Congressional Research Service
Informing the legislative debate since 1914

COVID-19: Remote Voting Trends and the Election Infrastructure Subsector

June 10, 2020

Congressional Research Service
https://crsreports.congress.gov
R46407

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R46407

June 10, 2020

Brian E. Humphreys
Analyst in Science and Technology Policy

COVID-19: Remote Voting Trends and the Election Infrastructure Subsector

The Department of Homeland Security (DHS) designated the systems and assets used to administer elections as a critical infrastructure subsector in 2017. The federal elections policy framework—including infrastructure protection—has generally assumed in-person voting at official polling places as the primary means of elections administration. Therefore, infrastructure security efforts have focused on reducing risk to existing systems and assets such as voter registration databases, voting machines, polling places, and elections storage facilities. However, recent elections cycles have witnessed increased use of alternatives to in-person voting.

Public health concerns about the Coronavirus Disease 2019 (COVID-19) pandemic have accelerated consideration of remote voting options as many voters have sought to avoid the possible health risks of crowded polling places. Elections authorities have invested in new physical and cyber infrastructures to reduce in-person interactions throughout all phases of the election cycle, including but not limited to the casting of ballots on Election Day. These efforts have focused on universal mail voting—the only form of remote voting in wide use. (Some states provide for electronic marking and return of ballots in certain limited cases.)

The rapid pursuit of expanded mail voting and development of accompanying infrastructures during the pandemic has presented near-term technical, logistical, administrative, and security challenges to the election infrastructure subsector (EIS). State and local preparedness to transition to mail voting varies widely. Several states already use universal mail voting for elections. However, most states still rely primarily upon in-person voting, with varying eligibility standards for absentee ballot access. Elections experts have cautioned that introduction of universal mail voting is typically a multi-year process even in the most favorable circumstances, as it involves elements with long lead times, such as legislative changes, contracting, manufacturing, property acquisitions, interagency coordination, and systems testing.

Emergency mail voting initiatives contend with a changed security environment. EIS coordination bodies have reported an increase in cyberattacks against state and local government agencies' computer systems, exploiting vulnerabilities created by the sudden increase in telework. In March, DHS issued an alert encouraging EIS stakeholders "to adopt a heightened state of cybersecurity" due to targeting of virtual private networks often used for telework. These conditions may impose additional challenges. Closures and restrictions, shortages of key goods, or illness of essential workers may disrupt efforts to implement mail voting. In addition, elections authorities may need to expand the physical footprint of ballot processing and other facilities to allow for social distancing, making it more difficult to secure these facilities. Federal agencies and official EIS coordination bodies have responded by providing a number of new informational products that describe emerging vulnerabilities of the EIS and best practices for mail voting, in addition to existing services.

Since the onset of the COVID-19 crisis, Congress has provided additional funds to states for election administration. The Coronavirus Aid, Relief, and Economic Security (CARES) Act (P.L. 116-136) provided an emergency supplemental appropriation of $400 million to help state elections authorities "prevent, prepare for, and respond to coronavirus ... ," but guidance from the Election Assistance Commission (EAC), an independent agency, imposes limitations on the use of these funds for emergency expansion of mail voting. States may use certain funds previously awarded under the Help America Vote Act (HAVA) of 2002 (P.L. 107-252, 52 U.S.C. §§20901-21145) for this purpose. DHS required states applying for certain homeland security grants to include election security activities in their proposals for FY2021 funding. The period of performance for these grants begins on September 1, 2020.

It is difficult to predict how emergency measures to aid balloting during a pandemic will affect longer-term structural changes within the EIS. Elections authorities may choose to retain or expand remote voting options in subsequent elections cycles for a variety of reasons, including changing public expectations, a desire to lower costs or increase resilience, and availability of emerging technologies. Although legislative proposals to expand remote voting introduced during the pandemic have focused on mail voting, Congress has demonstrated longstanding interest in electronic voting methods and technologies using the internet. In the early 2000s, Congress mandated pilot programs and government studies to develop the policy and technological frameworks for adoption of internet voting. Federal agencies oversaw a number of small-scale pilots—primarily targeting military and overseas voters—but these did not lead to wide scale adoption of emerging technologies for remote voting. Internet-based online voting systems have yet to win wide acceptance in the United States.

However, some elections authorities continue to show interest in internet voting technology that private sector firms are developing. Expansion of internet voting, should it occur, may raise new policy issues for Congress.

Contents

Figures

Tables

Contacts

Introduction

The Department of Homeland Security (DHS) designated the systems and assets used to administer elections as a critical infrastructure subsector in 2017. DHS defines critical infrastructure as "the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety."[1] The federal elections policy framework—including infrastructure protection—has generally assumed in-person voting at official polling places as the primary means of elections administration, excepting limited numbers of expatriates and service members deployed overseas.[2] However, recent elections cycles have witnessed increased use of remote voting options, and several states have already adopted mail voting as their default option.

Public health concerns about the Coronavirus Disease (COVID-19) pandemic have accelerated consideration of remote voting options during the 2020 election cycle, as many voters have sought to avoid the possible health risks of crowded polling places.[3] These efforts have focused on universal mail voting—the only form of remote voting in wide use—although some states provide for electronic marking and return of ballots in certain limited cases. The rapid pursuit of expanded mail voting and the development of accompanying infrastructures—both paper-based and digital—presents technical, logistical, administrative, and security challenges to election infrastructure subsector (EIS) stakeholders.

This report describes the development of remote voting infrastructure in the United States, and the planning and policy challenges that rapid expansion of mail voting may raise within the EIS. Additionally, it contains a section on internet voting. Although internet voting remains a minor element of election infrastructure and administration during the 2020 cycle, Congress has historically demonstrated interest in this technology. Likewise, some state and local elections authorities have conducted small-scale demonstration projects and may expand internet voting to certain voters, including those affected by the pandemic.[4] Future technological breakthroughs or high profile failures of other modes of election administration might serve to increase public interest in internet voting. Furthermore, a number of private firms continue to invest in and promote the technology to election authorities. Expansion of internet voting beyond small-scale applications, should it occur, may raise new policy issues for Congress.

Scope of Report and Key Terms

Federal, state, and local investments in election infrastructure in response to the COVID-19 pandemic and longer-term trends may change the structure of the EIS itself. This report focuses on structural change within the EIS as stakeholders adapt to a rapidly changing environment. As used in this report, structural change refers broadly to incorporation of new systems and assets into election infrastructure, changes in roles and relationships between stakeholders, legislative

[1] Cybersecurity and Infrastructure Security Agency (CISA), "Critical Infrastructure Sectors," https://www.cisa.gov/critical-infrastructure-sectors.

[2] For example, an update to voluntary federal certification requirements for voting systems (in the comment period as of the date of this report) specifically excludes remote ballot marking systems. See Election Assistance Commission, Technical Guidelines Development Committee, *Voluntary Voting System Guidelines Version 2.0 Requirements*, February 29, 2020, p. 13.

[3] See, for example, Jeff Barker and Emily Opilo, "An Election During a Pandemic? There's Never Been One Like Tuesday's Baltimore-Area Congressional Contest," *The Baltimore Sun*, April 26, 2020.

[4] David E. Sanger, Nicole Perlroth, and Matthew Rosenburg, "Amid Pandemic and Upheaval, New Cyberthreats to the Presidential Election," *New York Times*, June 9, 2020.

changes, and widespread adoption of new modes of election administration and operational procedures within the EIS.

For example, state and local governments may invest in new physical or cyber systems and assets to handle certain election administration functions, such as bulk processing of mail-in ballots and computerized tracking systems. Congress and state legislatures may pass legislation and use appropriations to either limit or expand use of these technologies and methods. Greater reliance on mail would likely increase reliance upon the U.S. Postal Service (USPS), which is designated as critical infrastructure but is not part of the EIS. However, it might decrease reliance upon in-person voting infrastructure, such as polling places and voting machines, leading to changes in election administration. Such changes may present new challenges to the infrastructure protection and resilience enterprise within the EIS.

Federal election policy is the focus of this report only inasmuch as it relates to structural changes within the EIS. Readers with general interest in the current legislative debates over election policy issues should consult CRS reports that examine these topics in detail.[5] Likewise, this report does not assess comparative risks of different voting systems. For a general overview of vote-by-mail policy considerations and a summary of security issues, see CRS In Focus IF11477, *Early Voting and Mail Voting: Overview & Issues for Congress*, by Sarah J. Eckman and Karen L. Shanton.

Table 1 defines three key terms used in this report, as their meaning and usage may vary by context: remote voting; mail voting; and internet voting.

Table 1. Key Terms

Term	Definition
Remote Voting	Casting a ballot "outside of a polling place or election official's office." Sometimes referred to as absentee voting.
Mail Voting	Remote voting using a printed-paper ballot deposited in the mail or at a designated drop-box location for elections authorities. Voters may receive their ballots in paper form via mail or electronic form via email or web browser. In the latter case, voters print and mark ballots themselves.
Internet Voting	Remote voting using an electronic ballot delivered to the voter, marked, and returned to an official vote counting location via the internet using a web browser or smartphone app on a personal computing device.

Sources: CRS, National Council of State Legislatures (NCSL), and Smartmatic.

Policy Background and Issues

The EIS is part of a federal critical infrastructure protection and resilience framework first outlined during the Clinton Administration and subsequently expanded and elaborated over multiple presidential administrations. The framework, currently established under DHS auspices,

[5] Some recent reports include CRS Legal Sidebar LSB10470, *Election 2020 and the COVID-19 Pandemic: Legal Issues in Absentee and All-Mail Voting*, by L. Paige Whitaker; CRS In Focus IF11456, *Disrupted Federal Elections: Policy Issues for Congress*, by R. Sam Garrett; CRS Report R46146, *Campaign and Election Security Policy: Overview and Recent Developments for Congress*, coordinated by R. Sam Garrett; and CRS In Focus IF11286, *Election Security: Federal Funding for Securing Election Systems*, by Karen L. Shanton.

is largely voluntary. Its defining features are coordination bodies that link government agencies, private sector stakeholders, and member-supported information sharing organizations across 16 officially recognized sectors that encompass diverse areas of the economy, government, and public safety and security.[6]

The Cybersecurity and Infrastructure Security Agency (CISA), an operational component of DHS, has primary responsibility for leading sector coordination bodies. (In several cases, the framework designates other federal agencies as sector-specific leads based on their customary missions and relevant expertise in a given critical infrastructure sector.) In addition to supporting coordination and information sharing organizations and activities, CISA provides infrastructure protection services, such as site assessments and computer network penetration testing. However, CISA does not assume direct responsibility for securing infrastructure owned and operated by private sector stakeholders or state and local government agencies.

The 2017 DHS critical infrastructure designation for election systems was intended to help reduce obstacles that election stakeholders faced in responding to foreign interference in the 2016 elections, such as a lack of timely information sharing about threats to election systems from hostile foreign governments or other malicious actors.[7] However, the designation did not anticipate a rapid transition of the subsector to remote voting systems in the context of a global pandemic occurring in an election year. Therefore, much of the effort to secure the subsector focused on reducing risk to existing infrastructure, such as voter registration databases, voting machines, polling places, and elections storage facilities.[8]

Many EIS stakeholders have since sought increased support for planning and policy efforts needed to expand remote voting at acceptable levels of risk. CISA, the Election Assistance Commission (EAC, an independent agency), and other relevant federal agencies have responded by providing informational products that describe best practices and emerging threats to the EIS.[9]

Federal Remote Voting Initiatives

Historically, federal remote voting initiatives have focused on expanding ballot access for uniformed service members, their families, and other Americans living overseas—a substantial number of voters, but a small percentage of the overall U.S. electorate.[10] The Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA), as amended, has been the primary legislative vehicle for federal remote voting initiatives since its passage in 1986.[11] The Department of

[6] See CRS Report R45809, *Critical Infrastructure: Emerging Trends and Policy Considerations for Congress*, by Brian E. Humphreys; and CRS Report R46146, *Campaign and Election Security Policy: Overview and Recent Developments for Congress*, coordinated by R. Sam Garrett.

[7] See CRS In Focus IF10677, *The Designation of Election Systems as Critical Infrastructure*, by Brian E. Humphreys.

[8] See DHS, "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," press release, January 6, 2017, https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

[9] For an overview of EAC organization and functions, see CRS Report R45770, *The U.S. Election Assistance Commission: Overview and Selected Issues for Congress*, by Karen L. Shanton.

[10] In its 2018 post-election report to Congress, the Federal Voter Assistance Program (FVAP) reported that 344,392 UOCAVA voters—about half of those who requested a ballot—voted that year. By contrast, the U.S. Census Bureau estimates that more than 122 million citizens voted in the 2018 midterm elections. See FVAP, "FVAP Releases 2018 Post-Election Report to Congress," https://www.fvap.gov/info/news/2019/7/31/fvap-releases-2018-post-election-report-to-congress, and U.S. Census Bureau, "Voting and Registration in the Election of November 2018," https://www.census.gov/data/tables/time-series/demo/voting-and-registration/p20-583.html.

[11] 52 U.S.C. §§20301 et seq. For a full overview of UOCAVA including internet voting initiatives, see CRS Report

Defense (DOD), through its Federal Voting Assistance Program (FVAP), has played a leading role in federal remote voting initiatives and associated technology development in coordination with the EAC, other federal agencies, and state and local elections authorities.[12]

Legislation in the 116th Congress to Expand Mail Voting Systems

Several bills introduced in the 116th Congress would expand mail-voting options. A proposed amendment (S. 1397) to the Help America Vote Act of 2002 (P.L. 107-252) introduced in 2019 would require the EAC to create a national federal write-in absentee ballot and make it available on the internet in a printable format to individuals affected by certain disasters or health emergencies. The Vote by Mail Act of 2019 (S. 26 and H.R. 92) would require states to allow voting in federal elections to be by mail without additional conditions or requirements, except a deadline for returning the ballot. Additionally, it would require the U.S. Postal Service to carry ballots mailed by a state expeditiously and free of charge.

After the onset of the COVID-19 emergency, Members introduced several more bills. The Resilient Elections During Quarantines and Natural Disasters Act of 2020 (S. 3440 and H.R. 6202) would require each state and jurisdiction to create and publish a plan to operate its federal elections if a significant number of voters or poll workers were quarantined due to COVID-19. Plans must (1) permit registered voters to submit online requests for absentee ballots and vote in federal elections by mail, and (2) extend vote-by-mail deadlines if COVID-19 disrupts postal service. The Natural Disaster and Emergency Ballot Act of 2020 (S. 3529) would require states to permit registered voters to submit online requests for absentee ballots and vote by mail or by drop-off location, among other provisions. It also contains provisions for a "cure process" that would require states to allow voters the opportunity to resolve discrepancies between a signature affixed to the return ballot mailer and a signature in official databases used for verification of voter identity and eligibility.[13] The American Coronavirus/COVID-19 Election Safety and Security (ACCESS) Act, passed in the House on May 15, 2020, as part of The Health and Economic Recovery Omnibus Emergency Solutions (HEROES) Act (H.R. 6800), contains provisions similar to those described above, among others.

Internet Voting

Congressional and DOD interest in using digital communications technology to serve UOCAVA voters more efficiently grew as internet adoption accelerated in the 1990s and the logistical difficulties in providing paper ballots to far-flung service members via conventional mail became apparent.[14] In December 2001, Congress mandated that DOD conduct an internet voting demonstration at a "statistically relevant" scale in time for the November 2002 elections.[15] In October 2002, Congress enacted HAVA, which established the EAC as an independent federal agency. HAVA mandated that the EAC provide a detailed report to Congress on internet voting

RS20764, *The Uniformed and Overseas Citizens Absentee Voting Act: Overview and Issues*, by R. Sam Garrett.

[12] Department of Defense, *Review of FVAP's Work Related to Remote Electronic Voting for the UOCAVA Program*, Washington, DC, December 15, 2015, p. 2.

[13] For more information, see CRS In Focus IF11456, *Disrupted Federal Elections: Policy Issues for Congress*, by R. Sam Garrett.

[14] See FVAP, *2010 Electronic Voting Support Wizard: Technology Pilot Program Report to Congress*, Washington, DC, July 2013, p. 2.

[15] The National Defense Authorization Act (NDAA) for Fiscal Year 2002 (P.L. 107-107). DOD exercised authorities granted under the legislation to cancel the project due to security concerns.

technologies and processes within 20 months of enactment. In 2004, Congress reiterated the original mandate for an internet demonstration project, but postponed implementation until EAC established electronic absentee voting guidelines to assist DOD.[16]

EAC had not established those guidelines before 2015, when Congress repealed its original requirement for a demonstration project.[17] Also in 2015, FVAP released its final report detailing findings of research and pilot programs—presenting them as a resource for state elections authorities seeking to pursue internet-voting solutions.[18] Broadly speaking, the body of research and testing undertaken to meet the congressional mandate between 2002 and 2015 found that electronic remote voting could be reasonably secure in the context of small-scale pilot studies in controlled environments. However, regulatory and technological hurdles, complicated by the U.S. state-based system of elections administration, imposed significant barriers to wider-scale adoption. Overcoming these would require a concerted policy and technology development effort by a broad array of elections stakeholders at every level of government and the private sector.[19]

The Military and Overseas Voter Empowerment (MOVE) Act of 2009 (a subtitle of P.L. 111-84) required states to allow eligible voters to receive ballots electronically. States have since made limited use of email, fax, and web portals to transmit blank ballots to UOCAVA voters under this act's provisions. Many states allow these voters to return completed ballots by email and fax, and several offer or have experimented with the use of web portals for this purpose.[20]

Remote Voting Infrastructure

Remote voting systems in use during the 2020 election cycle rely largely on paper ballots, since in most cases, electronic ballot return systems remain in the pilot phase or are available only to UOCAVA voters. Oregon, Washington, Colorado, Utah, and Hawaii currently use vote-by-mail as their primary means of election administration, and many other states have expanded eligibility for absentee mail-in ballots.[21] Vote-by-mail states may also have drop-box locations for voters who wish to hand deliver their ballots or otherwise avoid using the postal system for ballot return.

Even though state remote voting systems use paper mail-in ballots for most voters, they may also rely on automated electronic components and networked information systems to facilitate voter registration, ballot delivery to voters, ballot tracking, processing of ballots returned electronically or by mail, and updating of voter records. Some state elections systems combine elements of internet voting and paper-based ballots, delivering ballots electronically via email or web portal and then requiring voters to print out marked ballots and return them by mail. Therefore, elections authorities in many cases must integrate physical and digital media, communications networks,

[16] Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005 (P.L. 108-375).

[17] CRS Report RS20764, *The Uniformed and Overseas Citizens Absentee Voting Act: Overview and Issues,* by R. Sam Garrett, p. 11.

[18] Department of Defense, *Review of FVAP's Work Related to Remote Electronic Voting for the UOCAVA Program*, p. 16.

[19] Ibid., pp. 25-39.

[20] See FVAP, "How Voters Can Submit Their Ballot or FWAB Federal Write-in Absentee Ballot," https://www.fvap.gov/covid-19. Also, National Conference of State Legislatures (NCSL), "Electronic Transmission of Ballots," https://www.ncsl.org/research/elections-and-campaigns/Internet-voting.aspx.

[21] National Vote at Home Institute, *Vote at Home*, Policy and Research Guide, April 5, 2020.

and internet-based technologies into an elections system that can process ballots securely in a variety of different physical and digital formats.[22]

Although vote-by-mail is relatively simple in concept, implementing it on a large scale presents many complexities, and many states might have to process more ballots by mail than they have during previous election cycles.[23] State and local preparedness to transition to remote voting varies widely, and broader challenges across the government information technology (IT) sector—exacerbated by the COVID-19 pandemic—may complicate major initiatives to expand the cyber and physical infrastructure needed for remote voting. Supply chain disruptions, aging or outdated IT infrastructure, limited IT support resources, and competing priorities such as expansion of unemployment benefit processing may hinder many functions of governance—including elections administration.

Elections experts have cautioned that expansion of mail-in ballot access to the entire electorate is typically a multiyear process.[24] Even when implemented on an emergency basis, building vote-by-mail infrastructure requires elements with long lead times, such as legislative changes, contracting, manufacturing, property acquisitions, interagency coordination, and systems testing.[25] Elections experts note that seemingly simple tasks such as printing ballots, designing elections materials to comply with U.S. Postal Service guidelines, setting up secure drop-box locations and ballot storage facilities, opening returned envelopes, and verifying signatures may present significant procedural and logistical hurdles.[26] In addition, self-printed ballots may require manual processing because they are typically not machine-readable.

According to elections officials, states that have already implemented no-excuse and permanent absentee voting over multiple elections cycles are usually better positioned to transition to remote voting systems than states where absentee ballots have not been used widely.[27] Media reports indicate that the record number of requests for absentee ballots during the COVID-19 pandemic has led to lost, misprinted, misplaced, or misdirected ballots in some contests, which may lead to court challenges.[28] The nonprofit Brennan Center for Justice estimated in March 2020 that implementing universal vote-by-mail by November 2020 would cost the states between $982

[22] Technical Guidelines Development Committee, *Voluntary Voting System Guidelines Version 2.0 Requirements*, p. 12.

[23] See CRS Insight IN11356, *Mail Voting and COVID-19: Developments and Potential Challenges*, by Karen L. Shanton and Sarah J. Eckman.

[24] See interviews with elections officials online at EAC, "Voting by Mail/Absentee Voting," https://www.eac.gov/election-officials/voting-by-mail-absentee-voting; and CISA, EIS Government Coordinating Council (GCC) and Sector Coordinating Council (SCC) Joint COVID Working Group, *Electronic Ballot Delivery and Marking*, 2020, https://www.cisa.gov/sites/default/files/publications/e-ballot-delivery_and_marking_final_508_0.pdf, p. 1.

[25] See EAC, "GCC and SCC Resources," https://www.eac.gov/election-officials/voting-by-mail-absentee-voting.

[26] See EAC, "Voting by Mail/Absentee Voting" and "GCC and SCC Resources," https://www.eac.gov/election-officials/voting-by-mail-absentee-voting; and U.S. Postal Service, "Election Mail," https://about.usps.com/gov-services/election-mail/.

[27] EAC, ibid.

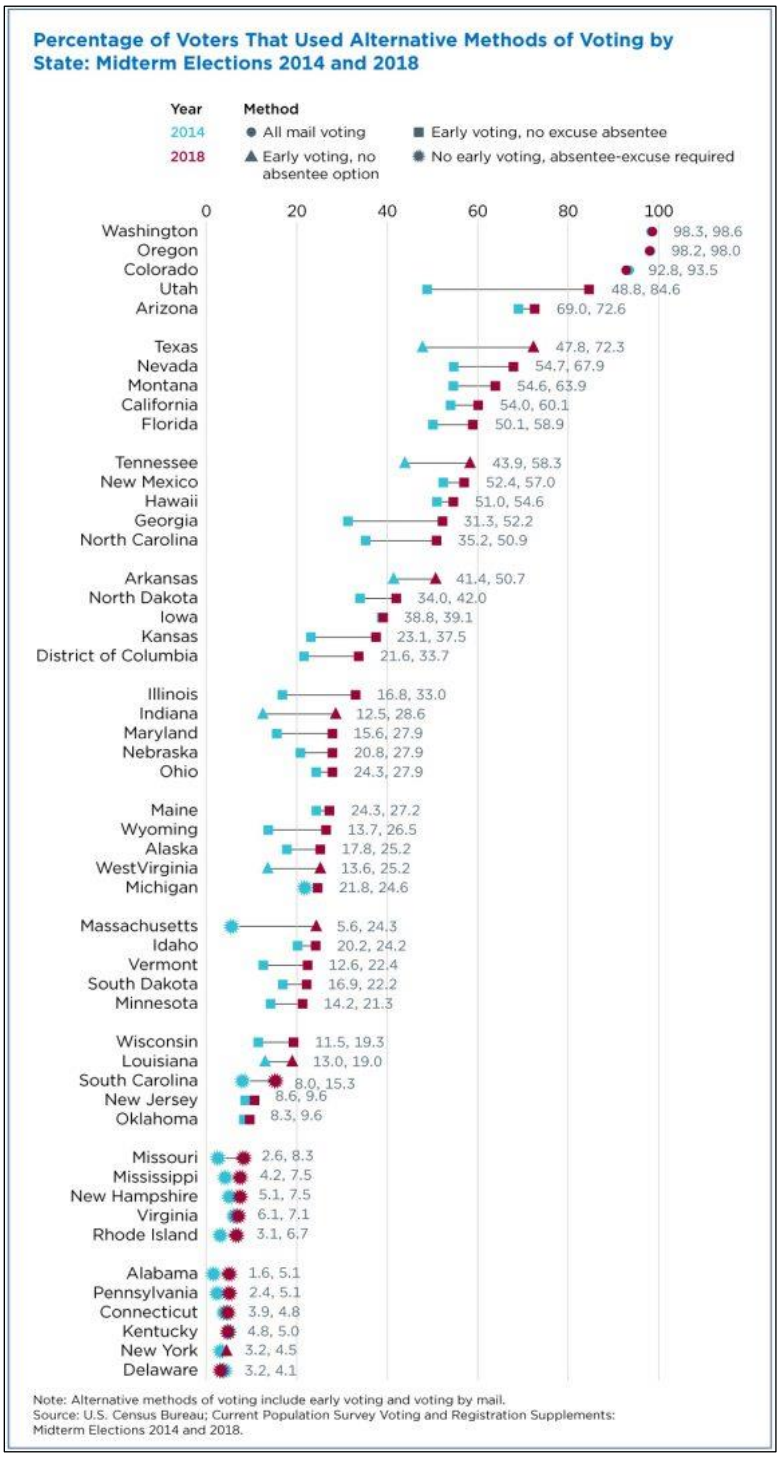
[28] See, for example, Chris Rickert, "Group Files Lawsuit to Count Votes of Those 'Disenfranchised' by Decision to Hold April 7 Election," *Wisconsin State Journal*, April 14, 2020, https://madison.com/wsj/news/local/crime-and-courts/group-files-lawsuit-to-count-votes-of-those-disenfranchised-by-decision-to-hold-april-7/article_add7bf20-4362-50a6-be88-f56506098f3b.html; and Tim Prudente, "Baltimore's Mail-in Primary Got Off to a Rocky Start. What Problems May Lie Ahead?" *The Baltimore Sun*, June 4, 2020, https://www.baltimoresun.com/politics/bs-md-pol-election-legal-20200604-c7seszdotzeklj6jqi5po5lpy4-story.html.

million and $1.4 billion and would require significant investment in new physical and cyber infrastructure to handle the anticipated increase in volume of mailed ballots.[29]

[29] Brennan Center for Justice, "Estimated Costs of COVID-19 Election Resiliency Measures," https://www.brennancenter.org/our-work/research-reports/estimated-costs-covid-19-election-resiliency-measures.

Figure 1. Expanding Use of Alternative Voting Methods

2014 and 2018 Midterm Elections



Source: Jordan Misra, U.S. Census Bureau, "Behind the U.S. Midterm Election Turnout," https://www.census.gov/library/stories/2019/04/behind-2018-united-states-midterm-election-turnout.html.

Development of Mail Voting Infrastructure During the COVID-19 Emergency

In January 2020, CISA released a tabletop exercise package for elections officials. One of the three scenarios focused on malicious exploitation of vote-by-mail systems. In the scenario, attackers target local elections offices with phishing emails and malware embedded in an emailed ballot from an overseas voter. Additionally, attackers target the local vendor responsible for printing ballots with a phishing email. The attacks in the tabletop create severe disruptions, including a spike in false registrations, misprinted and misaddressed ballots, altered public-facing election information websites, and computer malfunctions in the local election office. In the exercise, a coordinated social media campaign spurs street protests that block access to ballot drop-box locations and harassment of elections officials.[30]

Although the scenario is fictional, CISA developed it based on analysis of existing cyber and physical threats. The threat environment for elections systems has become more complex since the publication of the exercise package due to the onset of the COVID-19 pandemic. The Election Infrastructure Information Sharing and Analysis Center (EI-ISAC), founded under DHS auspices in 2018 as a private non-profit EIS coordination body for threat reporting and analysis, has reported an increase in cyberattacks against state and local government agencies. The attacks have attempted to exploit vulnerabilities created by the sudden increase in remote telework by agency employees as well as workers' concerns about the pandemic.[31]

On March 13, 2020, CISA issued an alert regarding enterprise virtual private network (VPN) security that encouraged EIS stakeholders to "adopt a heightened state of cybersecurity."[32] According to EI-ISAC, rapid expansion of telework has meant that some jurisdictions did not implement security features like multi-factor authentication or VPN access before employees began working from home. Bandwidth limitations are also commonplace. These conditions may increase the vulnerability of state and local networks to malware and denial of service (DDOS) attacks.[33] Likewise, social engineering attacks have exploited the pandemic by using COVID-19-themed phishing lures for ransomware and other malware.

In addition to its effects on cybersecurity, the pandemic prompted many state and local authorities to issue stay-at-home orders that have resulted in business closures and other disruptions. Although CISA has issued non-binding guidance for identifying critical infrastructure during the pandemic, state and local authorities have wide discretion in applying emergency mandates to businesses, non-profits, and government offices.[34] Experts believe that closures and restrictions, shortages of key goods, or illness of essential workers may disrupt certain planning, production, and logistics functions necessary to implement remote voting.

---

[30] CISA, *Elections Cyber Tabletop Exercise Package*, Situation Manual, Washington, DC, January 2020, pp. 10-11, https://www.cisa.gov/publication/elections-cyber-tabletop-box.

[31] Center for Internet Security (CIS), "Resource Guide for Cybersecurity During the COVID-19 Pandemic: COVID-19 Related Cyber-Attacks," https://www.cisecurity.org/blog/resource-guide-for-cybersecurity-during-the-covid-19-pandemic/.

[32] CISA, "Alert (AA20-073A) Enterprise VPN Security," March 13, 2020, https://www.us-cert.gov/ncas/alerts/aa20-073a.

[33] CIS, "Resource Guide for Cybersecurity During the COVID-19 Pandemic: COVID-19 Related Cyber-Attacks."

[34] See CRS Insight IN11284, *COVID-19: State and Local Shut-Down Orders and Exemptions for Critical Infrastructure*, by Brian E. Humphreys.

The U.S. Postal Service reports undertaking extensive prophylactic measures to preserve its operational and business continuity, which is critical to the implementation of vote-by-mail initiatives.[35] In 2020, as part of the Coronavirus Aid, Relief, and Economic Security (CARES) Act (P.L. 116-136), Congress approved a $10 billion line of credit to ensure the financial solvency of the U.S. Postal Service and guarantee continued operations. According to media reports, the Trump Administration threatened to withhold the funds unless the USPS increases parcel delivery prices fourfold—a move it has opposed. The USPS said it might not be able to continue operations beyond September 2020 without the funds.[36]

The primary purpose of the U.S. critical infrastructure protection framework is to enhance information sharing on best practices and common threats, and provide certain security assessments and other services to sector stakeholders as a public good. Designation of election systems as critical infrastructure gave DHS authority to create official coordination bodies and raised the priority for the agency to provide security assistance to election jurisdictions that request it. However, DHS cannot require election authorities or vendors to join coordination bodies, implement security or other guidelines, or accept assistance. Its assistance to the EIS includes informational products, voluntary security guidelines, site-specific risk assessments, and threat reporting and monitoring.

Stakeholder participation in the EIS has increased rapidly since its inception in 2017. According to DHS, the EI-ISAC is the fastest growing of the existing ISACs, with nearly 2,500 members as of February 2020, including many state, local, tribal, and territorial (SLTT) election authorities. Nevertheless, CISA and state officials have reported difficulty getting some local officials to engage with the subsector. Some states, localities, and vendors have also been reluctant to share information about threats and vulnerabilities in their systems—a common challenge across critical infrastructure sectors. Some SLTT election officials have reported that the volume of information they receive as part of the EIS can be overwhelming and that security notifications are not always actionable.[37]

Several other considerations may apply in the context of the COVID-19 pandemic. State and local authorities may introduce new or updated remote voting systems late in the 2020 election cycle, given significant lead times required for prior completion of complex infrastructure buildouts. CISA and other service providers may receive a large number of requests for security-related assessments of system architectures and functions. It is not clear that resources will be sufficient to meet demand within the time available. Widespread social distancing and telework have expanded the attack surfaces that threat actors may seek to access, according to experts. Rapid introduction of new election infrastructure and novel work practices of elections officials may make it more difficult for experts to assess risk accurately.

COVID-19 Informational Resources

The CISA EIS Government Coordinating Council (GCC) and EIS Sector Coordinating Council (SCC) Joint COVID Working Group, in consultation with EIS stakeholders, has developed a series of issue papers that detail planning considerations for remote voting during the pandemic

[35] See U.S. Postal Service, "Media Statement," press release, April 2, 2020, https://about.usps.com/newsroom/statements/usps-statement-on-coronavirus.htm.

[36] CRS Insight IN11384, *U.S. Postal Service Financial Condition and Title VI of the CARES Act,* by Meghan M. Stuessy and Raj Gnanarajah; also Lisa Rein and Jacob Bogage, "Trump Says He Will Block Coronavirus Aid for U.S. Postal Service If It Doesn't Hike Prices Immediately," *Washington Post,* April 24, 2020.

[37] See CRS In Focus IF11445, *The Election Infrastructure Subsector: Development and Challenges,* by Brian E. Humphreys and Karen L. Shanton.

(see **Table 2**). Themes that appear in several of these papers include the anticipated increase in demand for mail-in ballots; the shortened timeframe to contract for and implement infrastructure upgrades; locating qualified vendors for printing and bulk mail processing; hiring and training staff in pandemic conditions; and cybersecurity and security of physical infrastructure. Some papers also conclude that social distancing requirements may require the expansion of facility footprints and changes to the layout and organization of workstations.

Table 2. EIS GCC and EIS SCC COVID-19 Issue Papers

Planning Considerations for Remote Voting During the Pandemic

Issue	Pandemic-Specific Planning Considerations
Ballot Drop Box	Closure of public places typically used as drop-box sites; alternative drop box sites with social distancing; policies for care provider or other third party ballot drop-off; personal protective equipment (PPE) and other protective measures for collection and processing teams.
Election Education and Outreach for Increased Absentee or Mail Voting	Public communication about increased ballot processing time and delayed results; increased demand for voter education about absentee or mail voting; policy for third-party collection, mailing, or drop-off; COVID-19 public service announcements by text; virtual press tours and briefings.
Electronic Ballot Delivery and Marking	Shortened timeframe for design, testing, and introduction of new electronic systems; acceptable risk tolerance policy; e-ballot eligibility policy; increased load on current or prospective electronic systems.
Helping Voters to Request a Mail-in Ballot	Consolidation of mailings (registration, address verification, ballot request) to conserve funds and account for shortened timelines.
Importance of Accurate Voter Data When Expanding Absentee or Mail Ballot Voting	Updated addresses and other information for voters displaced by COVID-19; increased number of undeliverable addresses and temporary address changes.
Inbound Ballot Process	Increased processing times and facility footprints due to social distancing measures; emergency deadline changes affecting vendors and postal system; supply-chain disruptions affecting procurement of automated processing equipment; safe handoff of ballot boxes to processing facility workers; PPE.
Managing an Increase in Outbound Ballots	Increased processing times and facility footprints due to social distancing measures; emergency deadline changes affecting vendors and postal system; potential staffing shortages due to health concerns; PPE.
Signature Verification and Cure Process	Potential bottleneck in process when scaled up rapidly. General COVID-19 considerations for acquisitions, hiring, contracting, and facilities management apply.

Source: Adapted from CISA, "COVID-19 & Elections," https://www.cisa.gov/covid-19-and-elections.

A joint EIS GCC and SCC vote-by-mail timeline, published separately, lists over 100 discrete tasks—many requiring months to complete—that elections authorities would need to include in their plans.[38] Examples include legislative changes, remote workforce planning, software

[38] CISA EIS GCC and EIS SCC Joint COVID Working Group, "Vote by Mail Project Timeline," https://www.eac.gov/sites/default/files/electionofficials/vbm/VBMProjectTimeline.xlsx.

development and integration, graphic design of mailing materials, implementation of ballot tracking and signature verification systems, and various forms of systems testing, among others.

Grants and Emergency Expansion of Mail Voting

Decreases in state revenues due to economic disruptions caused by COVID-19 may place fiscal constraints on state and local efforts to expand remote voting. Congress has periodically provided funds for state elections administration through HAVA and subsequent appropriations legislation. The Consolidated Appropriations Act, 2018 (P.L. 115-141) and the Consolidated Appropriations Act, 2020 (P.L. 116-93) included $380 million and $425 million, respectively, for payments to states, territories, and the District of Columbia under HAVA.[39] Although not specifically intended to fund expansion of mail voting, EAC guidance gives states discretion in use of these funds for unanticipated expenses associated with the pandemic, including postage and certain other expenses incurred by increased demand for mail voting.[40]

The CARES Act provides an additional $400 million in election security grants as a supplement to the existing Election Security Grant program originally authorized under HAVA. According to media reports, there has been disagreement in Congress over whether states may use the supplemental funding to expand mail voting.[41] The EAC, which administers the grant program, has released guidance allowing for limited use of funds for states to reimburse counties for vote-by-mail postage expenses if used for one-time emergency response to the pandemic and the recipient election authority does not continue the practice in future elections. According to EAC guidance, general improvement to mail voting systems must use previously approved HAVA funding for elections administration.[42]

Congress also regularly appropriates funding for homeland security grants to the states.[43] The Federal Emergency Management Agency (FEMA) administers these grants. FEMA announced in February 2020 that elections security would be included as a priority area for FY2020 State Homeland Security Program (SHSP) grants. State administrative agencies are required to include at least one election security project under each of two priority areas: Enhancing Security, and Enhancing the Protection of Soft Targets/Crowded Places.[44] According to the FEMA Notice of Funding Opportunity, relevant project types might include cybersecurity risk assessments, remediation of identified cybersecurity vulnerabilities, and physical security enhancements for election infrastructure facilities.[45]

SHSP grants do not directly support remote voting initiatives, but can support cybersecurity and physical security of elections infrastructure, and thus may indirectly enable remote voting expansion. Total grant funding for all SHSP categories is $415 million. It is not clear whether

[39] See CRS In Focus IF11286, *Election Security: Federal Funding for Securing Election Systems*, by Karen L. Shanton.

[40] See EAC, "Guidance on Use of HAVA Funds for Expenses Related to COVID-19," https://www.eac.gov/election-officials/guidance-use-hava-funds-expenses-related-covid-19.

[41] See, for example, Benjamin Siegel, "How Experts Worry the Coronavirus Outbreak Could Cloud the 2020 General Election," *ABC News*, April 2, 2020, https://abcnews.go.com/Politics/experts-worry-coronavirus-outbreak-cloud-2020-general-election/story?id=69908301.

[42] EAC, "2020 Cares Act Grant FAQs," https://www.eac.gov/payments-and-grants/2020-cares-act-grant-faqs.

[43] For an overview of preparedness grants, see CRS Report R44669, *Department of Homeland Security Preparedness Grants: A Summary and Issues*, by Shawn Reese.

[44] DHS, *Notice of Funding Opportunity, Fiscal Year (FY) 2020 Homeland Security Grant Program*, Washington, DC, 2020, p. 6, https://www.fema.gov/media-library/assets/documents/185911.

[45] Ibid., p. 4.

states would have sufficient time to use FY2020 SHSP grants to fund election security activities before the 2020 general election. The period of performance for the grants begins on September 1, 2020. Election Day is November 3, 2020.

Some observers have suggested that states might reprioritize and reallocate unspent SHSP balances from previous years to fund election security initiatives during the 2020 elections cycle.[46] FEMA has periodically allowed waivers for reprioritization of grants or other flexibilities, such as expansion of allowable costs, if granted discretion to do so by Congress or the Office of Management and Budget.

Cybersecurity and Infrastructure Security Services for State and Local Authorities

CISA provides a number of election security related services to elections authorities at no cost. Cybersecurity Advisors and Protective Security Advisors may visit election infrastructure sites to provide assessments, if requested. Other CISA services relevant to expansion of remote voting infrastructure are summarized in **Table 3**. Elections authorities may also use third-party services in addition to, or in place of, services provided by CISA.

Table 3. Select CISA Services for EIS

Resources	Services
Cybersecurity Assessments	Cyber Resilience Review
	External Dependencies Management Assessment
	Cyber Infrastructure Survey
	Phishing Campaign Assessment
	Risk and Vulnerability Assessment
	Remote Penetration Testing
	Vulnerability Scanning
	Validated Architecture Design Review
Detection and Prevention	Continuous Diagnostics and Mitigation
	Incident Response, Recovery, and Cyber Threat Hunting
	Malware Analysis
Information Sharing and Awareness	Automated Indicator Sharing
	National Cyber Awareness System
Training and Career Development	Cybersecurity Exercises
	National Initiative for Cybersecurity Careers and Studies
	Federal Virtual Training Environment

Source: CISA, *Election Infrastructure Security Resource Guide*, May 2019, https://www.dhs.gov/publication/election-security-resource-library.

[46] Dan Lips, "States and Cities Could Use Billions of Unspent DHS Grants to #Protect 2020," *Lawfare*, February 28, 2020.

Prospective Development of Internet Voting

Experts have described vote-by-mail and internet voting as conceptually analogous to each other.[47] In each case, the voter receives a ballot at a remote location outside the direct oversight of elections officials and then marks and transmits the ballot, either as a sealed paper-and-envelope package or as digitally encrypted data, to a central repository for processing. Each stage of the process from registration to certification of results presents identity management and security challenges, whether using paper or electronic ballots. Elections authorities must be able to verify voter identity and eligibility, while still preserving the secret ballot—a unique aspect of elections that adds complexity to elections administration and the systems used for remote voting.[48]

In the case of mail voting, a widely accepted solution is the use of two envelopes for return of marked ballots. The outer envelope bears the voter's name, registration information, and signature, while the inner envelope (with no personally identifiable information) contains the marked ballot. Once elections workers verify voter eligibility via manual or automated means, they remove the inner envelope and deposit it in a ballot box to ensure voter confidentiality. Although this system is widely accepted, some elections authorities have provided voters with a single envelope for voter information and marked ballots for elections held during the pandemic.[49] Some internet voting solutions use a combination of encryption/decryption technologies and protocols that seek to mirror the paper "double envelope" process virtually.[50]

Advocates for internet voting claim that it has advantages in security, cost, reliability, and convenience over conventional mail-in ballots if properly executed.[51] Private organizations such as artistic guilds, labor unions, and corporations have used commercially available internet voting systems for many years.[52] However, experts note that elections for public office present unique security challenges not applicable to private organizations with relatively small and well-defined voting memberships.[53] Some companies have adapted existing products to elections for public office and marketed them to EIS stakeholders, while others have designed systems from the ground up for public elections. Many assessments of available product offerings by academic researchers, private labs, and government agencies have found potentially significant security

[47] For example, see Ülle Madise and Priit Vinkel, "Internet Voting in Estonia: From Constitutional Debate to Evaluation of Experience Overs Six Elections," in *Regulating eTechnologies in the European Union: Normative Realities and Trends*, ed. Tanel Kerikmäe (Heidelberg: Springer, 2014), p. 62; and U.S. Election Assistance Commission, Voting Testing and Certification Division, *A Survey of Internet Voting*, Washington, DC, September 14, 2011, p. 44.

[48] Zach Montellaro, "Why You (Still) Can't Vote Online," *The Atlantic*, January 28, 2016, https://www.theatlantic.com/politics/archive/2016/01/why-you-still-cant-vote-online/459183/.

[49] Personal experience of the author.

[50] Michael A. Specter, James Koppel, and Daniel Weitzner, "The Ballot Is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections" *(preprint)*, 2020, p. 3, https://internetpolicy.mit.edu/wp-content/uploads/2020/02/SecurityAnalysisOfVoatz_Public.pdf; and Tadas Limbda, Konstantin Agafonov, and Linas Paukste, et al., "Peculiarities of Cyber Security Management in the Process of Internet Voting Implementation," *The International Journal of Entrepreneurship and Sustainability Issues*, vol. 5, no. 2 (December 2017), p. 379.

[51] See, for example, Hillarie Orman, "Online Voting: We Can Do It! (We Have To)," *Communications of the Association for Computing Machinery*, vol. 62, no. 9 (September 2019), pp. 25-27.

[52] Rebecca Heilweil, "Nine Companies That Want to Revolutionize Voting Technology," *Forbes*, December 2, 2017.

[53] Jeremy Epstein, "Internet Voting, Security, and Privacy," *William and Mary Bill of Rights Journal*, vol. 19, no. 4 (2011), p. 905.

vulnerabilities, although some have also offered limited praise with caveats.[54] Security concerns apply both to the ballot and to sensitive personal information voters might provide to private vendors when voting.[55]

Many experts have stated that limitations of current technology and internet infrastructure present unacceptable risks to elections integrity during the 2020 election cycle. Some say that risk inherent to internet technology and personal computing devices—specifically, the prevalence of malware—is an insurmountable barrier to its use in future elections, while others allow for the possibility that emerging technology and social acceptance of certain inherent risks may ultimately allow for its use in U.S. elections.[56] Prominent academic researchers have published open letters to Congress and state officials to voice security concerns about online voting.[57] Some states have cancelled or altered plans to expand internet voting pilot programs in response to critical third-party security assessments.[58] In May 2020, CISA and other federal agencies released guidance to the states advising them to limit use of electronic ballot return systems due to "significant security risks to the confidentiality, integrity, and availability of voted ballots."[59]

Several foreign countries have used internet voting in regional or national elections for public office over multiple election cycles. In some countries where internet voting is already widely used, elections authorities have leveraged existing online national identity management systems that use cryptographic ID cards for voter authentication. Experts have identified voter authentication as a critical obstacle to internet voting in the United States.[60] Such systems typically rely on public key infrastructure (PKI), which uses cryptographic security mechanisms,

[54] See Internet Policy Research Initiative, "How to Protect Your Vote," by Michael A. Specter and J. Alex Halderman, https://internetpolicy.mit.edu/omniballot-advice/. For links to available analyses of the Voatz internet voting system, see Trail of Bits Blog, "Our Full Report on the Voatz Mobile Voting Platform," press release, March 13, 2020, https://blog.trailofbits.com/2020/03/13/our-full-report-on-the-voatz-mobile-voting-platform/. Also, Springall, Drew; Travis Finkenauer; Zakir Durumeric; Jason Kitcat; Harri Hursti; Margaret MacAlpine; and J. Alex Halderman, "Security Analysis of the Estonian Internet Voting System," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pp. 703-715.

[55] For example, see "Michael A. Specter and J. Alex Halderman, *Security Analysis of the Democracy Live Online Voting System*, Internet Policy Research Initiative: Massachusetts Institute of Technology, Cambridge, MA, June 7, 2020, p. 3, https://internetpolicy.mit.edu/omniballot.

[56] For example, see National Academies of Sciences, *Securing the Vote: Protecting American Democracy*, Washington, DC, 2018, pp. 9 and 12, https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy. The report recommends that internet voting not be adopted until security improvements are developed, but also recommends that Congress fund further research into benefits and risks of internet voting. Also see "Expert Statements," in Joseph R. Kiniry, Daniel M. Zimmerman, and Daniel Wagner, et al., *The Future of Voting: End-to-End Verifiable Internet Voting—Specification and Feasibility Study* (Washington, DC: U.S. Vote Foundation, 2015), pp. 2-9, https://usvotefoundation-drupal.s3.amazonaws.com/prod/E2EVIV_expert_statements.pdf.

[57] For example, see American Association for the Advancement of Science, *Letter to Governors and Secretaries of State on the Insecurity of Online Voting*, April 9, 2020, https://www.aaas.org/programs/epi-center/internet-voting-letter. The authors note the COVID-19 emergency, but urge officials not to use internet voting as a solution. Also see National Election Defense Coalition, letter to Members of Congress, June 21, 2017, https://www.electiondefense.org/election-integrity-expert-letter.

[58] For example, see Kate Polit, "West Virginia Ditches Controversial Voatz App for May Election," *MeriTalk*, March 5, 2020.

[59] CISA, EAC, NIST, and Federal Bureau of Investigation, *Risk Management for Electronic Ballot Delivery, Marking, and Return*, May 2020, p. 1. The document was marked For Official Use Only, but was widely reported on by media sources, which linked to the document. For example, Joseph Marks, "The Cybersecurity 202: Internet-Based Voting is the New Front in the Election Security Wars," *Washington Post*, May 11, 2020, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/05/11/the-cybersecurity-202-internet-based-voting-is-the-new-front-in-the-election-security-wars/5eb85e4e602ff11bb1179347/.

[60] See, "Expert Statements," ibid., p. 5.

digital signatures, and special administrative protocols to enable secure and confidential internet transactions among authorized network users.[61]

DOD PKI and Internet Voting

DOD was among the first federal agencies to develop public key infrastructure on a large scale to enable integrated identity management and secure internet transactions among service members and the various component commands. DOD therefore presented a potentially attractive opportunity for application of PKI to internet voting. FVAP studied—but did not implement—a complete internet voting solution for UOCAVA voters that would have used DOD PKI as its foundation. The 2015 FVAP study found that DOD would encounter both technical and legal difficulties integrating its PKI—implemented at the federal level—with state authorities' diverse elections systems and laws.

The FVAP study did not examine the general feasibility or security of PKI-based internet voting for the much larger population of non-UOCAVA voters, as this question was beyond the scope of its congressional mandate.

Given the cost and complexity of large-scale PKI, national governments have historically developed PKI for taxation, contracting, and licensing, and then subsequently adapted the system for remote voting.[62] Although many U.S. federal agencies have developed PKI for government use, the U.S. government has not developed a national-level PKI for citizen-government transactions that could be readily adapted for remote voting.

In the context of U.S. elections administration, it is not clear how the federal government would integrate PKI into multiple elections systems administered by the states (See text box "DOD PKI and Internet Voting"). However, several states have developed PKI identity management systems to enable issuance of digital driver's licenses and conduct of secure digital transactions for taxation, contracting, and licensing. A 2019 white paper published by the American Association of Motor Vehicle Administrators suggested that elections authorities could use this infrastructure for voter registration or identification with electronic driver's licenses.[63] Thus far, however, states have not proposed leveraging such PKI systems to enable a full internet voting solution.[64]

Commercial vendors marketing internet-voting products in the United States have sought to leverage emerging technologies such as blockchain-based secure transactions that do not require integration with PKI administered by a central government authority.[65] However, vendors have not yet demonstrated these technologies at scale. To date, the only attempt at general use of remote electronic voting in a U.S. public election occurred in 2012 on an emergency basis. Hurricane Sandy damaged many New Jersey polling places beyond repair before the general election. In response, state officials extended UOCAVA eligibility to all state residents, making them eligible to request and return ballots online by fax or email. Although voters cast 50,000 ballots via these methods, observers reported backlogs and other irregularities in ballot tracking and processing. Observers generally attributed these problems to the ad hoc use of communications infrastructure not intended to support wide-scale remote electronic voting.[66]

[61] National Academies of Sciences, *Securing the Vote: Protecting American Democracy*, p. 102.

[62] This was the case in Estonia, which observers generally recognize as the most extensive user of internet voting for public office. See National Academies of Sciences, *Securing the Vote: Protecting American Democracy*.

[63] American Association of Motor Vehicle Administrators, *Mobile Driver's License*, Functional Needs White Paper, Arlington, VA, March 7, 2019, p. 15, https://www.aamva.org/FunctionalNeedsWhitepaper-9/.

[64] NCSL, "Electronic Transmission of Ballots."

[65] For example, see Votem, "Secure Online Blockchain Voting," https://www.votem.com/blockchain-voting/.

[66] See Montellaro, Zach, "Why You (Still) Can't Vote Online," *The Atlantic*, January 28, 2016. https://www.theatlantic.com/politics/archive/2016/01/why-you-still-cant-vote-online/459183/, and Brian Heaton, "Has New Jersey Paved the Way for Voting via Email?," *Government Technology*, February 19, 2013, https://www.govtech.com/e-government/Has-New-Jersey-Paved-the-Way-for-Voting-via-Email.html.

Options for Congress

To address the issues discussed in this report, Congress may consider a variety of options, including the following:

- To clarify how states may use the $400 million in supplemental HAVA funding provided by the CARES Act, Congress might engage in agency oversight or enact additional legislation to either expand or further restrict the use of these funds for vote-by-mail expenses related to the COVID-19 pandemic.
- The continued solvency of USPS may become an issue that affects election administration if states choose to rely on expanded mail voting in response to COVID-19 contingencies. If Congress wishes to support expanded mail voting, Members might consider whether additional emergency funding for USPS is necessary.
- The period of performance for SHSP grants awarded during the FY2020 funding cycle begins on September 1, 2020—two months before Election Day. Congress might provide FEMA with additional waiver authorities to allow states to reprioritize or redirect prior-year SHSP funding, originally awarded for other activities, to support election security programs on an emergency basis. These authorities could be provided retroactively. Alternatively, Congress might allow states to use grant funds awarded in FY2021 to reimburse eligible election security expenses incurred during FY2020.
- The current funding issues related to the COVID-19 emergency are part of a broader debate among some Members about the proper role of Congress in supporting state election administration. Congress might provide regular funding to implement and sustain reliability improvements and security measures. Alternatively, it might provide funding on a contingency basis or choose to delegate responsibility for funding elections administration and security entirely to the states.
- In 2020, EAC continued a multiyear drafting and review process for updated voluntary voting system guidelines for states. The guidelines focus on elections systems used for in-person voting. In the past, Congress has directed EAC and the National Institute of Standards and Technology (NIST) to develop standards and guidelines for various forms of electronic remote voting—something many in the elections administration community see as an essential precursor to any wide scale rollout of these systems.[67] If Congress wishes to support long-term expansion of remote voting, beyond the current election cycle, it might direct relevant federal agencies to develop additional technical standards and guidelines.
- Congress might direct federal agencies to develop or conduct pilot studies of electronic remote voting systems to support UOCAVA voters, as it has in the past through annual defense authorizations and other legislation. If Congress seeks broader expansion of electronic remote voting access, beyond UOCAVA voters, it might also direct relevant federal agencies to provide technical assistance to

[67] Department of Defense, *Review of FVAP's Work Related to Remote Electronic Voting for the UOCAVA Program*, Washington, DC, December 15, 2015, p. 14.

- states seeking to adapt elections related applications to state electronic ID infrastructure.
- Some Members have voiced objections to a wide-scale and long-term expansion of remote voting on a variety of grounds. To address these objections, Congress might choose to regulate or restrict the use of vote-by-mail systems or online voting. For example, it might require that states adopting remote voting systems achieve certain reliability and security benchmarks or implement certain administrative protocols, or it might prohibit the use of certain technologies and practices in state election systems.
- Congress might seek testimony or other information from CISA and other relevant federal agencies on the potential risks and costs of rapidly expanding vote-by-mail and supporting infrastructure during the COVID-19 pandemic. For example, it might seek estimates from agency leaders on the expected scope of election authorities' infrastructure buildouts in response to COVID-19 contingencies, and whether agencies will be able to meet demand for vulnerability assessments, penetration testing, and other services—especially in the case of election infrastructure systems coming online shortly before the general election.
- In light of information received from agencies about demand for services, Congress might also consider whether existing appropriations will be sufficient to fund federal cybersecurity and infrastructure security services, currently provided to state election authorities on a no-cost basis.

Author Information

Brian E. Humphreys
Analyst in Science and Technology Policy

Disclaimer