NASS

National Association
of Secretaries of State

CYBERSECURITY RESOURCE GUIDE

DESIGNED FOR NASS MEMBERS

Last updated: July 2020

NASS makes no endorsement, expressed or implied, of any products, services, or websites in this guide. NASS is not responsible for the content or activities of any linked organizations or websites. Any questions related to products, services, or websites should be directed to the administrators of the specific sites to which this guide provides links. All critical information should be independently verified.

Executive Summary

This cybersecurity resource guide is an initiative of the Cybersecurity Committee of the National Association of Secretaries of State (NASS). The committee is comprised of all NASS members and is dedicated to information sharing of policies and practices across states. The committee focuses on cybersecurity as it relates to all facets of offices of Secretaries of State.

Cybersecurity has long been a priority for Secretaries of State. Across the 50 states, Secretaries of State have varying roles and responsibilities which include election administration, business services including online UCC (Uniform Commercial Code) and business filings, state archives, records management, and a range of other administrative tasks. Secretaries and their staff are focused on cybersecurity for all of the systems they manage and the data they collect and/or access.

The 40 Secretaries of State who have jurisdiction over elections faced increased scrutiny after the 2016 elections, which heightened awareness over how they secure their systems and create resiliency. All 50 states consider themselves a target for bad actors and are engaged in on-going efforts with federal, state, local, non-profit, and private sector partners to safeguard U.S. election systems from such threats. Secretaries of State recognize that election cybersecurity is a race with no finish line, and they will remain continuously engaged in this effort.

NASS serves in a support role in state cybersecurity efforts by acting as a conduit of information and a resource sharing platform to Secretaries of State and their staff. There are many relevant cybersecurity resources available to offices of Secretaries of State. The number of existing resources addressing both broad cybersecurity efforts and more specific election security efforts have increased significantly since the 2016 elections, but the sheer volume and ever-changing nature of the resources can be difficult to keep up with. The purpose of this guide is to help offices of Secretaries of State navigate available cybersecurity resources to include understanding the circumstances for which they may be useful, the differences between them, how to access them, and other relevant information.

The primary audience of this handbook is Secretaries of State and their staffs. It is also likely to be useful to local election officials as Secretaries of State work closely with local election officials in their states and regularly share resources. Additionally, other state government offices may find this a useful guide.

NASS Cybersecurity Committee 2020-2021 Co-Chairs:

Hon. Paul Pate
Iowa Secretary of State

Hon. Maggie Toulouse Oliver
New Mexico Secretary of State

NASS Cybersecurity Committee Meeting During 2020 Winter Conference
Washington, D.C.

Introduction

This guide contains a wide range of cybersecurity resources from extremely broad to more specific. The resources contained within the handbook are provided from a range of organizations including government offices and civic-minded nonprofit organizations. Most of the resources in the guide are free to state government offices, but some have a small to moderate cost.

The guide is organized alphabetically by the names of the organizations which provide resources. Below each organization name is an outline of their cybersecurity-related resources. Brief descriptions of the resources are provided which include summaries of their purpose, intended audience, and other relevant information. Links to additional information from each organization are included in the descriptions.

As there are many different types of cybersecurity resources available, the table on page 5 was created to help users navigate the guide. The table organizes the resources available from each organization by category, listed below.

Election-related Components

Incident Response Services

Information Sharing

Intergovernmental Coordination

Outreach Materials

Recommended Practices

Technology Procurement

Training

Workforce Development/Recruitment

Therefore, if you are looking for a resource that falls within a specific category, such as training, you can see from the table which organizations may provide relevant resource(s).

The guide will be updated as needed by NASS staff and reviewed for discussion and redistribution at each NASS Summer Conference. NASS member offices may email lforson@sso.org to suggest edits or add additional resources to this guide.

Organization Name (Page Number)	Election-related Components	Incident Response Services	Information Sharing	Intergovernmental Coordination	Outreach Materials	Recommended Practices	Technology Procurement	Training	Workforce Development/ Recruitment
Belfer Center - D3P (6)	X					X			
Center for Democracy & Technology (6)	X							X	
Center for Development of Security Excellence (CDSE) (6)					X			X	
Center for Internet Security (CIS)/MS-ISAC/EI-ISAC (6)	X	X	X			X	X	X	
Center for Technology and Civic Life (CTCL) (9)	X							X	
Council of State Governments (CSG) (9)	X			X		X			
CyberCorps - SFS Program (9)									X
Cyberseek (10)									X
Cyber Command (USCyberCom) (10)			X						
Department of Homeland Security (DHS) (10)	X	X	X	X	X	X		X	
Election Assistance Commission (EAC) (12)	X			X	X	X	X	X	
Election Center (12)	X			X		X		X	
Federal Bureau of Investigation (FBI) (13)	X	X	X	X	X				
General Services Administration (GSA) (13)							X		
Global Cyber Alliance (GCA) (13)	X					X		X	
International Association of Government Officials (iGO) (14)	X			X				X	
International Organization for Standardization (ISO) (14)						X			
Mitre (15)	X					X			
National Association of Secretaries of State (NASS) (15)	X		X	X					
National Association of State Chief Information Officers (NASCIO) (15)				X		X			
National Centers of Academic Excellence (16)									X
National Conference of State Legislatures (NCSL) (16)	X			X					
National Counterintelligence and Security Center (NCSC) (16)					X				
National Emergency Management Association (NEMA) (17)				X					
National Governors Association (NGA) (17)	X			X		X			
National Guard (17)	X	X		X				X	X
National Institute of Standards and Technology (NIST) (18)	X					X			X
Office of the Director of National Intelligence (ODNI) (19)	X		X	X					
State Fusion Centers (19)	X	X	X	X					

BELFER CENTER

Harvard's Belfer Center's Defending Digital Democracy Project (D3P) is a bipartisan effort which "aims to develop strategies, tools, and technology to protect democratic processes and systems from cyber and information attacks." D3P has provided direct assistance to election officials and worked with the election administration community to create some of the most commonly used election security resources.

The D3P Playbooks are widely implemented by election administration offices and campaigns throughout the country. The State and Local Election Cybersecurity Playbook was created to help state and local election officials formulate a cybersecurity strategy. It identifies risks and offers actionable solutions which include specific technical recommendations.

The Elections Battle Staff Playbook is also geared toward state and local election officials. It focuses on optimizing election operations processes and coordination to mitigate threats. The playbook covers how to build a "Battle Staff," create communication paths, develop an incident tracking system, build an operations center, develop standard operating procedures, and more.

The Election Cyber Incident Communications Plan Template was created to help individual election offices draft their communication plans for cyber incidents. It provides a template that can be customized and implemented by election offices at the state or local level. This template may be used by offices of Secretaries of State to create and update plans, and it may also be a good resource to send to local election officials.

The Cybersecurity Campaign Playbook is a resource to help political campaigns with cybersecurity. State and local election officials can distribute it or otherwise make it available to campaigns in their jurisdictions when candidates file to run for office.

CENTER FOR DEMOCRACY AND TECHNOLOGY (CDT)

The Center for Democracy & Technology (CDT) is a non-profit organization which works on policy challenges related to the internet. As part of this mission, they provide resources related to election security such as a glossary of terms related to election cybersecurity. They also partner with CTCL on their Online Series on Cybersecurity for Election Officials.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

The Center for Development of Security Excellence (CDSE) is a directorate within the Defense Counterintelligence and Security Agency (DCSA) which provides resources to help organizations increase their security posture. These resources include cybersecurity training videos, cybersecurity posters, security awareness games, and others. These resources may be used for promoting cyber risk and cybersecurity awareness among your staff and sharing with partners.

CENTER FOR INTERNET SECURITY (CIS)

The Center for Internet Security (CIS) is a non-profit organization which exists to help organizations defend themselves against cyber threats. CIS provides a range of broad cybersecurity resources and election security-specific resources that are widely utilized by offices of Secretaries of State. CIS is also the host of the Multi-State Information Sharing and Analysis Center (MS-ISAC) for which all state, local, tribal, and territorial (SLTT) government organizations are eligible to join and the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) for SLTT election offices.

The CIS/MS-ISAC Resources Guide was created to help SLTT governments navigate CIS, MS-ISAC, and EI-ISAC resources and services, as well as some open source resources. It maps the resources and services to the NIST Cybersecurity Framework.

- **CIS Controls**

The CIS Controls are a set of prioritized cybersecurity best practices which were developed by a community of IT experts and which can be utilized by organizations in any sector to improve their cyber defenses. The CIS Controls are available at no cost and can be used to catalogue current practices to help organizations understand their existing cyber posture. Further, the controls can help organizations prioritize staff time and other resources to implement additional practices.

According to CIS, the controls "are not limited to blocking the initial compromise of systems, but also address detecting already-compromised machines and preventing or disrupting attackers' follow-on actions." The CIS Controls reflect five tenets of cyber defense: (1) offense informs defense, (2) prioritization, (3) measurements and metrics, (4) continuous diagnostics and mitigation, (5) automation. The controls must be implemented based on organization-specific characteristics and current practices. CIS provides a self-assessment tool to help with customization.

The top 20 CIS Controls are broken into three categories: basic, foundational, and organizational. The first six controls comprise the basic category. According to CIS, these are "essential to success and should be considered among the very first things to be done."

Controls seven through 16, are the "foundational" controls. These are the next priorities after the basic controls are implemented. They are technical in nature and provide clear security benefits.

Finally, controls 17 through 20 are also considered priority items but are different in nature from the previous controls. They are more focused on the people and processes of an organization than technical practices.

Each control includes a list of sub-controls which are "specific actions that organizations should take to implement the control." The latest version of the CIS Controls provides customization of the sub-controls based on "implementation groups" which categorize organizations according to a self-assessment of size and cybersecurity attributes. If you are not sure where to start with the CIS Controls, take a look at the Implementation Groups (IGs). The IGs help organizations optimize the CIS Controls by classifying themselves and then focusing their security resources and expertise where they will get the most return.

The CIS Controls are applicable to any organization. The Controls are often used by organizations to create cybersecurity metrics and track progress. The CIS Controls are frequently discussed in conjunction with the NIST Cybersecurity Framework. Compared to the NIST Cybersecurity Framework, the CIS Controls are more focused on practices while the NIST Cybersecurity

Framework is focused on creating a risk-management plan to drive practices. The two complement each other.

For questions about the CIS Controls, contact: controlsinfo@cisecurity.org.

- **CIS Election Resources**

In addition to broad cybersecurity work, CIS provides election security best practices. The CIS Election Infrastructure Security Handbook aims to help election officials prioritize risk and understand best practices. It includes specific recommendations for securing election infrastructure components. The CIS Guide for Ensuring Security in Election Technology Procurements includes sample language for requests for proposals (RFPs) and requests for information (RFIs) for election technology as well as sample language of what might constitute a good vendor response. The CIS Security Best Practices for Non-Voting Election Technology recommends practices and provides implementation guidance related to non-voting election technology for election officials and election technology providers. The CIS Election Infrastructure Assessment Tool helps election offices self-assess and discuss their security posture. The EI-ISAC Cyber Incident Checklist outlines specific actions within a three-step response to cyber incidents. It is written broadly so that it could apply to both election offices and other organizations.

- **Multi-State Information Sharing and Analysis Center (MS-ISAC)**

The mission of the Multi-State Information Sharing and Analysis Center (MS-ISAC) is "to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial (SLTT) governments through focused cyber threat prevention, protection, response, and recovery." All SLTT government organizations are eligible to join the MS-ISAC, and there is no cost for membership. SLTT governments can report cyber incidents and threats to the MS-ISAC which analyzes information to keep members informed of emerging threats and trends through alerts.

Administered through CIS and funded through DHS, the MS-ISAC provides several services to its SLTT members including a 24/7 security operation center, incident response services, cybersecurity advisories and notifications, access to secure portals for communication and document sharing, a cyber alert map, a malicious code analysis platform, a weekly malicious domains/IP report, monthly members-only webcasts, access to security tabletop exercises, a vulnerability management program, and additional awareness and information materials. Most of these services are free to members, but others have a cost. The services included in MS-ISAC membership and those which are fee-based are described here.

The MS-ISAC also administers the Nationwide Cybersecurity Review (NCSR) which is available to all members at no cost. The NCSR is an anonymous, annual self-assessment designed to measure gaps and capabilities of SLTT governments' cybersecurity programs. It is based on the NIST Cybersecurity Framework. Completing the NCSR each year helps organizes measure and track their progress. The MS-ISAC also created a guide to cybersecurity policy templates from the SANS Institute which are mapped to the NIST Cybersecurity Framework and the NCSR.

Secretaries of State who are already members of the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) are also members of the MS-ISAC. All 50 state election offices belong to the EI-ISAC. If your office is a member of the EI-ISAC but is not receiving MS-ISAC alerts (or vice versa), use the contact information below to ensure you are enrolled in updates from both ISACs.

For questions about your MS-ISAC membership, contact: services@cisecurity.org or 518-880-0699.

- **Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)**

CIS also works with DHS to host the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC). The EI-ISAC is open to all SLTT election offices, and there is no cost to be a member.

Along with election security-specific alerts and information sharing, members have access to a range of EI-ISAC Services including vulnerability assessments, incident response services, malicious code analysis, and a vulnerability management program as well as additional fee based services including, but not limited to, network security monitoring or Albert sensors.

The EI-ISAC also hosts a Cyber Situational Awareness Room on dates surrounding key elections to facilitate real-time information sharing. EI-ISAC members receive information about joining Cyber Situational Awareness Rooms by email. All 50 state election offices are members of the EI-ISAC. Your state election office should receive regular alerts from the EI-ISAC. The EI-ISAC encourages state election offices to promote EI-ISAC membership among local election offices in your state.

For EI-ISAC issues or questions, contact elections@cisecurity.org or 518-880-0699.

CENTER FOR TECHNOLOGY AND CIVIC LIFE (CTCL)

The Center for Technology and Civic Life (CTCL) is a non-profit organization that seeks to "harness the promise of technology to modernize the American voting experience" by providing low-cost and no-cost resources and training to election officials to help them communicate with voters through the use of technology. Some of these resources are related to election security.

Of particular relevance, CTCL provides an Online Series on Cybersecurity for Election Officials. Through a partnership with the Election Assistance Commission, CTCL provides this series to election officials at no cost.

Contact CTCL at hello@techandciviclife.org.

COUNCIL OF STATE GOVERNMENTS (CSG)

The Council of State Governments (CSG) serves all three branches of state government across the 50 states. CSG produced an Election Cybersecurity Initiative Guide which provides results of qualitative research on intrastate coordination related to election security and an election security resource guide. This guide may be useful for state policymakers as well as state and local election officials.

For questions about the guide or CSG's work in this area contact: Casandra Hockenberry (chockenberry@csg.org) or Taylor Lansdale (tlansdale@csg.org).

CYBERCORPS: SCHOLARSHIP FOR SERVICE (SFS) PROGRAM

The CyberCorps: Scholarship for Service Program (SFS Program) is managed by the National Science Foundation (NSF), in collaboration with the U.S. Office of Personnel Management (OPM) and DHS. Its purpose is to train and recruit the next generation of security professionals to meet the needs of the cybersecurity mission of Federal, State, Local, and Tribal Governments.

The SFS Program provides scholarships to qualifying students for up to three years of funding for their undergraduate or graduate education. In turn, students must agree to the same length of time in service to the federal government or an SLTT government. Secretaries of State can recruit cybersecurity professionals through the SFS Program.

Begin here for more information about recruiting SFS students and graduates. You have multiple options for recruitment through the program. To get started, offices of Secretaries of State should register with the SFS program as an agency. The SFS program can distribute your job information to their students. They can also provide registered agencies with information on available students so you can contact prospects directly. You can also work directly with one or more SFS program participating institutions. The program can work with your office to determine the appropriate recruitment methods. Finally, you can also recruit through the SFS program by attending virtual or in-person job fairs. There is no cost to hire through the SFS Program or attend job fairs.

For questions about the SFS program, contact the program office at sfs@opm.gov.

CYBERSEEK

Cyberseek is an online tool, supported by NIST, that provides employers with actionable data about the cybersecurity workforce and job market. Cyberseek's interactive map allows users to see detailed information about the supply and demand of the cybersecurity workforce by state or metro area and by public sector or private sector. The cybersecurity career pathway tool allows you to learn more about common cybersecurity roles and career paths including the average salaries and skills needed for specific positions. The Cyberseek data complements the NICE Cybersecurity Workforce Framework.

CYBER COMMAND (USCyberCom)

The United States Cyber Command (USCyberCom) has the mission "to direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners." USCyberCom's Cyber National Mission Force publicly shares unclassified malware samples and cybersecurity advisories on Twitter using the handle @CNMF_CyberAlert.

DEPARTMENT OF HOMELAND SECURITY (DHS)

The Department of Homeland Security (DHS) serves as a federal cybersecurity partner for Secretaries of State through multiple avenues, including by funding the MS-ISAC and EI-ISAC. Several additional ways in which DHS offers resources and services to Secretaries of State are described below.

- **Cybersecurity and Infrastructure Security Agency (CISA)**

The mission of the Cybersecurity and Infrastructure Security Agency (CISA) within DHS "to partner with industry and government to understand and manage risk to our Nation's critical infrastructure."

CISA has 24x7 operational watch floor. States should report cyber incidents to the watch floor to receive incident response assistance from CISA.

Incidents can be reported by email at cisaservicedesk@cisa.dhs.gov or phone at 888-282-0870.

- **CISA's Election Security Initiative**

CISA prioritizes the protection of critical infrastructure. Since U.S. election systems, which are managed by states and localities, were designated as critical infrastructure, states have partnered with CISA in their efforts to protect these systems from cyber and physical threats.

Through the critical infrastructure designation, CISA prioritizes access for the Election Infrastructure (EI) Subsector to a range of no-cost services. CISA Services include regionally located Cybersecurity Advisors and Protective Security Advisors, cybersecurity assessments, detection and prevention, information sharing and awareness, incident response, and training and career development. Many state election offices utilize these services.

CISA's Election Infrastructure Security Resource Guide provides details on the services and resources available to state and local election offices. CISA also provides an online election security resource library that includes information on topics such as multifactor authentication and incident handling for election officials. One of CISA's newest election security resources is the Elections Cyber Tabletop Exercise Package also known as "Tabletop in a Box" which can help state and local election entities plan tabletop exercises.

The EI Subsector is informed by the Government Coordinating Council (EIS-GCC), a 29 member intergovernmental body and the Sector Coordinating Council (EISCC), the private sector council made up of election technology and service providers. The EIS-GCC and EISCC work together to develop a sector specific plan, priorities, and goals for the subsector. The EIS-GCC also develops and identifies resources to be utilized by the subsector, including protocols for threat information sharing and incident reporting. State and local election offices can contact NASS for a copy of these protocols.

The CISA Security Tip - Best Practices for Securing Election Systems is based on lessons learned through engagements with SLTT governments, election stakeholders, and others. The highlighted best practices can be implemented at little or no cost. CISA released the CISA Election Infrastructure Questionnaire in conjunction with the security tip to help election offices gain greater understanding of their election infrastructure by developing a systematic, catalogued set of practices.

- **Federal Virtual Training Environment (FedVTE)**

The Federal Virtual Training Environment (FedVTE) is an online cybersecurity training system which is managed by DHS and available free to government personnel, contractors, and veterans. FedVTE contains more than 800 hours of training on topics such as critical infrastructure protection, mobile and device security and wireless network security. SLTT governments can take advantage of FedVTE training. This technical training is likely to be most relevant to information technology (IT) staff. You can learn more about FedVTE here. FedVTE can be accessed through your MS-ISAC or EI-ISAC membership. Look under CIS in this guide for more on the MS-ISAC and EI-ISAC. Contact the MS-ISAC if you have questions about how to gain access to FedVTE.

- **Homeland Security Information Network (HSIN)**

State and local election officials can register with the Homeland Security Information Network (HSIN). HSIN is DHS's official system for the trusted sharing of sensitive but unclassified information between federal, state, local, territorial, tribal, international and private sector partners. EI-ISAC Cyber Situational Awareness Rooms for election officials are hosted by HSIN. However, EI-ISAC members can access the Cyber Situational Awareness Rooms through the EI-ISAC and are not required to be separately registered with HSIN. Contact the EI-ISAC for questions about accessing HSIN. You can find information on the EI-ISAC in this guide under CIS. For other information about HSIN, you can contact HSIN.Outreach@hq.dhs.gov.

- **Public Awareness Campaign: #BeCyberSmart**

DHS also released a public awareness campaign called "Be Cyber Smart." The campaign includes cyber lessons on topics such as phishing and using multi-factor authentication, facts about how cybercrime affects Americans, information about common scams, contact information for anyone to report cyber incidents to the federal government, and campaign videos that can be shared with the public through social media.

ELECTION ASSISTANCE COMMISSION (EAC)

The Election Assistance Commission (EAC) is an independent, bipartisan commission charged with developing guidance to help state and local election officials meet Help America Vote Act (HAVA) requirements. The EAC has several roles related to election security. The organization is tasked with developing and maintaining the Voluntary Voting System Guidelines (VVSG), a set of specifications and requirements against which voting systems can be tested.

The EAC also produces and compiles election security preparedness resources for election officials. This page includes general election security information, links to self-assessments, resources for securing non-voting election technology, procurement information, incident response resources, audit-related information, and more. The EAC has partnered with CTCL to offer no-cost election cybersecurity training to all election officials. The EAC also offers an Information Technology Management training program to state and local election officials at no-cost. Each training is customized to reflect state-specific voting and election systems. Contact the EAC to set up the training in your state.

In addition, the EAC has videos, voter pamphlets, and presentations that can be used by election officials to educate voters on election security.

Contact the EAC at clearinghouse@eac.gov.

ELECTION CENTER

The Election Center, also known as the National Association of Election Officials, is a membership association for government officials who serve in election administration and voter registration. The Election Center primarily serves election administrators at the local government level. They provide members with resources and election security training through conferences.

The Election Center Elections Security Checklist was created by a group of election officials. It is a checklist of specific action items that help election officials identify an inventory of critical election systems, assess risk and defensive measures, and plan for disaster recovery. This checklist is available to non-members and can be shared with local election officials in your state.

For questions about the Election Center, email: services@electioncenter.org.

FEDERAL BUREAU OF INVESTIGATION (FBI)

The Federal Bureau of Investigation is a cybersecurity information sharing partner for offices of Secretaries of State. If you experience a cyber incident, your local FBI field office is an important reporting channel. The FBI will investigate cyber incidents affecting your office.

Additionally, the FBI shares cybersecurity and election security threat indicators and other information collected through their field work with relevant stakeholders including Secretaries of State, local election officials, and other federal agencies such as DHS. Cybersecurity and election security alerts from the FBI are shared through the MS-ISAC and EI-ISAC.

The FBI also launched the Protected Voices initiative toward the goal of "mitigating the risk of cyber influence operations targeting US elections." The primary audience for Protected Voices is political campaigns, and the general public is a secondary audience. The initiative includes cybersecurity awareness videos and additional resources. The website can be shared with political candidates who register with your office.

GENERAL SERVICES ADMINISTRATION (GSA)

The General Services Administration (GSA) is a federal agency which administers DotGov (.gov) Domain Services. Use of the .gov domain comes with security and user-confidence benefits. As such, NASS supports the use of the .gov domain by SLTT government entities. The current cost of a .gov domain name is $400 per year. To register a new .gov domain, go to https://home.dotgov.gov/registration.

GSA also maintains GSA Schedules, also known as Multiple Award Schedules (MAS) and Federal Supply Schedules. GSA Schedules are "long-term governmentwide contracts with commercial firms providing federal, state, and local government buyers access to more than 11 million commercial supplies (products) and services at volume discount pricing."

GSA's Cooperative Purchasing Program allows state, local, and tribal governments to purchase IT, security, and law enforcement products and services offered through specific Schedule contracts.

GLOBAL CYBER ALLIANCE (GCA)

The Global Cyber Alliance (GCA) is "an international, cross-sector effort dedicated to eradicating cyber risk and improving our connected world." GCA offers cybersecurity webinars and tools such as DMARC for email authentication and Quad9 DNS service which can help to protect users from malicious websites.

GCA has a cybersecurity toolkit for small businesses which can be shared with small businesses that register and renew in your state.

GCA, in partnership with CIS, also recently created a cybersecurity toolkit for elections which complements the CIS Election Infrastructure Security Handbook by providing tools that can help officials implement the handbook's recommendations. The tools help users to implement cybersecurity best practices, such as multi-factor authentication. Tools are organized into "toolboxes" based on different elements of cybersecurity.

Contact GCA here.

INTERNATIONAL ASSOCIATION OF GOVERNMENT OFFICIALS (iGO)

International Association for Government Officials (iGO) is an association for local government officials. Many local election officials belong to iGO, and it provides election security training through webinars and conferences.

Contact iGO at info@iaogo.org or 919-459-2080.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) / INTERNATIONAL ELECTROTECHNICAL COMMISSIONS (IEC)

The International Organization for Standardization/ International Electrotechnical Commission 27000 (ISO/IEC 27000) family of standards was produced by ISO and the IEC to help organizations secure information assets. ISO/IEC 27000 includes over a dozen standards. The standards tend to be broad in scope, but each goes into great detail providing rules, guidelines and characteristics for activities.

The best-known standard is ISO/IEC 27001 which provides requirements for information security management systems (ISMS). ISO/IEC 27001 can be used to complement implementation of the NIST CSF and the CIS Controls.

ISO/IEC also provide standards which can help organizations manage vulnerability disclosure programs. ISO/IEC 29147 includes security techniques for vulnerability disclosure, and ISO 30111 includes security techniques for vulnerability handling processes.

Some of the ISO/IEC standards, including ISO/IEC 27000 are publicly available for download. Electronic access to other ISO/IEC standards is available for purchase through ISO store. The cost is approximately $144 for the ISO/IEC 29147 and about $92 for the ISO 30111.

For questions about purchasing or using the ISO/IEC standards, contact: customerservice@iso.org.

MITRE

The MITRE Corporation or “MITRE” is a not-for-profit organization that operates federally funded research and development centers (FFRDCs). MITRE conducts research and produces products and services to assist partners in government, industry and academia. Cybersecurity is one of MITRE’s core capabilities.

MITRE maintains the Common Vulnerabilities and Exposures (CVE) list which includes common identifiers of publicly known vulnerabilities. MITRE also offers election-specific cybersecurity products and services. MITRE’s Recommended Security Controls for Voter Registration are intended for state election officials and IT leaders. MITRE recently launched the National Election Security Laboratory through which election officials and technology providers can test election technology to evaluate risk and potential solutions.

For questions about the lab or any of MITRE’s election security efforts, contact Emily Frye (fefrye@mitre.org).

NATIONAL ASSOCIATION OF SECRETARIES OF STATE (NASS)

In addition to this handbook, the NASS cybersecurity committee has produced a number of informational resources. Our cybersecurity issue briefings address coordinated vulnerability disclosure, cyber incident response planning, and tabletop exercises.

Beyond the work of the NASS Cybersecurity Committee, NASS provides networking and information sharing opportunities for the IT and cybersecurity staff within Secretaries of State offices. NASS hosts a roundtable discussion called a “Tech Talk” for this group once or twice per year. Staff of NASS member offices can register and attend Tech Talks; there is a registration fee to pay for event costs. Secretary of State IT staff will receive information about NASS Tech Talks through NASS communications.

NASS maintains a distribution list through which cybersecurity-related information is shared. NASS members and their staff can utilize this list for official business, including surveying other member offices about IT and cybersecurity practices. Email lforson@sso.org to access the list.

NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS (NASCIO)

Secretaries of State work with their states’ chief information officers (CIO) and chief information security officers (CISO) on state cybersecurity. The National Association of State Chief Information Officers (NASCIO) represents state CIOs throughout the US. The NASCIO Resource Center includes information on state government cybersecurity and information technology. The NASCIO Cyber Disruption Response Planning Guide has been used by offices of Secretaries of State as a reference for the development of cyber incident response plans. Working with state CIOs and CISOs is not limited to election cybersecurity work but to the security of all the systems managed by the Secretary of State office.

For questions related to NASCIO’s work contact Matt Pincus (pincus@nascio.org).

NATIONAL CENTERS FOR ACADEMIC EXCELLENCE

The National Security Agency (NSA) sponsors two types of Centers of Academic Excellence:

National Centers of Academic Excellence in Cyber Defense (CAE-CD)

The goal of the CAE- CD program is "to reduce vulnerability in our national information infrastructure by promoting higher education and research in cyber defense and producing professionals with cyber defense expertise." Institutions with the designation have applied and met stringent criteria.

National Centers of Academic Excellence in Cyber Operations (CAE-CO)

The CAE-CO program builds onto the CAE-CD program. It is "a deeply technical, inter-disciplinary, higher education program firmly grounded in the computer science, computer engineering, and/or electrical engineering disciplines, with extensive opportunities for hands-on applications via labs and exercises."

National Centers of Cyber Excellence provide opportunities for recruiting interns and employees as well as opportunities for collaboration on research and outreach projects of the academic programs. States can find nearby CAE-CO programs here and CAE-CD programs here.

NATIONAL CONFERENCE OF STATE LEGISLATURES (NCSL)

The National Conference of State Legislatures (NCSL) conducts research and provides information to state legislators throughout the nation and their staffers to help them navigate complex policy issues.

NCSL has a Taskforce on Cybersecurity which helps consolidate cybersecurity resources and information to inform state legislators on cybersecurity issues. This information can also inform Secretaries of State related to their cybersecurity policy work. In addition to NCSL, Secretaries of State work closely with state legislatures in their individual states on cybersecurity policy issues, especially election security policy and funding.

For questions about the NCSL Cybersecurity Taskforce, contact Pam Greenberg (pam.greenberg@ncsl.org) or Susan Frederick (susan.frederick@ncsl.org).

NCSL has also conducted extensive election security research to inform state legislators. This information can also help state election officials with their policy work.

NCSL also hosts forums and conference sessions to inform its members on cybersecurity and election security topics.

For questions about the NCSL Election-related research, contact Wendy Underhill (wendy.underhill@ncsl.org).

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER (NCSC)

The National Counterintelligence and Security Center (NCSC) within the Office of the Director of National Intelligence (ODNI) provides online materials toward their goal of "raising awareness among government employees and private industry about…foreign intelligence threats, the risks they pose, and the defensive measures necessary for individuals and organizations to safeguard that which has been entrusted to their protection." These awareness materials include videos on topics such as social media deception and spear-phishing, threat awareness posters, flyers that address issues such as mobile device safety and reducing your digital footprint, and other electronic and print materials. They can be shared with staff, the public and partners of your office, such as local election administrators.

NATIONAL EMERGENCY MANAGEMENT ASSOCIATION (NEMA)

Secretaries of State work closely with state emergency management personnel on emergency management issues and incident response planning as it relates to cybersecurity. The National Emergency Management Association (NEMA) is the professional association which represents the emergency management directors from the 50 states.

NEMA can be contacted here.

NATIONAL GOVERNORS ASSOCIATION (NGA)

The National Governor's Association (NGA) represents the nation's governors with whom Secretaries of State coordinate with on state cybersecurity. In addition to NGA, the office of the governor and the agencies overseen by the governor in individual states are partners to Secretaries of State in cybersecurity.

NGA has created the NGA Resource Center for State Cybersecurity to assist state officials. The resource center includes NGA-produced resources and outside resources. Additionally, NGA hosts an annual summit on state cybersecurity. NGA also periodically hosts policy academies on state cybersecurity or election security for competitively selected states through which they provide technical assistance and facilitate intrastate coordination.

Contact the NGA Homeland Security & Public Safety Division at hsps@nga.org with questions about NGA's work.

NATIONAL GUARD

The National Guard serves as a partner in election security for many state election officials. National Guard troops provide cybersecurity assessments to state election offices as training exercises. In many states, the National Guard has coordinated with state election offices and is prepared to be called on in case of an election cybersecurity incident. The National Guard may also provide a recruitment opportunity to Secretaries of State looking to hire cybersecurity professionals.

The National Guard by State:

Alabama National Guard
Alaska National Guard
Arizona National Guard
Arkansas National Guard
California National Guard
Colorado National Guard
Connecticut National Guard
Delaware National Guard
Florida National Guard
Georgia National Guard
Hawaii National Guard
Idaho National Guard

Illinois National Guard
Kansas National Guard
Maine National Guard
Michigan National Guard
Missouri National Guard
Nevada National Guard
New York National Guard
Ohio National Guard
Pennsylvania National Guard
South Dakota National Guard
Utah National Guard
Washington National Guard
Wyoming National Guard

Indiana National Guard
Kentucky National Guard
Maryland National Guard
Minnesota National Guard
Montana National Guard
New Hampshire National Guard
North Carolina National Guard
Oklahoma National Guard
Rhode Island National Guard
Tennessee National Guard
Vermont National Guard
West Virginia National Guard

Iowa National Guard
Louisiana National Guard
Massachusetts National Guard
Mississippi National Guard
Nebraska National Guard
New Jersey National Guard
North Dakota National Guard
Oregon National Guard
South Carolina National Guard
Texas National Guard
Virginia National Guard
Wisconsin National Guard

NASS has a list of National Guard contacts for election security for most states. Contact NASS's Lindsey Forson at lforson@sso.org for a direct contact in your state.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

The National Institute of Standards and Technology (NIST) is a non-regulatory organization within the U.S. Department of Commerce which creates standards and metrics to support U.S. innovation and industrial competitiveness. The NIST Special Publication 800-series consists of recommendations, guidelines and other documents related to cybersecurity. The NIST Special Publication 800-61, for example, presents recommendations for handling computer security incidents. While the NIST guidance in the 800-series is geared toward federal government entities, much of it is broadly applicable.

- **NIST Cybersecurity Framework**

One of NIST's most well-known products is the NIST Cybersecurity Framework (NIST CSF). It was created to help organizations manage cybersecurity risk. There is no cost to access the voluntary standards, guidelines and best practices which make up the NIST CSF.

The NIST CSF can support the development of cybersecurity policies, recommended practices and risk-related metrics. It was created to support critical infrastructure sectors, but it is applicable to organizations in any sector, of any size, and with any degree of cybersecurity risk or sophistication.

The NIST CSF is not one-size-fits-all but is one of the most broadly applicable resources in this guide. It is meant to provide a common organizing structure for cybersecurity risk management regardless of an organization's approach to cybersecurity. The NIST CSF is often compared to the CIS Controls. Compared to the CIS controls, the NIST CSF is oriented toward broader risk management planning and organization, while the CIS controls are more focused on the execution of a specific set of actions. The NIST CSF references CIS Controls which fit within specific categories of the framework. The two resources work well together.

For questions about NIST CSF contact: cyberframework@nist.gov.

- **NICE Cybersecurity Workforce Framework**

NIST published the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. The NICE Framework "is a nationally focused resource that establishes a taxonomy and common lexicon to describe cybersecurity work, and workers, regardless of where, or for whom, the work is performed." There is no cost for using the NICE framework.

There are a range of intended benefits of the NICE Framework relevant to various players in the cybersecurity community. For example, it intends to help employers "assess their cybersecurity workforce, identify critical gaps in cybersecurity staffing, and improve position descriptions and recruitment."

The NICE Cybersecurity Workforce Framework Mapping Tool is a free tool that helps users navigate the NICE Framework. Users can "answer questions about each cybersecurity related position and the tool will show you how each position aligns to the NICE Framework and what can be done to strengthen your cybersecurity team."

- **NIST – election security**

NIST also plays a role specific to election security: NIST works with the EAC in the development of the VVSG, and NIST also works with the election administration community through the EIS-GCC on how best to apply the NIST Cybersecurity Framework to elections.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI)

The Director of National Intelligence (DNI) leads the Intelligence Community (IC) in intelligence integration. The Office of the Director of National Intelligence (ODNI) recently established the position of Election Threats Executive (ETE) to integrate intelligence relating to election security. ODNI created Cyber Threats to Elections: A Lexicon. This Lexicon was created based on ODNI's experience promoting interagency situational awareness and information sharing during previous significant cyber events and is meant to serve as a guide in the creation of future documents. The Lexicon describes common cyber and election terms and addresses misused and confusing terms.

STATE FUSION CENTERS

State Fusion Centers are focal points for intergovernmental cooperation related to the analysis and sharing of threat information. Your state fusion center can provide expertise and situational awareness. Fusion centers can foster engagement with other state agencies and organizations, as well as with other levels of government. For example, some state election offices have connected with the National Guard for cybersecurity support through their state's Fusion Center. Fusion centers can also serve as a secure location for sensitive and classified communications. Many Secretaries of State regularly coordinate with and receive information from their state fusion centers.

Locations and contact information for your state fusion centers are available here.

About NASS:
The National Association of Secretaries of State (NASS) is the nation's oldest, nonpartisan professional organization for public officials. NASS membership is open to the 50 states, the District of Columbia, and all US territories. NASS serves as a medium 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, cybersecurity, state business services, and state heritage/archives.

Index

Organization	Page Number
Belfer Center - D3P	6
Center for Democracy and Technology (CDT)	6
Center for Development of Security Excellence (CDSE)	6
Center for Internet Security (CIS)/MS-ISAC/EI-ISAC	6
Center for Technology and Civic Life (CTCL)	9
Council of State Governments (CSG)	9
CyberCorps - SFS Program	9
Cyberseek	10
Cyber Command (USCyberCom)	10
Department of Homeland Security (DHS)	10
Election Assistance Commission (EAC)	12
Election Center	12
Federal Bureau of Investigation (FBI)	13
General Services Administration (GSA)	13
Global Cyber Alliance (GCA)	13
International Association of Government Officials (iGO)	14
International Organization for Standardization (ISO)	14
Mitre	15
National Association of Secretaries of State (NASS)	15
National Association of State Chief Information Officers (NASCIO)	15
National Centers of Academic Excellence	16
National Conference of State Legislature (NCSL)	16
National Counterintelligence and Security Center (NCSC)	16
National Emergency Management Association (NEMA)	17
National Governors Association (NGA)	17
National Guard	17
National Institute of Standards and Technology (NIST)	18
Office of the Director of National Intelligence (ODNI)	19
State Fusion Centers	19