The Council of State Governments, or CGS, has partnered with the Democracy Fund to create an advisory group to help states address increasingly complex cybersecurity concerns. This resource guide is one of the tools created by the advisory group, which includes state and local officials as well as cybersecurity and election experts.

Election cybersecurity has been a hot topic for researchers, think tanks and non-profit associations, governments and other stakeholders. As a result, a flurry of research and guides have been published to assist state and local government officials as they strive to fully protect their election systems. This guide provides a list of some of those resources, including a brief summary of each and links to reports or organization websites that contain helpful information. It is not a comprehensive list, but is a starting place for policymakers as they strive to be more informed and better prepared for the threats facing their states.

ORGANIZATIONS AND PUBLICATIONS

- National Association of State Chief Information Officers (NASCIO)
- National Association of Secretaries of State (NASS)
- National Association of State Election Directors (NASED)
- National Association of State Technology Directors (NASTD)
- National Conference of State Legislatures (NCSL)
- National Governors Association (NGA)
- Center for Democracy and Technology (CDT)
- Center for Internet Security (CIS) and the Multi-State Information Sharing and Analysis Center (MS-ISAC)
- DEFCON 25 – Voting Machine Hacking Village
- Defending Digital Democracy (DDD), Harvard Kennedy School executive education
- Federal Voting Assistance Program (FVAP), U.S. Department of Defense
- International Association of Governmental Officials (IAGO)
- National Institute of Standards and Technology (NIST), U.S. Department of Commerce
- The Election Center, also known as the National Association of Election Officials
- U.S. Department of Homeland Security (DHS)
- U.S. Election Assistance Commission (EAC)

NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS (NASCIO)

www.nascio.org

Founded in 1969, NASCIO is a nonprofit, 501(c)3 association representing state chief information officers and information technology executives and managers for the states, territories and the District of Columbia. The primary state members are senior officials from state government who have executive-level and statewide responsibility for information technology leadership. State CIOs and their unique understanding of state government technology and systems means they will play a key role in securing election systems from cybersecurity threats.

NATIONAL ASSOCIATION OF SECRETARIES OF STATE (NASS)

www.nass.org

Representing secretaries of state across the country, NASS serves as a forum for the exchange of information between states and fosters cooperation in the development of public policy. The association has key initiatives in the areas of elections and voting and 40 members of NASS serve as their state's designated chief election official, overseeing the conduct of elections according to law. Ensuring the integrity of the voting process is central to this role, which includes cybersecurity preparedness and contingency planning, as well as administrative and technical support for local election officials. Membership is open to the 50 states, the District of Columbia and all U.S. territories. NASS has a page on its website devoted to election cybersecurity (http://www.nass.org/initiatives/election-cybersecurity), which includes briefings, news, statements, positions NASS has taken on major policy initiatives and additional resources.

NATIONAL ASSOCIATION OF STATE ELECTION DIRECTORS (NASED)

www.nased.org

NASED is a nonprofit professional organization that disseminates election administration best practices and information across the states. The association's members are election directors from across the country who are responsible for implementing election policies, maintaining the voter registration databases, working with local election officials to ensure a successful voting experience for all voters, and more. The association's website has a list of helpful links, including key cybersecurity resources, at (https://www.nased.org/helpful-links/)

NATIONAL ASSOCIATION OF STATE TECHNOLOGY DIRECTORS (NASTD)

www.nastd.org

NASTD is a member-driven organization whose purpose is to advance and promote the effective use of information technology and services to improve the operation of state government. The association represents information technology professionals from the 50 states, divided into four regions, and the private sector. State members provide and manage state government information technology services and facilities for state agencies and other public entities, often including hospitals, prisons, colleges and universities. These members also play a strategic role in planning and shaping state government technology infrastructure and services.

NATIONAL CONFERENCE OF STATE LEGISLATURES (NCSL)

www.ncsl.org

Since it was created in 1975, NCSL has worked to advance the effectiveness, independence and integrity of legislatures, to foster interstate cooperation and to represent states at the federal level. NCSL's membership consists of the legislators of the states, the District of Columbia, and the territories and commonwealths of the United States. The association has created a Task Force on Cybersecurity (https://www.ncsl.org/blogpost/le-dictat-forces-task-force-on-cybersecurity.aspx) and a page on NCSL's website is dedicated to election security (https://www.ncsl.org/research/elections-and-campaigns/election-security-state-policies.aspx). The page includes articles and resources on election cybersecurity.

NATIONAL GOVERNORS ASSOCIATION (NGA)

www.nga.org

NGA founded in 1908, NGA is the collective voice of the nation's governors and one of Washington, D.C.'s most respected public policy organizations. Its members are the governors of the 50 states, territories and commonwealths. To help states address the consequences of the rapidly evolving and expanding technological threats now faced by law enforcement agencies, public works and energy agencies, private financial and communications sectors and the general public, NGA launched a Resource Center for State Cybersecurity (https://www.nga.org/cms/center/issues/haps/state/cybersecurity). The center is co-chaired by Michigan Gov. Rick Snyder and Virginia Gov. Terry McAuliffe and will provide governors with resources, tools and recommendations to help craft and implement effective state cybersecurity policies and practices.

CENTER FOR DEMOCRACY AND TECHNOLOGY (CDT)

www.cdt.org

CDT, a think tank and advocacy-focused organization, is headquartered in Washington, D.C., with an International Presence in London and Brussels. CDT works inclusively across sectors and the political spectrum to find tangible solutions to today’s most pressing internet policy challenges. The center’s Election Security and Privacy Project seeks to identify and update election cybersecurity practices and work towards potential remedies in a few critical areas: state voter registration systems, election auditing and campaign data, the center is also working to create a gap analysis of current election cybersecurity best practices compared to those practices of entities that regularly defend against nation-state threats.

CENTER FOR INTERNET SECURITY (CIS) AND THE MULTI-STATE INFORMATION SHARING AND ANALYSIS CENTER (MS-ISAC)

www.cisecurity.org

CIS is a non-profit group that works with the global IT community to safeguard private and public organizations against cybersecurity threats. CIS Compliant and CIS benchmarks are the global standard and recognized best practices for securing IT systems and data against the most pervasive attacks. These guidelines are continuously refined and verified by a volunteer, global community of experienced IT professionals. CIS is also home to the MS-ISAC (https://www.cisecurity.org/ms-isac/), a key resource for cybersecurity threat protection, prevention, response and recovery for U.S. state, local, tribal and territorial government entities.

CS published A Handbook for Elections Infrastructure Security (https://www.elections.gov/elections/infrastructure-security) in February 2018. The handbook is designed to help election officials and those that manufacture, own, operate, or are otherwise involved with elections systems and IT components, better understand and prioritize risks, understand best practices that can identify threats, detect attacks, allow for recovery from cybersecurity incidents and, ultimately, continue to provide and support systems for the execution of free and fair elections.

DEFCON REPORT

www.defcon.org


DEFENDING DIGITAL DEMOCRACY (DDD), HARVARD KENNEDY SCHOOL BELFER CENTER

www.belfercenter.org/ODSP

DDD is a project of the Harvard Kennedy School Belber Center for Science and International Affairs. The project aims to identify and recommend strategic tools and technology to protect democratic processes and systems from cybersecurity and information attacks. In February 2018, the group published three intuitive guides related to election cybersecurity for election administrators.

THE STATE AND LOCAL ELECTION CYBERSECURITY PLAYBOOK

https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook

Declaring that it is crucial that everyone involved in the election process—from secretaries of state and election administrators to clerks and election workers—understand their role in protecting the process and the threats that it faces, the playbook had two goals: (1) to make the most likely and most serious cybersecurity and information coxation threats understandable to everyone involved in the election process and (2) to offer state and local election officials basic risk-miti- gation strategies.

The playbook provides background to frame the elections operating environment, offers 10 best practice principles applicable to every election jurisdiction and a list of research security insights by election system, and provides basic risk-mitigation recommendations specific to five components of the election system: voter registration databases, vote casting, vote tallying, election night reporting, and internal and public communications.
The Election Center, also known as the National Association of Election Officials, is a nonprofit organization whose mission is to promote, preserve and improve democracy. With more than 1,000 members nationwide, the Election Center touts the largest number of the state and local election and voter registration administrators as members of any elections-related organization in America. Its members are almost exclusively government employees whose profession it is to serve in voter registration and elections administration, including voter registrars, elections supervisors, city clerks/city secretaries, county clerks, county recorders, state legislative staff members, state election directors and secretaries of state for each of the individual states, territories and the District of Columbia.

The Election Center has produced an Elections Security Checklist focused on risk assessment, defense and disaster recovery (https://www.electioncenter.org/election-security-infrastructure-elec
tions-security-checklist.html).

The U.S. Department of Homeland Security (DHS)

DHS was established in 2002 and combined 22 different federal departments and agencies into a unified, integrated cabinet agency. DHS resources include on-going and current information about threats, risks and vulnerability assessments, and security best practices as well as hands-on advice.

U.S. Election Assistance Commission (EAC)

The EAC was established by the Help America Vote Act of 2002, also known as HAVA, as an independent, bipartisan commission. The commission is charged with developing guidance to meet HAVA requirements, adopting voluntary voting system guidelines, and enforcing the National Voter Registration Act.

The EAC has a number of resources available, including a page on election security at https://www.eac.gov/electionsecurityr, a page on election security preparedness at https://www.eac.gov/election-offi

ELECTION CYBER INCIDENT COMMUNICATIONS COORDINATION GUIDE

This guide was designed to help coordinate and align communications across jurisdictional boundaries in an election-related cybersecurity incident that involves more than one state. Its primary purpose is to maintain (or regain) public confidence in the face of such an incident. The guide includes a set of best practices for communicating about an election-related cybersecurity incident and a process for coordinating multistate communications decision-making, including spokespeople and communications messages.

ELECTION CYBER INCIDENT COMMUNICATIONS PLAN TEMPLATE

The plan template outlines key components of a communications plan that state election officials can build out and tailor to the needs of their jurisdiction. It can also be used at the local level, particularly for large counties. A communications plan includes guidelines and template materials to help election officials respond to an election-related cybersecurity incident quickly and in a coordinated fashion during the first several days of a cybersecurity incident. The plan template is designed to be used in conjunction with the State and Local Election Cybersecurity Playbook and the Election Cyber Incident Communications Coordination Guide.

FEDERAL VOTING ASSISTANCE PROGRAM (FVAP), U.S. Department of Defense

FVAP works to ensure service members, their eligible family members and overseas citizens are aware of their right to vote and have the tools and resources to successfully do so—anywhere in the world. The director of FVAP administers the Uniformed and Overseas Citizens Absentee Voting Act, or UOCAVA, as amended by the Military and Overseas Voters Empowerment, or MOVE Act, requires states to transmit requested absentee ballots to UOCAVA voters no later than 45 days before a federal election. FVAP assists voters through partnerships with the military services, Department of State, Department of Justice and election officials from 50 States, U.S. territories and the District of Columbia.

FVAP conducted research (https://www.fvap.gov/uploads/FVAP/FVAP Reports/FVAP_5DBP_3951329_final.pdf) to inform the project planning and execution of the Department of Defense’s previously mandated electronic voting demonstration requirement. Although Congress eliminated this requirement and the Department of Defense is no longer exploring program implementation in this area, FVAP believes the research and identification of outstanding questions are valuable and should be shared. Much of the supporting research may hold value for any future deliberations on the merits of remote electronic voting and information security considerations.

INTERNATIONAL ASSOCIATION OF GOVERNMENT OFFICIALS (IGO)

www.iona.org

IGO provides professional training and leadership development for recorders, clerk, election officials and treasurers. IGO offers members opportunities to exchange ideas, elevate standards through education, encourage legislative awareness, develop efficient ways to serve the public and promote the ethics of public service internationally. The association introduces the latest in technology and innovations to government officials while developing contacts in furtherance of their profession.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), U.S. Department of Commerce

NIST was established by Congress in 1901 and is part of the U.S. Department of Commerce. The agency’s mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life. NIST implements practical cybersecurity and privacy through outreach and effective application of standards and best practices necessary for the U.S. to adopt cybersecurity capabilities. The agency’s most recent Framework for Improving Critical Infrastructure Cybersecurity describes a voluntary risk management framework consisting of standards, guidelines and best practices to manage cybersecurity-related risk (https://www.nist.gov/cyber-framework).

In addition, the Help America Vote Act of 2002, or HAVA, requires the director of NIST to chair the Technical Guidelines Development Committee and to provide technical support to the committee in the development of these voluntary guidelines (https://www.eac.gov/electionsecurityr). NIST directs NIST to conduct an evaluation of independent non-federal laboratories to carry out the testing of voting systems and to submit recommendations of qualified laboratories to the Accreditation for electronic voting.

A NIST-EAC Cybersecurity Working Group (https://www.nist.gov/itl/voting/cybersecurity-working-group) has been created for the discussion and development of guidance for voting system cyberse

Another NIST-EAC working group formed to examine the various processes necessary for the administration of an election, the Election Modeling Working Group (https://collaborate.nist.gov/voting/lnk/ view/Paging/ElectionModeling), aims to define models for both common and state-specific election operations. The models will "define the election public working groups and serve as a basis for use cases for other Common Data Format (CDF) efforts." Related to this effort is the Election Glossary, which has two main goals: define all election terminology and cross-reference any related state-specific terms.

The ELECTION CENTER

www.electioncenter.org

Cybersecurity Advisors: DHS’s Cybersecurity Advisors, or CSAs, are trained personnel assigned to 10 regions throughout the United States to help private sector entities and state, local, territorial, or tribal, or SLTT, governments prepare for—and protect themselves against—cybersecurity threats. For more information, or to reach your local CSA, contact cyberadvisor@hq.dhs.gov.

Protective Security Advisors: Serving 73 districts in 50 States and Puerto Rico, Protective Security Advisors, or PSAs, are trained in the physical aspects of Infrastructure Protection and serve as the link to DHS infrastructure protection resources and the Federal Emergency Management Agency. For more information or to reach your local PSA, please contact PSO@hq.dhs.gov.

National Cybersecurity and Communications Integration Center: DHS’s National Cybersecurity and Communications Integration Center is a 24/7 cybersecurity situational awareness, incident response, and cybersecurity risk management center that is the national nexus of cybersecurity and communications information. The Computer Readiness Team is part of this center and has some tips on securing voter registration data on their site (https://www.usa.gov/nasips/nta/files/STSI-001). To report an incident, contact ncciccustservnacsvc@hq.dhs.gov.

Additional DHS resources include cybersecurity assessments such as a no-cost, voluntary Interview-based assessment to evaluate an organization’s operational resilience and cybersecurity practices; detection and prevention services such as network protection, incident response, recovery and cyber threat hunting; information exchange, including the National Cyber Awareness System and training and career development, including cybersecurity exercises.

U.S. Election Assistance Commission (EAC)

www.eac.gov

The EAC was established by the Help America Vote Act of 2002, also known as HAVA, as an independent, bipartisan commission. The commission is charged with developing guidance to meet HAVA requirements, adopting voluntary voting system guidelines, and enforcing the National Voter Registration Act. The commission also accredits testing laboratories and certifies voting systems, as well as audits the use of HAVA funds.

The EAC has a number of resources available, including a page on election security at https://www.eac.gov/electionsecurityr, a page on election security preparedness at https://www.eac.gov/election-offi
CSG ELECTION CYBERSECURITY INITIATIVE ADVISORY GROUP MEMBERS

- David Beirne, director, Federal Voting Assistance Program
- Amy Cohen, executive director, National Association of State Election Directors
- Yejin Cooke, director of government affairs, National Association of State Chief Information Officers
- David Forscey, policy analyst, Homeland Security & Public Safety Division, National Governors Association
- Robert Giles, director, Division of Elections, New Jersey Department of State
- Kathleen Hale, member, Election Center Board of Directors
- Joseph Hall, chief technologist, Center for Democracy & Technology
- Tom Hicks, chairman, U.S. Election Assistance Commission
- Gema Howell, computer scientist, National Institute of Standards and Technology, U.S. Department of Commerce
- Matt Masterson, senior cybersecurity adviser, U.S. Department of Homeland Security
- Noah Praetz, director of elections, Cook County, Illinois Clerk’s Office
- Leslie Reynolds, executive director, National Association of Secretaries of State
- Brad Steele, treasurer of the National Association of State Technology Directors (NASTD), senior director of unified communications for the Executive Office of Technology Services and Security (EOTSS), Massachusetts

THE COUNCIL OF STATE GOVERNMENTS
www.csg.org

As our nation’s only organization serving all three branches of state government, CSG has decades of experience convening forums that foster the exchange of insights and ideas to help state officials shape public policy. CSG also has considerable experience helping states develop public policy specifically suited to their needs.

DEMOCRACY FUND
www.democracyfund.org

The Democracy Fund is a bipartisan foundation established by eBay founder and philanthropist Pierre Omidyar to help ensure that the American people come first in our democracy. The organization is a resource for those who want to strengthen our nation’s democracy and invests in change makers whose ideas and energy can make a difference.