Assessment of Democracy Fund’s Improving Security and Confidence in Elections Portfolio

NOVEMBER 2021

TABLE OF CONTENTS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Democracy Fund contracted with Fernandez Advisors to assess its Improving Security and Confidence in Elections portfolio which is part of its Trust In Elections strategy. This strategy was created by Democracy Fund in 2017 in response to cyber threats to state and local election systems as well as declines in public opinion measures of election integrity following the 2016 presidential election. The portfolio funded programs that would enable election officials to have the resources, knowledge, and will to execute physical and digital defenses to secure election systems. The theory of change proposed that these investments would improve capacity to adapt and protect against ongoing threats to election systems and increase public confidence that elections are secure.

Specifically, Democracy Fund wanted this assessment to answer a small number of questions:

- How do experts in the field perceive the impacts of different kinds of investments made within the portfolio? Were they useful? And why?
- Which efforts supported by Democracy Fund were adopted by government and why? For those initiatives adopted by government are they stable and likely to continue through any political change?
- What changes are occurring in the field?
- What gaps exist?

This executive summary describes the methodology used for the assessment and previews our key findings. The rest of the assessment does two things:

- Provides context for the current state of trust in elections by reviewing the last five years.
- Provides greater detail on each of the findings.

Methodolgy

In June of 2021, Democracy Fund staff working on the Security and Confidence in Elections portfolio developed a memo summarizing the history and key decision-points in this track of work. This was followed by a portfolio review meeting to further clarify how investments within the track of work fit into Democracy Fund's theory of change. Both the memo and debriefing identified key issues and experts to include in this assessment. Fernandez Advisors reviewed the memo and participated in the debriefing.

Subsequently in August and September of 2021, Fernandez Advisors conducted qualitative interviews with 22 election cybersecurity and election law experts, current and former government officials, and advocates for secure and modern elections. We solicited their perspective on the current state of election cybersecurity and trust in elections, as well as changes in the last five years and capacity gaps that remain. Some but not all of those interviewed were current or former grantees of Democracy Fund.

From these interviews and the materials provided by Democracy Fund, Fernandez Advisors identified the state of the field, the types of investments that appear most useful, and gaps that need to be filled.

Findings Summarized

Which Democracy Fund investments were useful?

Interviewees expressed support and respect for Democracy Fund's understanding of the field, and generally felt Democracy Fund's investments were impactful. However, certain investments were highlighted more frequently. These included:

- The Belfer Center's Tabletop exercises and Cybersecurity Train the Trainer modules adapted for election administrators.
- Practical tools and guides to election audits (including Risk-Limiting Audits), tailored for an election administrator audience and other practitioners.
- On-call technical assistance available to election administrators to assist with prioritizing cybersecurity and cyberhygiene plans and understanding and implementing post-election audits. Praise was notable for no-cost expert support from The Elections Group.
- National Governors' Association Policy Academy sessions focused on cybersecurity and crisis communications planning.

What made these investments useful?

Investments with the following characteristics generally rose to the top when experts were discussing value:

- Investments that recognized and sought to bridge siloes between levels and branches of local, state, and federal government, recognizing that a cross-agency model is often necessary given the nature of election administration, cybersecurity, and the diversity of threats.
- Investments that directly supported capacity building for state and local election administrators, especially in the areas of cybersecurity and cyberthreats.
- Tools that were more practical and that could be applicable to on the ground needs (as opposed to those that might be more appropriate for discussion in academic settings).
- Investments that demonstrate proof of concept through working with a smaller number of pilot projects or jurisdictions, and which can then ultimately reach scale, generally through government adoption.
- Interviewees appreciated Democracy Fund's ability as a philanthropic institution to absorb the risks associated with innovation at a moment of high stakes and intense public scrutiny on election processes and administrators. Interviewees pointed to monetary and reputational risks that stem from investing in new or unproven programs or approaches. Current and former government officials noted that due to the accountability and public scrutiny that generally accompanies the use of public funds, government dollars are often not useful for initial tests of innovative tools or new approaches.

What investments were adopted by government, what are their characteristics, and how stable is continued government adoption?

Certain Democracy Fund supported activities were adopted by government. Characteristics that are consistent with government adoption include:

- Tools were used in multiple jurisdictions, and thus clearly replicable.
- Tools solved a problem that government understood, for example the lack of coordination across different levels of government and across different departments.
- Government adoption occurred after Democracy Fund and nonprofit partners assumed the risk to establish proof of concept.
- Tools need to be perceived as nonpartisan. Alternatively, government's leeriness for tools perceived as partisan can lead to important improvements not being adopted.

Continued government adoption of these types of tools is not ensured for at least two reasons:

- The potential for increased politicization of election administration.
- Instability of funding for cybersecurity specifically and election administration generally.

State of the Field

Interviewees were proud of the progress on cybersecurity analysis and capacity built over the last five years. However, interviewees also raised key concerns:

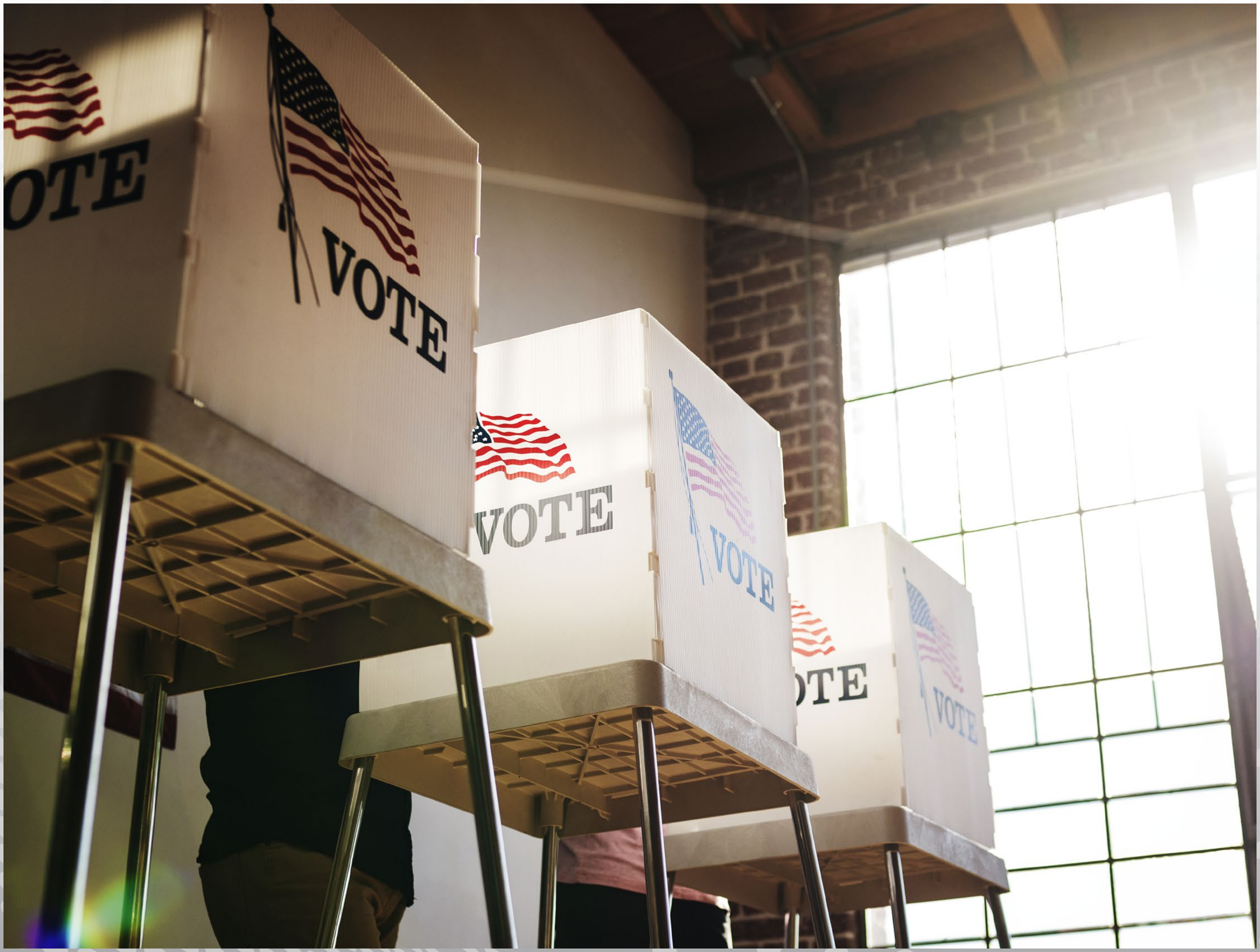
- The scale of cyberthreats and attacks, as well as increases in misinformation, disinformation, and malinformation (MDM) threaten to reverse advances made in the last five years.
- Respondents also expressed considerable apprehension at the resilience of unfounded attacks on the integrity of the election process and their corrosive impact on Americans' trust in elections and other public institutions. While no respondents knew exactly what to do about organized misinformation, there was strong agreement on the need for a national and perhaps international mobilization to counteract its effects.
- Many interviewees pointed to the threat of complacency on cybersecurity after a secure 2020 election, raising the prospect of insufficient future and sustained funding from the federal government to continue vigilance across the country.

Persistent and Emerging Gaps in the Field

Interviewees pointed to an array of gaps that continue to characterize the field. These are generally tied to a combination of attacks on the field, the politicization of election administration, the changing role of audits, and ongoing financial gaps.

- Capacity gaps for election administrators are growing because of expanding threats. Many of these gaps are at the intersection of technology, cybersecurity, and MDM.
- As more states expand mail voting, absentee voting, early voting and online registration, the entry points for bad actors to attack voter databases and public access portals expands significantly.
- There is an increasingly symbiotic relationship between misinformation and disinformation on the one hand and cybersecurity threats and attacks on the other, with the two phenomena reinforcing each other.

- There is uncertainty on how to create accountability for social media platforms in stopping the spread of MDM.
- The politicization of election administration raised concerns for interviewees, as they foresee negative impacts on day-to-day elections operations, the proliferation of partisan election audits, and an undermining of the basic idea of nonpartisan election administration.
- Post-election audits and RLAs are here to stay, fueling a continued need for technical assistance and support for election administrators. State and local election officials need training, technical support, and access to best practices on audits. There is also a need for standards establishing the requirements of a valid post-election audit.
- There does not appear to be significant new election administration cybersecurity funding coming from the federal government.
- The field lacks message development and communications training for election officials. This gap is more pronounced as attacks on election administration proliferate in television and social media.
- There is a lack of philanthropic support for election cybersecurity and post-election audit work. There is a need to convene funders to build support for this as well as for a communications campaign to help build trust in elections.



BACKGROUND AND CONTEXT

The 2016 United States presidential elections witnessed interference from foreign states and actors that sought to influence the outcome of the election and sow distrust in democracy and democratic institutions. Foreign actors also leveraged material gained from cyberattacks to seed misinformation and confusion among the electorate.

Malware and other tools were used to break into state election system databases. The Illinois and Arizona voter registration databases were breached — likely by Russian agents.[1] Up to 500,000 individual voter records were potentially compromised in Illinois.[2] Election officials in Durham County, North Carolina reported widespread problems with voter records and misleading messages sent to poll workers, possible indications of a cybersecurity breach of a Florida company that provided data support for Durham County e-poll books.[3] As one interviewee noted:

> *“[We saw the] exposure of fundamental security weaknesses in our brittle election infrastructure. Now that our adversaries saw how brittle it was, this exposed us to more threats and attacks on the operation side of our infrastructure. This is straining our democratic process.”*

Democracy Fund’s Trust In Elections strategy was started in 2017 in response to these types of cyber threats to state and local election systems and concurrent declining levels of public trust in those systems. Following initial research, Democracy Fund chose to fund in four areas:

1. Fortify the field with workable solutions and best practices, bolstered by research and collaboration between civic technologists, cybersecurity experts, and election officials.
2. Empower election officials to advocate for greater funding to better protect and strengthen election technology, while preserving the right to vote.
3. Lead research efforts, and the dissemination of contingency policies, verification practices, and resiliency efforts (physical, digital, and process-based) for election officials.
4. Lead public education efforts around the legitimate risks to election systems and thwart the ability of malevolent actors to foster distrust by identifying and disseminating effective messages to trusted validators and the media.

[1] ”Russian Interference in 2016 U.S, Elections”, https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections, accessed November 15, 2022.
[2] Politico.com, “How Close Did Russia Really Come to Hacking the 2016 Election?”, December 26, 2019, https://www.politico.com/news/magazine/2019/12/26/did-russia-really-hack-2016-election-088171, accessed 10.5.21
[3] Politico.com, “How Close Did Russia Really Come to Hacking the 2016 Election?”, December 26, 2019, https://www.politico.com/news/magazine/2019/12/26/did-russia-really-hack 2016-election-088171, accessed 10.5.21.

Democracy Fund's initial grantmaking in the third quarter of 2017, focused on building election law resources, deterring foreign influence in elections, and producing election cybersecurity research and best practices.

Simultaneously, federal agencies began to investigate election cybersecurity failures to understand how to shore up American election systems and cybersecurity infrastructure. In January of 2017, President Obama's Secretary of the Department of Homeland Security designated elections infrastructure as part of the nation's critical infrastructure. This designation made election infrastructure a priority for federal cybersecurity assistance and protections.

It was clear that there was a dearth of election cybersecurity infrastructure nationwide. Cybersecurity literacy and preparedness were new terrain for many of the nearly 10,000 election jurisdictions across the country. Election administrators faced a learning curve on cyberhygiene and systems analysis, and often lacked the capacity to address and avert potential cyberthreats. Collaboration across functions and levels of government needed to be established from the ground up.

Throughout 2018, Democracy Fund made investments to attempt to address these gaps, via making available trainings, tools, and hands-on support for election administrators. In May of 2018, to address declining levels of trust for the integrity of elections, Democracy Fund launched the Election Validation Project and through this project produced a series of how-to guides called "Knowing It's Right". This project sought to build public trust through rigorous audits, standards, and testing of election results and systems. To facilitate the project, Democracy Fund made a small number of grants and hired expert consultants to develop tools, materials, and trainings to support effective audits of elections.

In November of 2018, Donald Trump signed the Cybersecurity and Infrastructure Security Agency Act into law. This created within the Department of Homeland Security, the Cybersecurity and Infrastructure Security Agency (CISA). CISA is tasked with identifying and leading responses to cybersecurity threats and vulnerabilities across the nation, including through coordinating cybersecurity efforts with state governments. Through CISA, expert support and technical resources are made available to state and local election administrators to assess their cybersecurity preparedness and prepare for future cyberthreats.

In 2018, $380 million in federal funding was appropriated for election security and cybersecurity preparedness efforts via Help America Vote Act Election Security Funds.[4] State matching funds were required for receipt of HAVA election security dollars. Another tranche of $425 million in election security funding was appropriated in early 2020. This federal funding, in addition to some additional federal support in 2020 via the CARES Act, was intended to provide support to state and local election jurisdictions for their proactive work to assess and protect their election infrastructure from cyberattacks.

From January 2019 to January 2020, Democracy Fund made grants to organizations to support election administrators' preparations for the 2020 election. The grantees continued to focus on addressing cybersecurity in campaigns and election administration, auditing tools, information sharing, and other needs of election officials. All of this was done while the global pandemic changed how everyone was doing their work and election administrators needed to accommodate changes in how people were voting (with many more people voting early or via mail).

Prior to and following the November election, a new phenomenon threatened public confidence in elections. Donald Trump adopted the position that the election was stolen and persistently repeated claims that election administration lacked integrity. Election workers were threatened. Election audits were used for political purposes to attempt to demonstrate that Trump was cheated. Fortunately, all of these audits, no matter their quality, wound up demonstrating that the elections were free, fair, and accurately decided.

These false claims spread through social media, talk radio, and new television media outlets that were willing to share misinformation on election administration, the precision of vote counts and accuracy of voting machines. On January 6, 2021, a coup was attempted as marauding rioters attacked Capitol Police and ransacked the halls of Congress trying to stop the counting of electors and certification of the election. Fully eight Republican Senators, and 139 Republican House Members voted to overturn the election of President Biden citing many of the same arguments that Trump, and his lawyers, made unsuccessfully in courts around the country.

Because this became the dominant post-election story, some key aspects of this election have not received as much attention. The election was hugely successful, with more people voting and higher percentages of people voting than ever before. As well, more people and higher percentages of people voted early and voted by mail than in any previous national election. Despite this growth in electorate size and the complexity of managing an election during the pandemic, there were no major election cybersecurity breaches. The tools, trainings, multi-level communications, and investments made by government and private philanthropy to reduce risk appear to have been successful.

[4] United States Election Assistance Commission, "Election Security Funds", https://www.eac.gov/payments-and-grants/election-security-funds, accessed 10.5.21.

FINDINGS AND ANALYSIS

Which Democracy Fund investments were useful?

There were a number of tools and practices that resulted from Democracy Fund's investments that were cited consistently by interviewees as having important impacts.

The Belfer Center's Tabletop Exercises and Cybersecurity Train the Trainer Modules

Democracy Fund's investments in tools and training resources adapted by the Belfer Center were cited by nearly all interviewees as having high impact for their work and for the field overall. These were identified as highly impactful investments that supported effective collaboration across agencies, functions, and levels of government to bridge siloes. Belfer Center tools supported collaborating on response protocols, information sharing, and scenario planning.

The Belfer Center's Train the Trainer models were seen as effective at responding to the need for tailored and easily digestible training on cybersecurity. Election administrators in leadership positions appreciated that these trainings could be replicated by their staff working on the front lines.

The Center's Tabletop exercises, which adapted a simulation approach long used by government to deal with natural disasters and military planning, continue to be used by various government agencies at the state and federal level, including CISA and election administrators. The Belfer Center decided to end its cybersecurity training programs in 2020 to avoid duplication, as it felt other nonprofits including Stanford University's Center for International Security and Cooperation as well as the Center for Internet Security had taken on similar work.

Tools and guides for election officials on how to administer post-election audits

Post-election audits, including Risk Limiting Audits (RLAs), are increasing in use. There are both good and bad reasons for this. Some states are legitimately trying to ensure secure and modern elections. In other states, politicians are attempting to legitimize erroneous concerns about "election integrity" and use audits for political purposes.[5]

Well run risk limiting audits are an important and legitimate way to ensure elections are run securely and thus build public trust. A serious concern is that when audits become politicized, best practices will not be used. The State of Arizona's so-called "forensic audit" of Maricopa County did not follow best practices.

Prior to 2017, when Colorado had its first statewide RLA, no state had conducted a statewide RLA. Since 2018, seven additional states have implemented RLAs (CA, OH, WA, GA, IN, NV, OR). Four states (RI, MI, GA,

[5] At the time of this report, the state legislatures of Pennsylvania and Wisconsin were both considering large-scale post-election audits to investigate the validity of the 2020 election results. Three other states (Georgia, Michigan, and Arizona) conducted or considered post-election audits in specific counties and specific voting mechanisms such as absentee ballots or voting machines alone. Information available at https://www.brennancenter.org/our-work/research-reports/partisan-election-review-efforts-five-states. Accessed 9.29.21.

PA) conducted statewide RLAs in 2020, and multiple counties in three states (VA, CA, NV) completed RLAs in the same year. VotingWorks developed RLA software called Arlo that was used in 5 states in 2020. The State of Washington brought on a dedicated staff person to begin implementing RLAs statewide in 2021—a resource commitment that interviewees believe will add significant capacity.

There is real value in tools that support officials trying to manage audits effectively. Many election administrators found themselves scrambling in 2021 to facilitate audits, often for the first time and frequently with little advance planning time. Democracy Fund supported and published a series of reports from Jennifer Morell. These included *Knowing It's Right: Limiting the Risk of Certifying Elections*[6] which explains the policy issues that underpin post-election audits, what state policymakers should consider in this context, and an implementation guide for election administrators on post-election audits and RLAs.

Similarly, the Elections Group's post-election audit tools and resources that explain and provide step-by-step implementation guidance were perceived by interviewees as responding to the evolving election landscape. Elections Group's presentations at the 2021 conferences of the National Association of State Election Directors and the National Association of Secretaries of State were pointed to by interviewees as helpful to inform their understanding of post-election audits, RLAs, and the considerations that accompany audit implementation at the state level.

> *"Because of the ever-changing election laws, having these third-party groups can fill the void by providing best practices from other states. You can just pick up the phone and say, 'They just passed a law, I don't know what to do.'"*

On-call technical assistance available to election administrators.

On-call expertise was cited repeatedly as worthwhile. Jennifer Morell and Noah Praetz from the Elections Group were identified as crucial supports for election administrators as they tackled evolving cybersecurity needs and priorities. Morell and Praetz, themselves former elections officials, were seen by interviewees as understanding election cybersecurity needs on the ground as well as best practices from other states. These experts' ability to be on call at no cost is valuable as the elections landscape continues to evolve rapidly. The Elections Group provides a host of best practices and other resources free of charge on their website that respond to emerging issues, including the continued effects of election misinformation and other challenges faced by elections administrators.[8]

[6] Available at https://democracyfund.org/idea/knowing-its-right-limiting-the-risk-of-certifying-elections/. Accessed 9.29.21.

NGA Policy Academy sessions on cybersecurity and crisis communications planning

The National Governors Association (NGA) strategy sessions and NGA Policy Academy that focused on crisis communications responses for Governors were cited as useful. These sessions involving Governors and election administrators were highlighted for bridging siloes often seen between state and local government on election cybersecurity. As ransomware and phishing incidents continue to target municipalities and businesses, multiple interviewees pointed out the importance of Governors understanding cybersecurity threats and vulnerabilities. With a focus on scenario planning and response protocols, both in an operations setting and from a communications perspective, interviewees felt these efforts were able to meaningfully engage governors on cybersecurity preparedness.

> *"Governors now realize more that election cybersecurity is under their purview given the critical infrastructure designation. They see this as their responsibility and that they need to step up."*

What made Democracy Fund investments useful?

Bridging siloes between levels and branches of local, state, and federal government

Noting progress on coordination across the field, interviewees pointed to a wide gulf prior to the 2016 elections between federal cybersecurity experts, local election administrators, state elected leaders, and cybersecurity professionals. As one interviewee described it,

> *"We had 8000 islands within all the local election jurisdictions. There still are islands, but that's mostly . . . their own choosing, not because of lack of [election] infrastructure."*

While collaboration between levels of government has improved since 2016, the decentralized nature of American election administration results in a wide variety of practices, standards, and levels of resources available to jurisdictions.

> *"We've gone into a digitally complex and technical operation in the last ten years. The skills that we hired for ten years ago aren't the skills that we need today. . . . Human capital hasn't transformed at the same rate as the field."*

Interviewees pointed to a persistent jurisdictional tug of war between federal agencies tasked with cybersecurity responses such as CISA and state or local election offices responsible for implementing cybersecurity practices on the ground.[9] Planning sessions such as the National Governors' Association Policy Academy, the Belfer Center's Tabletop exercises, and technical assistance from The Elections Group allowed election administrators, elected officials, and cybersecurity professionals to collaborate and demonstrated that such collaboration is beneficial for all participants.

Support for cybersecurity capacity building for state and local election administrators

2020 witnessed a groundbreaking election accompanied by a global pandemic, the highest voter turnout in American history, and high levels of misinformation and disinformation targeting voters, election administrators, and election systems. Each of these dynamics taken individually would present a considerable challenge for election administrators. When occurring simultaneously with cybersecurity threats, they created historic hurdles.

> *"It's outside of [election administrators'] comfort zone to discuss security . . . can compete with their main goals, or slow them down. . . . We also have to realize that these people have a logistics job to do as well."*

Interviewees pointed to a persistent lack of understanding of cybersecurity by election administrators, especially those from small to medium jurisdictions without technical capacity and human capital. Many election administrators entered the field prior to the evolution of election cybersecurity. As well, many elections offices are already understaffed and over worked, further diminishing their capacity to become cybersecurity experts. Larger election jurisdictions with the resources for dedicated information technology and cybersecurity personnel often still struggle to train local election staff on cyberhygiene and best practices in the field.

Practical tools applicable to on the ground needs of election administrators

In 2020, many state legislatures and election jurisdictions sought to ensure voters' safe access to the franchise in the midst of COVID-19. State laws and regulations shifted rapidly to expand absentee voting, voting centers, vote by mail, and early voting. Many were implemented with little lead time before the election. This expansion increased potential points of entry for bad actors into various state and local election databases, voter registration systems, and computer networks.

CISA produced guides that outlined considerations for election administrators in the midst of rapid-fire changes to state election law. However, CISA did not provide specific advice or step-by-step implementation guides for election administrators.

Simultaneously, calls for election audits were also increasing, particularly in 2020. Many election administrators, even those from larger jurisdictions with relatively more resources, felt overwhelmed by the sheer scale of considerations that accompanied the 2020 elections. Many struggled with how to prioritize a laundry list of concerns, last-minute election policy changes, and the scope of communications needs associated with such a high-priority election. Election administrators contending with multiple priorities recounted a need for detailed and directive advice on where to start to shore up and protect their election and voter registration systems. This challenge is magnified for small to medium-size election jurisdictions, which have fewer staff and resources to devote to cybersecurity.

> *"How do we implement the advice out there for small and medium counties and prioritize it for local election administrators? They've got no one to help implement the .gov domain, for example, and have no idea where to start. We need to start with what are the five most important things to do to manage our risk now?"*

Resources described as most relevant are those that focus on direct application in the field and outline where election administrators should start in their cybersecurity preparedness efforts. An example of this is the Center for Internet Security's cybersecurity prioritization guide. Similarly, interviewees pointed to the usefulness of step-by-step resources and implementation guides such as the 'Knowing It's Right' toolkit and scenario planning exercises.

Tools and trainings that focused on practical implementation and real-time scenarios in election administration and crisis communications were described as directly responsive to real needs. From Tabletop exercises to train the trainer modules to the National Governors' Association's crisis communications playbook to the Center for Internet Security guides on how to prioritize competing cyberhygiene needs, interviewees favored resources that were concrete and quickly applicable.

Investments that demonstrate proof of concept

For multiple reasons, it can be difficult for government to develop new innovations or tools in election cybersecurity. Government can however play a role in taking concepts that have been proven in a small number of jurisdictions and bring those to a much larger audience. Democracy Fund supported projects such as the Belfer Center's train the trainer modules and the Center for Internet Security checklists on cybersecurity were seen as good examples of bringing best practices to scale.

The open source risk limiting audit tool conceived by VotingWorks in partnership with CISA called "Arlo" was cited as a potentially scalable resource where government could now take on the lead role. However, some interviewees felt that Arlo may present hurdles because of the need for technical support for most jurisdictions to make use of the tool.

What investments were adopted by government, what are their characteristics, and how stable is continued government adoption?

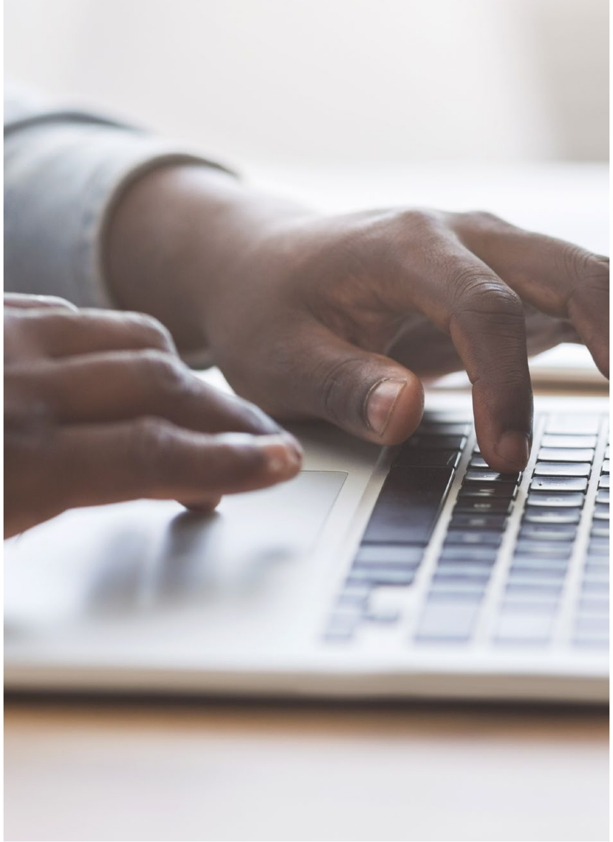
Government can adopt tools developed by Democracy Fund supported initiatives in multiple ways, and in so doing help bring these tools to scale. Two primary methods of adoption were highlighted in our interviews:

- Multiple local or state governments or election jurisdictions take advantage of best practices or instructional resources developed by grantees.
- The federal or a state government adopts approaches that have been previously managed and proven successful by a grantee.

Interviewees indicated some key characteristics for government adoption.

```
elif _operation == "MIRROR_Y":
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

    #selection at the end -add back the deselected mirror modifier object
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
    #mirror_ob.select = 0
```



Tools proven in multiple jurisdictions

Tools that were used in multiple jurisdictions demonstrated their replicability and were compelling for government adoption as a result. Examples of these include:

- The Belfer Center's Cybersecurity Tabletop exercises;
- The Center for Internet Security's Cybersecurity Checklist; and,
- Election Validation Project's "Knowing It's Right" resources.

Each of these were described as tools that are being widely implemented in the field. For example, CISA now has integrated the Belfer Center's Tabletop exercises into its cybersecurity support menu offered to election jurisdictions nationwide.

Tools solved a problem that government understood

Interviewees pointed to a persistent historic lack of coordination between federal agencies and state or local government with regard to election administration. The lack of federal control over election administration combined with CISA's limited scope[10] effectively require voluntary agreement on the part of state and local election officials to collaborate and share information with CISA and other federal agencies. In the United States' form of government where roles on a whole range of issues are differentiated between federal, state and local governments, government leaders are well aware of the need to build cross level cooperation to solve complex problems.

The National Governors' Association Policy Academy planning sessions, the Belfer Center's Tabletop exercises, and technical assistance from The Elections Group all facilitate officials from different levels of government working together with cybersecurity experts.

Government adoption occurred after philanthropy and nonprofit partners assumed initial risk to establish proof of concept

Interviewees pointed to the importance of piloting cybersecurity innovations at the local level. This allows for adjustments to strategies based on real world experience before attempting to go to scale. However, while local government can be a good petri dish for identifying needs and potentially replicable solutions, it generally lacks funds for testing unproven innovations and may lack the expertise to identify and test new approaches. Thus, Democracy Fund's willingness to invest in new endeavors and nonprofit partners' willingness to take on risk in administering projects that may not work are essential to creating innovation in the election cybersecurity field.

[10] CISA's mandate is to address jurisdictions' cybersecurity basic resiliency needs without significant operational oversight over election administrators.

Interviewees identified at least two reasons why nonprofits and philanthropy may be better positioned to initiate innovation. First, is monetary risk. Operating on limited budgets, local and even state governments generally do not have funds available that they can use to try out new technologies. They need to know that a tool has worked for similar jurisdictions before spending public dollars. When philanthropy invests funds, it can financially “afford to fail.” As one interviewee noted:

> *“I think there’s a flexibility in the nonprofit world. You’re not using tax dollars . . . so that innovation to find jurisdictions willing to experiment. You can use that technical expertise to come up with solutions . . . and have the nonprofit sector help the government sector engage. It’s important to use the flexibility of the philanthropic sector to support that innovation: you’re more likely to find pilot jurisdictions if they’re not bearing out the cost. . . . In general, that’s a much faster route to piloting and ultimate adoption.”*

Second is reputational risk. Government spending is generally subject to heavy scrutiny. Budgets are public and elected officials can be undone quickly by the perception of misuse of funds or scandal. This can make it difficult for government leaders or agencies to pioneer new approaches. Nonprofits funded by philanthropic dollars and working in collaboration with government, can help ameliorate these concerns. One former government official explained:

> *“There’s got to be trust that the innovation doesn’t blow up in [your] face – when [philanthropy] is willing to pilot it and someone can be an ambassador, that’s nice.”*

Some interviewees noted that this up-front philanthropy supported risk taking can also help drive market forces. Gathering a critical mass of state or local jurisdictions to pilot new programs or innovations can demonstrate to vendors a sufficiently robust market to justify continued investment.

Tools need to be perceived as nonpartisan

The expanded role of CISA in 2018 provided focus to the federal government’s response to cybersecurity threats targeting the nation’s infrastructure. At the height of the COVID-19 pandemic in 2020, many states were adopting changes in election laws that expanded voter access. This coincided with new tools that allowed for broader use of online voter registration and mail in ballot applications, remote access for election officials to voter databases, and other technologies to make it possible to run

[11] See: https://www.washingtonpost.com/opinions/christopher-krebs-trump-election-wasnt-hacked/2020/12/01/88da94a0-340f-11eb-8d38-6aea1adb3839_story.html

elections during a global pandemic. This created the potential for new election security threats and CISA responded with nonpartisan support offerings to state and local election administrators.

The agency had a newly expanded mission, and its leadership was generally nonpartisan in its approach to election administration. As such, it developed resources and cybersecurity tools for local and state election offices to be responsive to the cybersecurity threats most likely to occur as a result of the expansion of online registration, vote by mail, early voting, election centers and drop boxes that occurred across the country. Because of the nonpartisan nature of both CISA and the Democracy Fund supported initiatives, there was a positive working relationship between CISA and many of Democracy Fund's grantees.

Observers we interviewed noted that the newness of the agency's expanded mission and Trump's focus on the pandemic meant that CISA went largely unnoticed and uncontested in its nonpartisan election security efforts. While Trump was speaking out against expanded voting by mail, CISA was supporting states in ensuring the security of vote by mail efforts. While Trump declared inaccurately that there was massive fraud in the election, CISA's director Kris Krebs called the election the most secure in American history. Trump fired Krebs by tweet on November 17th, 2020.[12]

Ultimately, for cybersecurity tools and initiatives to go to scale, they need to be seen as nonpartisan so that they can be used in multiple states and across many local jurisdictions. There is a history of nonpartisanship in both election administration and federal responses to cybersecurity issues. The Trump White House put much of that nonpartisan tradition at risk and created a toxic environment where any perception of partisanship can doom even the most basic of positive working relations. Thus, it is even more important that initiatives and tool implementation embrace nonpartisanship and are available to every official who wants to make elections run fairly and securely. Otherwise, government's leeriness of anything perceived as partisan could lead to important improvements not being adopted.

> *"Government is risk averse in the current political environment – they feel better following up on some strands outlined by academics, nonprofits, and philanthropies . . . because they're so nervous [about] being partisan."*

Continued and increased government adoption is not ensured

While government adoption of tools supported by Democracy Fund has been broad, it is not yet clear how durable this adoption is. Two factors were elevated as creating concerns for interviewees on sustained and expanded government adoption.

[12] See: https://www.washingtonpost.com/opinions/christopher-krebs-trump-election-wasnt-hacked/2020/12/01/88da94a0-340f-11eb-8d38-6aea1adb3839_story.html

First is the threat to adoption due to the increased politicization of election administration.

“Certainly, there are things happening at the state level in reaction to conspiracy theories. Things that require funding and are unnecessary are sometimes taking away funding from other key needs, such as post-election audits. Funding for audits of elections is so important. Funding for audits that aren’t legitimate isn’t as helpful.”

Second are concerns about the commitment to sustained cybersecurity funding, at both the federal and state level. This opinion was shared by election officials from both parties.

“Another perennial challenge is the level of funding for cybersecurity. We don’t fund elections enough anyway, and [cybersecurity preparedness] makes elections more expensive.”

Several interviewees highlighted that state legislatures commonly do not understand the need for election cybersecurity funding.

“Continued funding for cybersecurity needs and programs needs is important, but not always understood by state legislators – that underscores the need for election officials . . . to ask for sustained funding.”

As a result, only a small number of states, including Illinois, Michigan, Colorado, Pennsylvania, Wisconsin, and New Jersey have consistent designated cybersecurity support available to local election administrators. Federal funding for cybersecurity is seen by interviewees as similarly fickle and unreliable.

"There's never going to be enough [cybersecurity] funding from the federal government. It's the reality."

"We get these chunks of funding, and then hear from the federal government, why aren't you spending it? Our answer is, 'Because I don't when I'm going to get another chunk of money.' If I know I have a steady funding source, I could do a lot more and make a long-term plan."

Overarching Concerns

Interviewees were proud of the progress on cybersecurity analysis and capacity built over the last five years. However, interviewees also raised two key concerns about the capacity and resilience of the field in the face of mounting challenges.

The scale of MDM threatens to reverse advances

Interviewees were concerned about the rise of MDM and its implications for continued mistrust in the American election system and election administrators. There was unanimous sentiment that MDM significantly increased in the lead up to the 2020 election, and never really subsided after the election.

> *“[Bad actors] are trying to get in . . . as we moved towards 2020, we were realizing how much MDM was out there, [which is] easier for bad actors to manipulate.”*

False assertions about reportedly “lost” ballots, fraudulent ballot drop boxes, and other fact-free conspiracies raise doubts among the public. Voter-centered policies such as expanded access to vote-by-mail, absentee ballots, ballot drop boxes, and voting centers are the result of hard-fought battles by election administrators and voting rights advocates to make voting easier and more convenient. Misinformation raises baseless questions about the integrity of these pro-voter and pro-democracy tools, threatening to undo advances.

> *“The Big Lie is coming to push up against improvements in expanded voting access and convenience in some states.”*

Respondents did not know what to specifically do about the widespread misinformation but agreed on the need for a national and perhaps international mobilization to counteract its effects.

Complacency on cybersecurity after a secure 2020 election

Interviewees are concerned about cybersecurity remaining a priority, especially for those in government and legislative appropriations positions. The steps taken to increase cybersecurity ahead of the 2020 elections, reduced threats and the election was heralded for its security. Interviewees worried that this success could paradoxically lead to less attention and funding.

> *“Some may say, ‘2020 was secure, so we can take our foot off the gas.’ Yes, it was safe because you were paying attention, so now’s the time to double down.”*

Persistent and emerging gaps in the field

Interviewees pointed to an array of gaps that characterize the field. These are tied to a combination of attacks on the field, the politicization of election administration, the changing role of audits, and ongoing funding gaps.

Threats are growing at the intersection of technology, cybersecurity, and MDM

Election administrators are contending with simultaneous threats ranging from physical violence, rapidly-shifting state election laws, high burnout and attrition after the 2020 elections, a constant flow of MDM, as well as increased scrutiny spurred by inaccurate accusations that the 2020 election was decided incorrectly. Seven states have already created or increased criminal or financial penalties for election officials in 2021.[12] Election administrators are being pulled in multiple directions as the stakes associated with performing their jobs increase and the resources available to them remain level at best or diminished.

> *“When the loser doesn’t concede, and so many people haven’t put [the] 2020 [election] to bed—the physical threats to election officials continue.”*

Interviewees pointed to an increasing volume of phishing, ransomware, and other daily cyberthreats that constantly threaten to engulf election worker.

> *“The bad actors have plenty of money and plenty of resources. You’re like wow, I’m just some guy. I don’t have the resources to stay on top of it.”*

Uncertainty on how to create accountability for social media platforms

Interviewees described being at a loss on how to tackle online MDM effectively given its scale and reach. It has become clear that many social media platforms’ business models benefit from accelerating the clicks and ad revenue generated by content that incites or angers the viewer, including MDM. This disincentivizes key large social media companies from removing statements that fuel conspiracy theories and lies about elections.

[12] Stateline, an initiative of The Pew Charitable Trusts, “Republican Officials Curb Authority of County, State Election Officials”, https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/07/28/republican-legislators-curb-authority-of-county-state-election-officials. Accessed 10.4.21.

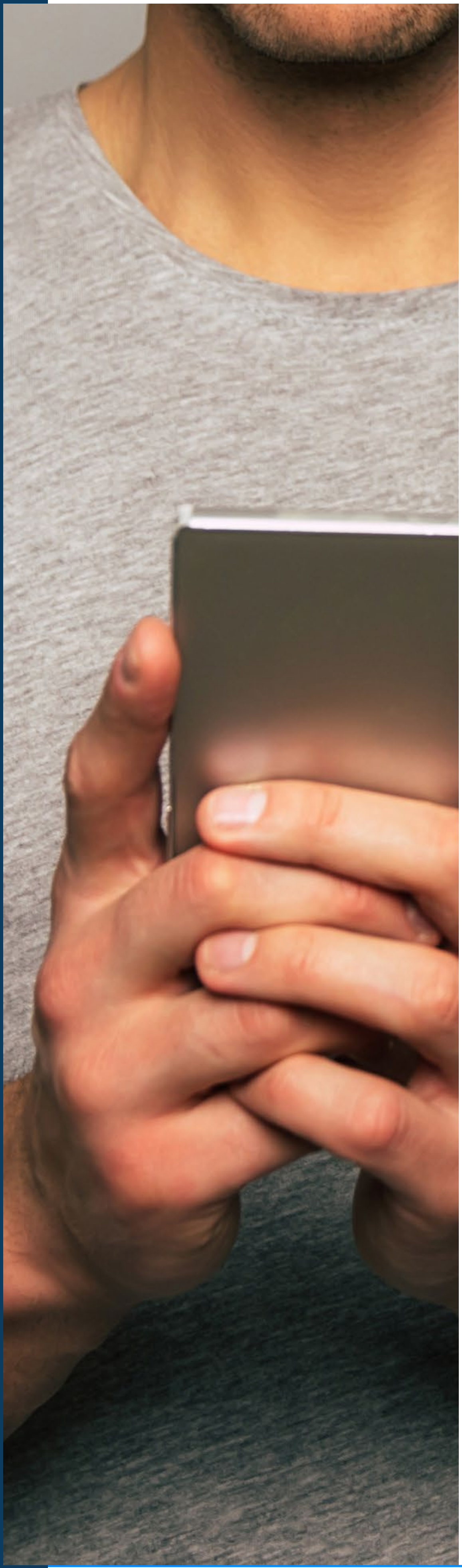
Interviewees cited a lack of accountability for social media companies as a central reason for the spread of MDM. Despite public announcements and policy changes by Facebook and Google/YouTube, before and after the 2020 elections, these large social media companies remained primary methods for spreading misinformation about the accuracy of the election through the end of 2020, and ultimately were a vehicle for organizers of the January 6th attack on Congress. Interviewees pointed to the need for a national multi-sector effort to address the proliferation of misinformation and disinformation regarding elections.

Current and former government officials we interviewed pointed to First Amendment concerns as a limiting factor on government taking a more active role cracking down on misinformation on social media platforms.

“CISA feels it’s tricky to step in on MDM, as they got some political blowback for being proactive in 2020 on this.”

Given this, many interviewees felt addressing the proliferation of elections MDM on social media will need to start with civil society organizations, academics, and philanthropic institutions. Such an effort will have to deal with government’s hesitance to use laws or regulations as part of the solution.

“The levers of action are much smaller for government, What are the appropriate levels and lanes for government? Who can do what?”



Expanded voting options increase entry points for cyberattacks

Many interviewees expressed concerns on the cybersecurity implications associated with the popularity of election laws designed to increase access and convenience for voters. Interviewees pointed to an urgent need to expand security practices and protections given the increased levels of access into voter databases and election computer systems.

Changes in state election law designed to increase voter access, that have been popular and crucial given COVID-19, have implications for cybersecurity. These can present more opportunities for public access to election systems and more use of those systems in new ways by election officials. This in turn opens cyber vulnerabilities. Interviewees raised potential cybersecurity concerns about:

- Voting centers which often use e-poll books and other tools to allow election workers to access voter databases, away from election administrators' offices;
- Electronic submission of absentee ballot requests (with the potential for malware and phishing); and,
- Public portals for voter registration, ballot tracking, and other steps in the voting process.

There is a potentially symbiotic relationship between disinformation and cybersecurity attacks

Interviewees described a tsunami of MDM that portrays election systems as vulnerable and corrupt. These lies have the potential to spur cyberattacks targeting those same election systems. Similarly, foreign or domestic actors could coordinate cyberattacks with MDM efforts to decrease public confidence in election systems. MDM raises persistent questions about the validity of American elections and the integrity of those who administer them. These unfounded assertions create a feedback loop that would be even more dangerous if coordinated with a cyberattack.

"If your election cybersecurity system isn't strong enough, then you have a situation where you're more vulnerable to MDM and have more threats for outside actors to exploit them."

"If I was a funder, I'd encourage folks to invest in monitoring supply and demand of MDM – take it off of election administrators' plate. Election officials are spending much-needed financial resources on social media monitoring, which they can ill-afford."

Tracking and responding to MDM is also time consuming. Adding it as a responsibility for local election administrators can take time away from running elections.

"Folks are trying to figure out how to answer calls and emails from voters who've heard the Big Lie and are seeking reassurance or to tell election administrators how to address the Big Lie. These are resources spent on responding to the Big Lie, but they're resources taken away from election administration, from audits."

Need for more technical assistance

Many interviewees reported that election administrators struggle to stay updated on cybersecurity threats and vulnerabilities. As well, many are simply not aware of best practices in addressing cybersecurity vulnerabilities. Technical assistance and information on cybersecurity best practices remain an urgent gap for many election administrators. This is certainly true for election administrators in medium size or smaller jurisdictions, but interviewees also perceived a need for ongoing technical assistance for larger jurisdictions given the continuing changes in the field, including: voter access, staff turnover, technologies, threats, and the interactions between cyber threats and MDM.

“We need more technical assistance available on the ground. Some of it is cyber, some operational. The idea that right now, all 8800 local election jurisdictions have to be competent across multiple competencies – there’s just no way to scale that competency all over the place.”

“The threats are real. Elections officials are operating in an environment where human fallibility feels dangerous, and [they] are chronically short-staffed.”

The politicization of election administration

While interviewees pointed to the importance of the professionalism and nonpartisan conduct of local and state election officials nationwide in 2020, many worried about the demise of this code of conduct in the wake of organized misinformation. As attitudes toward election integrity and operations increasingly fall along partisan lines in American political discourse, many interviewees were anxious about the impact on fair and nonpartisan elections.

“I’m worried about political tradecraft impacting the work.”

A plurality of interviewees expressed concerns that organized misinformation is politicizing election administrators and creating opportunities for partisan election administrators to implement elections according to partisan bias. Paradoxically, this could reinforce claims of rigged elections if nonpartisan election officials are replaced.

> *"You're going to start seeing people running for election administrator positions that are much more interested in following a political perspective, security will be the reason they'll give for making changes, and I'm not sure it's going to be warranted, especially around politics and procedures."*

This was a dynamic for which interviewees struggled to offer constructive solutions.

Growth in post-election audits fuels need for standards and support for election administrators

Interviewees felt there was no one-size fits all approach for post-election audits and RLAs. Instead, these tools should be adapted to state contexts and needs. Many respondents felt piloting audits at the state level could create an on-ramp for local election administrators to learn about and begin implementing audits. Respondents noted the public's lack of understanding of what an audit actually does. Interviewees pointed to the need for a comprehensive and well-resourced public messaging strategy on election audits. Most felt there was considerable value to making the case to the general public on the important quality control role and checks provided by audits. Audits were perceived by several interviewees as crucial tools to educate the public on the process and mechanics of elections and demonstrate the checks and balances included in our election systems.

Resources, training, and technical support on post-election audits including RLAs were perceived as essential for continued philanthropic investments. Audits and RLAs in particular need to be accompanied by implementation support for election administrators, who often have no idea where to start.

There is a fair amount of variation in election audit design and implementation, and it can be difficult for election administrators to identify the best practices. Many interviewees pointed to the high stakes of post-election audits. If done incorrectly, they can further diminish public trust in elections systems and processes. While the Brennan Center[13] and the Center for Democracy and Technology have outlined a set of key characteristics[14] of an effective post-election audit, there is no mechanism to ensure the adoption of these elements across varied election jurisdictions.

[13] See an example at: "Risk Limiting Audit Methods in the State of Rhode Island," https://www.brennancenter.org/our-work/research-reports/pilot-implementation-study-risk-limiting-audit-methods-state-rhode-island Accessed November 15, 2022.

[14] Outlined in a recent Center for Democracy and Technology report on what makes a 'good' post-election audit in the context of a proliferation of post-election audits after the 2020 elections and the long 'forensic audit' conducted in Maricopa County, AZ. https://cdt.org/insights/we-need-a-way-to-distinguish-good-post-election-audits-from-bad-ones/ Accessed 9.21.2021.

“People have recognized that there need to be standards to outline post-election tabulation audits. . . . Elections officials need to systematize their procedures.”

Federal funding for election cybersecurity is inconsistent and insufficient

In 2018, the federal government funded state cybersecurity programs through appropriations via the Help America Vote Act (HAVA) infrastructure. Congress also began to appropriate more resources for CISA in anticipation of the 2018 midterm elections and the 2020 Presidential elections. This amounted to an increase in available resources for cybersecurity preparedness. However, most interviewees, including current and former federal officials, saw this funding as unlikely to be sustained and insufficient overall. Philanthropic funds to support state and local cybersecurity preparedness continue to be viewed by interviewees as crucial.

Lack of funding, particularly consistent federal funding, remains a considerable challenge for election administrators and for innovators in the election cybersecurity space. This gap impacts election administrators’ ability to plan and budget for the recurring expenses of bolstering election cybersecurity. Interviewees felt there likely would not in the foreseeable future be enough federal funding for election cybersecurity. Interviewees were also pessimistic about the availability of sufficient state funds in most places.

Election officials we interviewed pointed to this ‘boom or bust’ federal funding cycle as limiting their ability to plan and effectively allocate funds for election security. Software upgrades and IT professionals, for example, are not one-time expenses.

“I hope there’s more funding, or at least consistent funding. We don’t need $10 million, give us $1 million [consistently] and we can plan.”

Interviewees felt that the election cybersecurity field remains in constant flux due to the lack of consistent government funding, the proliferation of cybersecurity threats and attacks, and misinformation and disinformation targeting the trustworthiness of American elections, election systems, and election officials. Constant threats require constant and predictable resources.

Need for message development and communications training for election officials

For local and national media, state and local election officials are often a primary source on election security (both MDM and cybersecurity). But most election officials lack the training to be effective spokespeople. Being able to explain how elections are already safeguarded can help build public confidence in elections and dispel lies.

> *"Election officials are terrible messengers at sharing their story—we need to support them to tell their story better and amplify their message."*

A speakers bureau of credible spokespeople could help to explain how cybersecurity works and address election-related MDM in print/broadcast channels as well as on social media. Spokespeople need to be media trained, ideally be bipartisan, and represent a diverse cross-section of geographies and political orientations. Ideally, these individuals would also be current or former election administrators themselves.

Lack of philanthropic support

The needs of the field exceed Democracy Fund's giving potential. Other funders have been less interested in the nuts and bolts of building public trust for elections generally and supporting things like election cybersecurity and post-election audits specifically. This is likely the result of at least a couple of factors: (1) other elections funding opportunities are easier to understand and come with communities of donors already working in the space, and (2) funders perceive that in our democracy, government should be funding the basics of election administration.

Thus, it will take a bit of work to get additional funders engaged. This may include identifying discrete projects and targeting initiatives at a proof-of-concept phase that are likely to be ultimately adopted by government. Many funders are particularly concerned about MDM, so this may present an opportunity for funders and experts to convene to lay out a strategy for 2022.

Funders may also be interested in building a communications campaign to push back nationally on the constant lies about election integrity.

A well-designed communications campaign could educate the public on just how secure and transparent elections are. It could also demystify election administration and engage in communication on platforms where people are currently being fed disinformation. It could also be done in conjunction with an effort to hold social media companies responsible for more aggressively removing MDM and its purveyors from their platforms.

CONCLUSION

The election security field has taken significant steps forward over the last five years. This facilitated a largely secure election in 2020, when election security is judged from the perspective of diminished cyberthreats and cyberattacks, as well as when considering the growth of tools to support election officials and facilitate high quality election audits. This should be considered a major victory.

However, threats continue. Some of these threats are familiar, including ongoing efforts to hack into election systems as well as attempts to manipulate public opinion through mass disinformation campaigns online. Other threats are new and are effectively attacks on the legitimacy of our election infrastructure and administrators.

Both political actors and profit-making media resources have seen fit to attempt to delegitimize a fundamental element of American democracy, our decentralized election administration system. This has created a level of physical threat not seen in American elections possibly since the end of the denial of African Americans' right to vote. While the most extreme example of this introduction of violence was the attack on Congress on January 6, 2021, election officials continue to receive violent threats across the country.

When addressing public trust in elections, these new hazards must be considered in tandem with efforts to maintain cybersecurity and develop effective tools for election officials. Solutions will require breaking new ground at the intersection of emerging and older threats.

Fernandez Advisors // 2021

https://www.fernandezadvisors.net