Center for Internet Security		
A Handbook for Elections Infrastructure Security	Best practices handbook and other resources from CIS and our elections partners.	www.cisecurity.org/elections-resources/
Best Practices Excel Spreadsheet	Best practices Excel spreadsheet to start securing your elections infrastructure.	
Election Infrastructure Information Sharing Analysis Center (EI-ISAC)	• 24x7x365 network monitoring • Incident response and remediation • Threat and vulnerability monitoring • Election-specific threat intelligence • Training sessions and webinars • Promote security best practices • DDoS mitigation and web protection services	Membership: https://learn.cisecurity.org/ei-isac-registration
Multi-State Information Sharing & Analysis Center (MS-ISAC)	• 24x7x365 Security Operations Center (SOC) • Cybersecurity exercises • Cyber security advisories and daily tips • Cyber event notifications • Weekly top-malicious domains and IPs report • Awareness/education materials • Network monitoring • Incident response resources	Membership: https://learn.cisecurity.org/ms-isac-subscription
Incident Response Computer Emergency Response Team (CERT)	Malware analysis, reverse engineering, log analysis, forensics analysis and security assessments	soc@cisecurity.org (866)787-4722
Department of Homeland Security		
Election Security - General	Seminar speaker contact information and DHS election security webpage	Bradford.Willke@HQ.DHS.GOV JAMES.CRATTY@HQ.DHS.GOV Election Sec. page: www.dhs.gov/topic/election-security
Federal Virtual Training Environment (FedVTE)	A Department of Homeland Security tool to provide free online cybersecurity training to government employees. A new course is available for election officials ("The Election Official as IT Manager"). You may sign up with the link on the right.	https://fedvte.usalearning.gov/
DHS Cyber Programs/Resources	Information on full range of DHS cyber programs	SLTTCyber@hq.dhs.gov www.dhs.gov/cyber

Cybersecurity Advisors (CSAs)	Trained personnel for DHS cybersecurity products	cyberadvisor@hq.dhs.gov
Protective Security Advisors (PSAs) – Physical Aspects of Infrastructure Protection	Trained personnel for physical aspect of infrastructure protection resources and FEMA	PSCDOperations@hq.dhs.gov
National Cybersecurity and Communications Integration Center	24/7 cyber situational awareness, incident response, and cyber risk management center	ncciccustomerservice@hq.dhs.gov
Physical Security		
IP Active Shooter Preparedness Program	Resources to reduce impacts of active shooter event.	ASWorkshop@hq.dhs.gov www.dhs.gov/active-shooter-preparedness
IP Unmanned Aircraft System (UAS) Initiative	Offers policies and risk mitigation solutions for safe, secure, and beneficial use of UAS, associated countermeasures, and cyber/physical emerging technology analysis.	IP-UAS@hq.dhs.gov
IP Soft Target Security Initiative	Provides national leadership on technology, standards, and best practices to demonstrably reduce the risk of successful attacks on soft targets.	IP-SoftTargetSecurity@hq.dhs.gov
Physical Assessments		
Identify and Limit Vulnerabilities	Assist Visit - On-site engagement to inform and educate owners and operators on threats from terrorism, the criticality of their facilities, and available Office of Infrastructure Protection (IP) and DHS resources.	www.dhs.gov/ecip www.dhs.gov/hometown-security
	Infrastructure Survey Tool (IST) - Facilitated survey to identify and document critical infrastructure overall security and resilience, and provide information for protective measures planning and resource allocation.	
	Hometown Security - Source for providing tools and resources to protect public-gathering venues.	
Cyber Detect and Prevent		
Detect Network Threats - Cyber Threat Hunting	Utilizes advanced hunting capabilities to identify adversary presence in a network that evades traditional security controls.	(888) 282-0870

Enhance Network Protection - Enhanced Cyber Services (ECS)	Intrusion prevention service to augment, not replace, existing cybersecurity capabilities. Leverages sensitive and classified cyber threat indicators to block malicious traffic from entering customer networks. Service offerings, available through accredited commercial service providers, include: Domain Name Service(DNS) Sinkholing, Email filtering, Netflow Analysis	www.dhs.gov/enhanced-cybersecurity-services
Cyber Information Sharing & Awareness		
Cyber Alerts and Advisories - National Cyber Awareness System (NCAS)	Provides current activity, alerts, bulletins, and security tips	www.us-cert.gov/ncas
Collaboration Homeland Security Information Network (HSIN)	Platform to securely collaborate and share cybersecurity information, threat analysis and products	HSIN.Outreach@hq.dhs.gov https://auth.dhs.gov/oam/hsinlogin/HSINLogin
Cyber Incident Response		
Analysis of Malicious Code -Advanced Malware Analysis Center	Provides 24/7 dynamic analyses of malicious code	www.malware.us-cert.gov
Mitigation and Recovery – Incident Response	Provides 24/7 intrusion analysis in response to a cyber incident. Dispatches skilled personnel when a cyber incident occurs to assist in identifying malicious actors, technical analysis, containment, mitigation guidance, and post-incident recovery.	www.us-cert.gov/forms/report Report an incident, at www.us-cert.gov/forms/report
National Guard		
Risk and Vulnerability Assessment (RVA)		
DHS RVA Qualification Program (DRQP)	A program designed to train 3rd parties on risk and vulnerability assessments (RVAs) to Department of Homeland Security standards. The National Guard is piloting this program in PA to conduct risk and vulnerability assessments on state and county networks.	https://stepfwd.cert.org/lms/
Other Election Security Resources and Services	Penetration testing and vulnerability assessments, remediation assistance, cybersecurity assistance and support, training	Contact Department of State for more information
Harvard Kennedy School – Belfer Center for Science and International Affairs		
Guides for Election Officials		
The State and Local Election Cybersecurity Playbook	The Belfer Center developed a cybersecurity playbook for state and local election officials to better understand cybersecurity vulnerabilities and potential mitigation options to improve	https://www.belfercenter.org/sites/default/files/files/publication/StateLocalPlaybook%201.1.pdf

	election security.	
Election Cyber Incident Communications Plan Template	The Belfer Center experts developed a communications template for state and local election officials as a foundation for developing their own communications response plans.	https://www.belfercenter.org/publication/election-cyber-incident-communications-plan-template
Guide for Campaigns		
The Cybersecurity Campaign Playbook	A bipartisan team of experts assembled cybersecurity best practices for campaigns. This resource could further reduce misinformation when campaigns implement strong cybersecurity protocols.	https://www.belfercenter.org/sites/default/files/files/publication/CampaignPlaybook_0.pdf
Pennsylvania Emergency Management Agency (PEMA)		
County EMAs		
County Emergency Coordinators	A list of emergency management coordinators for each county.	https://www.pema.pa.gov/about/Pages/County-EMA.aspx
Continuity of Operations (COOP) plans		
	Assistance in creating effective Continuity of Operations (COOP) plans to include critical election infrastructure.	If requested, PEMA can work with your county emergency management team.
Commonwealth's Office of Administration (OA) and County Commissioners Association of PA (CCAP)		
Phishing/Social Engineering Training		
PhishMe	A service from a company called Cofense available to county SURE users and soon to be extended at no cost to the county. Cofense and other Phishing training exercises send mock phishing emails to assess your risks and train your employees. They are very effective in teaching your employees how to recognize these types of attacks and greatly augment your security.	The Department of State will follow up shortly with more information about this program.