms if they don't do enough to remove mis- or disinformation about the elections they administer. Relevant content could include false information about how to vote and the election process, but also false allegations of fraud.

48 "EI-ISAC Charter," *Center for Internet Security*, January 2020, https://www.cisecurity.org/ei-isac/ei-isac-charter/.

49 "Communications Decency Act." 47 U.S.C. § 230, 8 February 1996, https://www.govinfo.gov/content/pkg/USCODE-2011-title47/html/USCODE-2011-title47-chap5-subchapII-partI-sec230.htm.

50 Liability for Content Hosts: An Overview of the Communication Decency Act's Section 230. LSB10306, *Congressional Research Service*, 6 June 2019, p. 5, https://crsreports.congress.gov/product/pdf/LSB/LSB10306.

4. Invest in election security talent

CHALLENGE:

Training and support for election officials remains inconsistent and hard to access. Human capital—an ongoing pain point for government offices that struggle to attract young election workers and retain cybersecurity talent—was buoyed by a massive influx of volunteer interest and philanthropic support in 2020. Meanwhile, the government's digital talent gap has only widened in recent years, as the capabilities of the digital workforce and capacities of technology companies to attract (and pay) such workers have increased exponentially.[51] The COVID-19 pandemic further highlighted the public sector's digital talent gap, underscoring the critical role that this workforce plays in fulfilling government responsibilities—especially election administration and security—during times of crisis. While curricula for election administration and cybersecurity exist, they are not deployed in a robust or consistent way. And in countless jurisdictions, many core processes and security standards stem from institutional knowledge that is not well documented for ongoing maintenance in the context of an aging election administration workforce.

(4a) Partner with accredited institutions to develop and expand cross-sector cybersecurity and election administration certification programs. This recommendation emulates the Defense Acquisition University (DAU)—a corporate university of the U.S. Department of Defense (DoD) that provides ongoing technology, logistics, and acquisitions training to military personnel. DAU leverages partnerships with colleges and universities—including American University, Purdue University, SUNY Empire State College, and UCLA Extension School—that allow DoD workforce members to transfer DAU course credits toward degrees and certificates. By working with these universities and other civil society stakeholders, state and federal election professionals can share the responsibility of standardizing and scaling election security training. Expanding partnerships with city and state universities could be critical to establishing a deeper, more experienced bench of election administrators, whose highly specific knowledge and expertise— including, but not limited to, cybersecurity—is critical to minimizing incidents of all kinds and responding appropriately before, during, and after elections (*Figure D*).

51 Clark, Danny, Jacobs, Marcy, McConnell, Megan and Tucker-Ray, Sarah. "Transforming the US government's approach to hiring digital talent." *McKinsey & Company*, 9 September 2020, https://www.mckinsey.com/industries/public-and-social-sector/our-insights/transforming-the-us-governments-approach-to-hiring-digital-talent.

FIGURE D:

During the 2020 election cycle, some academic institutions partnered with local election offices to supplement CISA's foundational package of trainings for administrators across jurisdictions:

- In March 2018, the University of West Florida's Center for Cybersecurity introduced election security into its training curriculum offered to Florida state- and county-level cybersecurity personnel.[52]
- In November 2019, the University of Southern California's Annenberg Center on Communication Leadership and Policy (CCLP) launched an "innovative training program that empowers election and campaign officials nationwide to reinforce their defenses against digital attacks that may affect the integrity and outcome of elections."[53]
- During the summer of 2020, D3P launched a national training tour effort for local election officials as they prepared for the election. The tour was conducted digitally, taking best practices from D3P's prior national in-person tabletop exercises. In addition to supporting local election officials through customized trainings, the tour also hosted special sessions for state and local election officials and involved civil society and government partners. The tour engaged over 750 officials across 17 states and was also made available afterward online.

(4b) Establish an election fellows program to support state and local jurisdictions during election cycles, like Presidential Innovation Fellows or United States Digital Service. A fellowship program can create new pathways for talent into election administration, and can help election officials bridge the gap between preparation and execution of election security measures and user experience during the peak period of future election cycles (e.g., June through November). For example, the University of Chicago's Election Cyber Surge program matched "volunteer cybersecurity professionals with local election officials to help them protect their voter registration databases, websites and anything else that might be targeted by foreign adversaries."[54] These programs not only embed top talent in government to improve public programs, but also serve as a unique entry point for highly-skilled young people who might not have considered a career in government service before the experience (*Figure E*).

52 Ryan Johnston, "Florida starts cybersecurity training through university, cyber range partnerships," *StateScoop,* 20 March 2018, https://statescoop.com/florida-starts-cybersecurity-training-through-university-cyber-range-partnerships/.

53 "USC Expands Effort to Protect Elections from Digital Attacks." *University of Southern California Press Room*, 14 November 2019, https://pressroom.usc.edu/usc-expands-effort-to-protect-elections-from-digital-attacks/.

54 Freed, Benjamin. "Why a think tank is connecting cybersecurity volunteers with election officials," *StateScoop*, 21 September 2020, https://statescoop.com/why-a-think-tank-is-connecting-cybersecurity-volunteers-with-election-officials/.

FIGURE E:

Federal and state government officials can look to a number of existing government-sponsored and civil society programs to build talent in the short- and long-term:

- The **Presidential Innovation Fellows** program, which places technologists, designers, and strategists with participating federal agencies as "entrepreneurs in residence" for one year, bringing "the best of data science, design, engineering, product, and systems thinking into government."[55]
- The **United States Digital Service**, (USDS) which "deploys small, responsive groups of designers, engineers, product managers, and bureaucracy specialists to…bring best practices and new approaches to support government modernization efforts."[56]
- TechCongress' **Congressional Digital Service Fellowship**, which places technologists within participating Congressional offices for an eight month sprint to help modernize the digital infrastructure of the Congress.[57]
- Coding It Forward's **Civic Digital Fellowship**, which places student software engineers, data scientists, product managers, and designers with participating federal agencies to innovate at the intersection of technology and public service.[58]
- ODNI's **IC Civilian Joint Duty Program**, which creates cross-agency expertise by fostering an environment of information-sharing, interagency cooperation and intelligence integration at all levels.[59]
- The Trump administration's proposed **Cybersecurity Cup competition**, which "will identify, challenge, and reward the government's best personnel supporting cybersecurity and cyber excellence," allow cybersecurity employees to rotate among agencies, and introduce a new cybersecurity aptitude test to reskill federal workers.[60]

55 "Who We Are." *Presidential Innovation Fellows*, https://presidentialinnovationfellows.gov/about/.

56 "Our Mission." *United States Digital Service*, https://usds.gov/mission.

57 "The Congressional Digital Service Fellowship." *TechCongress*, https://www.techcongress.io/congressional-digital-service.

58 "Civic Digital Fellowship." *Coding It Forward*, https://www.codingitforward.com/civic-digital-fellowship.

59 "Joint Duty." *Office of the Director of National Intelligence*, https://www.dni.gov/index.php/careers/joint-duty.

60 Vavra, Shannon. "White House Targets Federal Cybersecurity Workforce Development in New Executive Order." *FedScoop*, 3 May 2019, https://www.fedscoop.com/white-house-targets-federal-cybersecurity-workforce-development-new-executive-order/.

Conclusion

The above recommendations are meant to shed light for state and federal lawmakers on some of the most pressing challenges and opportunities facing the U.S. election system today. However, they are by no means comprehensive. We acknowledge that the environments and obstacles facing state and local election officials across all jurisdictions require unique solutions, and that state and federal budget shortfalls are not unique to election security. We also acknowledge that investing resources in election administration comes at the cost of investing in other pressing issues. However, electing officials who represent the will of the American people requires a secure election system that citizens trust. Election security should never need to be a crisis-driven issue—but despite the successes of 2020, the U.S. election system is facing innumerable, existential challenges that threaten one of the most defining features of democracy. Without swift, sufficient action from state and federal government leadership, widespread distrust in the 2020 election process and outcome will further deteriorate and destabilize the only institutions that can address this problem.

As the world's oldest continuous democracy, the United States holds a unique position as a beacon for self-rule throughout the world. In order to ensure that our democracy continues to set a global example, we must ensure that election security is a priority, not something we deal with only when the system is in crisis. The devolved nature of our election ecosystem is a strength; both because democracy is best administered at its grassroots, and because of the opportunity for innovation that local sovereignty presents. Our challenge now is to ensure that local, state, and federal officials work together to confront a more complex and difficult set of challenges than our democracy has ever encountered. If D3P's nationwide work with committed public servants is any indication, we are confident America's election officials and elected leaders who play a role in upholding and defending democracy can meet the challenge.

About the Defending Digital Democracy Project

The Belfer Center's nonpartisan Defending Digital Democracy Project (D3P) was founded with one goal: to help defend democratic elections from cyber attacks and information operations—persistent threats that emerged in the aftermath of the 2016 election.

Since July 2017, our team has worked alongside election administrators, national security and cybersecurity experts, political and civic thought leaders to develop and deliver practical strategies, tools, and recommendations to protect democratic processes and systems from cyber and information attacks. These efforts have taken the form of incident communication response plans, tabletop exercises, playbooks for countering and responding to cybersecurity attacks and information operations, data analysis, and national training events in person and online.

The project has also provided recommendations through congressional testimony and reports. D3P has engaged over a thousand election officials across more than 40 states and the District of Columbia.

Additional Resources

- **The Cybersecurity Campaign Playbook**
  November 2017
- **The State and Local Election Cybersecurity Playbook**
  February 2018
- **The Election Cyber Incident Communications Coordination Guide**
  February 2018
- **The Election Incident Communications Plan Template**
  February 2018
- **The Elections Battle Staff Playbook**
  December 2019
- **The Election Influence Operations Playbook, Part 1**
  September 2020
- **The Election Influence Operations Playbook, Part 2**
  September 2020

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

www.belfercenter.org/D3P

Printed in the United States of America