# ELECTION INFRASTRUCTURE SECURITY RESOURCE GUIDE

## Cybersecurity and Infrastructure Security Agency
## U.S. Department of Homeland Security

May 2019

# TABLE OF CONTENTS


IMPORTANCE OF A SECURE ELECTION SYSTEM ..... 1

ELECTION INFRASTRUCTURE'S NATIONAL LANDSCAPE ..... 1

Cybersecurity Advisors ..... 2

Protective Security Advisors ..... 3

National Cybersecurity and Communications Integration Center ..... 3

Elections Infrastructure Information Sharing and Analysis Center™ ..... 3

AVAILABLE RESOURCES ..... 4

Cybersecurity Assessments ..... 4

*Cyber Resilience Review* ..... *4*

*External Dependencies Management Assessment* ..... *6*

*Cyber Infrastructure Survey* ..... *6*

*Phishing Campaign Assessment* ..... *7*

*Risk and Vulnerability Assessment* ..... *7*

*Remote Penetration Testing* ..... *8*

*Vulnerability Scanning* ..... *8*

*Validated Architecture Design Review* ..... *9*

*Cyber Security Evaluation Tool (CSET®)* ..... *9*

Detection and Prevention ..... 10

*Continuous Diagnostics and Mitigation* ..... *10*

*Enhanced Cybersecurity Services* ..... *11*

*Incident Response, Recovery, and Cyber Threat Hunting* ..... *12*

*Malware Analysis* ..... *14*

Information Sharing and Awareness ..... 15

*Automated Indicator Sharing* ..... *15*

*Homeland Security Information Network* ..... *15*

*National Cyber Awareness System* ..... *17*

*Last Mile Posters* ..... *18*

Training and Career Development ..... 19

*Cybersecurity Exercises* ..... *19*

*National Initiative for Cybersecurity Careers and Studies* ..... *19*

*Federal Virtual Training Environment* ..... *21*

## IMPORTANCE OF A SECURE ELECTION SYSTEM

Americans' confidence that their votes count—and are counted correctly—relies on secure election systems. In recent years, American citizens have become increasingly uneasy about potential threats to the Nation's election infrastructure. Cyber intrusions to voting machines and voter registration systems diminish the overall public confidence elected officials need to perform their public duties, and undermine the integrity of the Nation's democratic process. If left unaddressed, system vulnerabilities will continue to threaten the stability of our Nation's democratic system.

Election infrastructure security is a priority for the Cybersecurity and Infrastructure Security Agency (CISA), based in the Department of Homeland Security (DHS). As the lead agency for securing the Nation's homeland, DHS, through CISA, is responsible for maintaining public trust and confidence in America's election system. CISA works directly with election officials throughout the United States to help them protect election systems by sharing timely and actionable threat information and offering cybersecurity services to safeguard their election systems.

## ELECTION INFRASTRUCTURE'S NATIONAL LANDSCAPE

State and local election officials in thousands of jurisdictions across the country govern and administer America's election process. These officials work both individually and collectively to ensure election security, reduce risks, and sustain the integrity of their elections. Although CISA plays an important role in protecting election systems, the Constitution charges state and local governments with managing the complex "system of systems"—a mix of people, processes, and equipment—that make up our Nation's election infrastructure. The Federal Government plays a supporting role by sharing information and intelligence, providing technical assistance, and responding to incidents.

In January 2017, DHS designated election systems as critical infrastructure. This designation is given to "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." [1]

The significance of this critical infrastructure designation is that it enables DHS to prioritize cybersecurity and physical security assistance to election officials upon request. It also emphasizes, both domestically and internationally, that election infrastructure possesses all the benefits and protections that the Nation has to offer. The designation enabled DHS to lead the formation of an Election Infrastructure Subsector Government Coordinating Council (EIS GCC) and the private sector's Election Infrastructure Subsector Sector Coordinating Council (EISCC) to serve as collaborative forums where the Federal Government, state and local government officials, and the private sector can establish mutually recognized information sharing to prevent or mitigate the effects of incidents that undermine the integrity of or public confidence in the election system.

CISA works with states and localities to improve their ability to detect and identify malicious cyber activity while also developing processes for coordinating mitigation efforts. CISA offers free, voluntary assistance to state and local election officials and authorities to support their infrastructure's security.

Through its partnership with the Elections Infrastructure Information Sharing and Analysis Center™ (EI-ISAC™), CISA equips election officials with the information they need to protect themselves from cyber threats. Through this effort and other programs, CISA shares actionable information about electoral infrastructure incidents with states and local governments. Also on request, CISA provides on-site and virtual assistance in identifying and remediating cyber incidents. CISA can guide election system owners and operators through cybersecurity evaluations and self-assessments while supporting risk management efforts for election systems. CISA is committed to helping its partners protect the Nation's election infrastructure.

## Cybersecurity Advisors

CISA's Cybersecurity Advisors (CSAs) are trained personnel based throughout the United States to help private sector entities and state, local, territorial, and tribal (SLTT) governments prepare for—and protect themselves against—cybersecurity threats. CSAs engage stakeholders through partnership and direct assistance activities to promote cybersecurity preparedness, risk mitigation, and incident response. CSAs introduce organizations to various cybersecurity products and services offered by CISA at no cost to the user, along with other public and private resources, and serve as liaisons to other CISA cyber programs and leadership. CSAs also offer education and awareness briefings, and perform cyber assessments, including the Cyber Resilience Review, the External Dependencies Management Assessment, and the Cyber Infrastructure Survey.

For more information, or to reach your local CSA, contact cyberadvisor@hq.dhs.gov.

[1] USA Patriot Act of 2001 (42 U.S.C. 519c(e)).

## Protective Security Advisors

Serving 73 districts in 50 states and Puerto Rico, Protective Security Advisors (PSAs) serve as the link to CISA infrastructure protection resources and the Federal Emergency Management Agency (FEMA). Trained in the physical aspects of infrastructure protection, PSAs share information and conduct resilience surveys and vulnerability assessments (such as the Infrastructure Survey Tool, Rapid Survey Tool, and the Regional Resiliency Assessment Program). PSAs assist facility owners and operators with obtaining security clearances, and offer resources, training, and access to other DHS products and services.

For more information, or to reach your local PSA, contact nicc@hq.dhs.gov.

## National Cybersecurity and Communications Integration Center

CISA's National Cybersecurity and Communications Integration Center (NCCIC) is a 24/7 cyber situational awareness, incident response, and cyber risk management center at the national nexus of cyber and communications information. NCCIC's mission is to reduce the likelihood and severity of incidents and vulnerabilities that may significantly affect the security and resilience of the Nation's critical infrastructure. NCCIC shares information to build awareness of cyber and communications vulnerabilities, threats, incidents, impacts, and mitigations.

To report an incident, contact ncciccustomerservice@hq.dhs.gov.

## Elections Infrastructure Information Sharing and Analysis Center™

The EI-ISAC is a voluntary, collaborative effort between its parent organization, the Center for Internet Security®, CISA, and the EIS GCC. Funded through DHS grants, the EI-ISAC addresses the cybersecurity needs of state and local election offices. The EI-ISAC offers state and local election officials a suite of elections-focused cyber defense tools, including

threat intelligence products, incident response and forensics, threat and vulnerability monitoring, cybersecurity awareness and training products, and best practices. For a complete list of services, visit cisecurity.org/ei-isac/ei-isac-services.

To join the EI-ISAC™, visit learn.cisecurity.org/ei-isac-registration.

# AVAILABLE RESOURCES

## Cybersecurity Assessments

In order to assist state and local election officials, CISA offers a range of cybersecurity assessments that evaluate operational resilience, cybersecurity practices, organizational management of external dependencies, and other key elements of a robust cybersecurity framework. These services are available upon request without cost to state and local election jurisdictions. CISA offers cybersecurity assessment services solely on a voluntary basis.

### Cyber Resilience Review

The Cyber Resilience Review (CRR) is an interview-based assessment that evaluates an organization's operational resilience and cybersecurity practices. This assessment derives from the CERT Resilience Management Model, a process improvement model developed by Carnegie Mellon University's Software Engineering Institute for managing operational resilience. The Cyber Resilience Review evaluates the maturity of an organization's capacities and capabilities in performing, planning, managing, measuring, and defining cybersecurity capabilities across 10 domains:

- Asset Management,
- Controls Management,
- Configuration and Change Management,
- Vulnerability Management,
- Incident Management,
- Service Continuity Management,
- Risk Management,
- External Dependency Management,
- Training and Awareness, and
- Situational Awareness.

Receiving a Cyber Resilience Review provides an organization with a more robust awareness of its cybersecurity posture by providing:

- Improved enterprise-wide awareness of the need for effective cybersecurity management,
- A review of capabilities essential to the continuity of critical services during operational challenges and crises,
- Integrated peer performance comparisons for each of the 10 domains covered in the assessment, and
- A comprehensive final report with options for improvement.

## Alignment to the NIST Cybersecurity Framework

The principles and recommended practices within the CRR align closely with the Cybersecurity Framework (Framework) developed by the National Institute of Standards and Technology (NIST) (nist.gov/cyberframework). After undergoing a CRR, an organization will be able to compare the results to the Framework to identify gaps, and where appropriate, any needed improvement efforts. A reference crosswalk mapping the relationship of the CRR goals and practices to the Framework categories and subcategories is included in the self-assessment kit. An organization's assessment of CRR practices and capabilities will show whether the organization aligns to the Framework.

## Data Privacy

The CRR report is created exclusively for an organization's internal use. All data collected and analysis performed during a CRR is protected under the DHS Protected Critical Infrastructure Information (PCII) Program (dhs.gov/pcii). PCII Program protection means CISA employees are trained in the safeguarding and handling of PCII; CISA cannot publicly disclose PCII; and PCII cannot be used for regulatory purposes.

## Assessment Logistics

- Notice required to schedule assessment: 10 business days
- Time needed to complete assessment: one business day
- Organization personnel required to perform assessment: IT policy and governance, IT security planning and management, IT infrastructure, IT operations, business operations, business continuity and disaster recovery planning, risk management, procurement and vendor management
- Timeframe for return of assessment results: 30 days

The CRR is available as a self-administered assessment or a CISA-facilitated assessment. For additional information, visit us-cert.gov/ccubedvp/assessments. To schedule a Cyber Resilience Review, contact cyberadvisor@hq.dhs.gov.

## External Dependencies Management Assessment

The External Dependencies Management (EDM) Assessment is an interview-based assessment evaluating an organization's management of external dependencies. This assessment focuses on the relationship between an organization's high-value services and assets, such as people, technology, facilities, and information, and evaluates how the organization manages risks derived from its use of the Information and Communications Technology (ICT) Supply Chain in the delivery of services. The EDM Assessment evaluates the maturity and capacity of an organization's external dependencies risk management across the three areas:

- Relationship formation,
- Relationship management and governance, and
- Service protection and sustainment.

The EDM Assessment provides an organization an informed understanding of its ability to respond to external dependency risks by providing and facilitating:

- Opportunities for internal discussion of vendor-related issues and the organization's reliance upon external entities in order to provide services;
- Improvement options for consideration derived from recognized standards and best practices, and
- A comprehensive report on the organization's third-party risk management practices and capabilities that includes peer performance comparisons.

To schedule an External Dependencies Management Assessment, contact cyberadvisor@hq.dhs.gov.

Any data CISA collects in the EDM Assessment is protected under the DHS PCII Program.

## Cyber Infrastructure Survey

The Cyber Infrastructure Survey (Survey) evaluates the effectiveness of organizational security controls, cybersecurity preparedness, and the overall resilience of an organization's cybersecurity ecosystem. The Survey provides a service-based view of cybersecurity, as opposed to a programmatic view. An organization's critical services are assessed against more than 80 cybersecurity controls grouped in five areas:

- Cybersecurity Management,
- Cybersecurity Forces,
- Cybersecurity Controls,
- Cyber Incident Response, and
- Cyber Dependencies.

After completing the Survey, the organization will receive a user-friendly dashboard to review the results and findings of the survey. Completing the Survey provides an organization with the following:

- Effective assessment of critical service cybersecurity controls,
- Interactive dashboard to support cybersecurity planning and resource allocation, and
- Peer performance data visually depicted on the dashboard.

To schedule a Cyber Infrastructure Survey, contact cyberadvisor@hq.dhs.gov.

Any data CISA collects in the Cyber Infrastructure Survey is protected under the DHS PCII Program.

## Phishing Campaign Assessment

The Phishing Campaign Assessment evaluates an organization's susceptibility and reaction to phishing emails of varying complexity.

After the assessment, the organization receives a Phishing Campaign Assessment Report highlighting organizational click rates for varying types of phishing emails and summarizing metrics related to the tendency of the organization to fall victim to phishing attacks.

To schedule a Phishing Campaign Assessment, contact ncciccustomerservice@hq.dhs.gov.

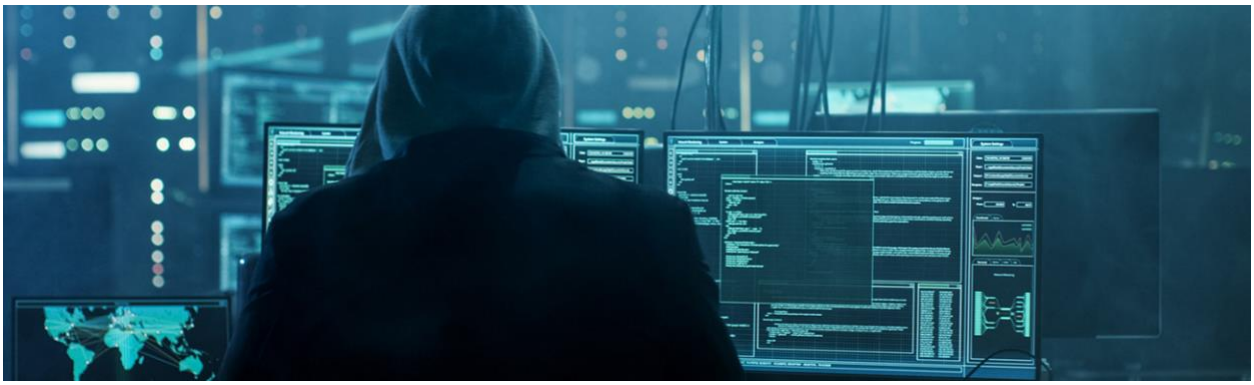
## Risk and Vulnerability Assessment

A Risk and Vulnerability Assessment (RVA) collects data through onsite assessments and combines it with national threat and vulnerability information in order to provide an organization with actionable remediation recommendations prioritized by risk. This assessment identifies vulnerabilities adversaries could exploit to compromise network security controls. An RVA may include the following methodologies:

- Scenario-based network penetration testing,
- Web application testing,
- Social engineering testing,
- Wireless testing,
- Configuration reviews of servers and databases, and
- Detection and response capability evaluation.

After completing the RVA, the organization receives a final report with business executive recommendations, specific findings and potential mitigations, and technical attack path details. An optional debrief presentation summarizing preliminary findings and observations can be provided upon request.

To schedule a Risk and Vulnerability Assessment, contact ncciccustomerservice@hq.dhs.gov.



## Remote Penetration Testing

Remote Penetration Testing (RPT) uses a dedicated remote team to assess, identify, and mitigate vulnerabilities to exploitable pathways into networks or election systems. While similar to a Risk and Vulnerability Assessment, an RPT focuses entirely on externally accessible systems. Remote Penetration Testing may include:

- Scenario-based external network penetration testing,
- External web application testing, and
- Phishing Campaign Assessment.

After completing Remote Penetration Testing, the organization receives a final report with recommendations for executive-level personnel, specific findings, potential mitigations, and technical attack path details. An optional debrief presentation summarizing preliminary findings and observations can be provided upon request.

To schedule Remote Penetration Testing, contact nccicustomerservice@hq.dhs.gov.

## Vulnerability Scanning

CISA offers Vulnerability Scanning (formerly known as Cyber Hygiene scanning) of Internet-accessible systems for known vulnerabilities on a continual basis. As CISA identifies potential vulnerabilities, it notifies the organization so preemptive risk mitigation efforts can be implemented to avert vulnerability exploitation.

After completing Vulnerability Scanning, the organization receives:

- Weekly reports detailing current and previously mitigated vulnerabilities and recommendations for mitigating uncovered vulnerabilities during scans,
- Special reporting and notices derived from enhanced scans, and
- Engineering support.

To schedule Vulnerability Scanning, contact nccicustomerservice@hq.dhs.gov.

## Validated Architecture Design Review

The Validated Architecture Design Review includes architecture and design review, system configuration, log file review, and analysis of network traffic to develop a detailed picture of the communications, flows, and relationships between devices to identify anomalous communication flows.

After the review, the organization receives an in-depth report of key discoveries and practical recommendations for improving operational maturity and cybersecurity posture.

To schedule a Validated Architecture Design Review, contact nccicustomerservice@hq.dhs.gov.

## Cyber Security Evaluation Tool (CSET®)

The Cyber Security Evaluation Tool (CSET®) is a stand-alone desktop application that guides asset owners and operators through a systematic process of evaluating operational technology and information technology (IT).

After the evaluation, the organization receives reports with assessment results. The organization can manipulate and filter content to analyze findings with varying degrees of detail.

For additional information on CSET®, visit ics-cert.gov. To request a physical copy of the software, contact nccicustomerservice@hq.dhs.gov.

# Detection and Prevention

## Continuous Diagnostics and Mitigation

The Continuous Diagnostics and Mitigation (CDM) program is a dynamic approach to fortifying the cybersecurity of government networks and systems. CDM capabilities and tools watch for and identify cybersecurity risks on an ongoing basis and prioritize needed repair based on potential impact by alerting personnel to mitigate significant problems first.

CDM capabilities and tools enable network administrators to know the state of their respective networks at any given time, thus reducing the attack surface of their networks. CDM informs on the relative risks of threats, making it possible for system personnel to identify and mitigate flaws at near-network speed.

The CDM Program improves government network security through automated control testing and progress tracking. This approach:

- Provides services to implement sensors and dashboards,
- Delivers near-real time results,
- Prioritizes the worst problems within minutes, versus quarterly or annually,
- Enables defenders to identify and mitigate flaws at network speed, and
- Lowers operational risk and exploitation of government IT systems and networks.

The CDM Program offers industry-leading, commercial off-the-shelf tools to support technical modernization as threats change. Agency-installed sensors perform on-going, automated searches for known cyber flaws. Results from the sensors feed into an agency dashboard producing customized reports to alert network managers to the most critical cyber risks. Prioritized alerts enable users to allocate resources based on the severity of the risk. Progress reports track results, which can be used to compare security postures among agency networks.

### CDM Capabilities

The CDM Program delivers capabilities in key areas:

- Dashboard – Receives, aggregates, and displays information from CDM tools at the agency and federal level.
- Asset Management – Manages hardware assets, software assets, security management configuration settings, and software vulnerabilities.
- Identity and Access Management – Manages account/access/managed privileges, trust determination for people granted access, credentials and authentication, and security-related training.
- Network Security Management – Manages network and perimeter components, host and device components, data at rest and in transit, and user behavior and activities. This includes management of events; operate, monitor, and improve; design and build-in security; boundary protection; supply chain risk management); and ongoing authorization.
- Discovery/classification – Data protection, data loss prevention, data breach/spillage mitigation, and information rights management.

For more information, visit us-cert.gov/cdm or email cdm.arm@hq.dhs.gov for acquisition-related questions or cdm@hq.dhs.gov for program and technical questions.

## Enhanced Cybersecurity Services

The Enhanced Cybersecurity Services (ECS) program helps protect IT networks by offering intrusion detection and analysis services through approved service providers. All U.S.-based public or private entities, including SLTT organizations, are eligible to participate.

ECS is a near real-time intrusion detection and analysis capability; it is not a threat feed. CISA partners with service providers who have completed a rigorous system accreditation process. ECS works by sharing sensitive and classified cyber threat information with accredited service providers who in turn use the information to block certain types of malicious traffic from entering customer networks. ECS is meant to augment, not replace, existing cybersecurity capabilities by blocking known or suspected cyber threats.

The ECS program currently offers two innovative intrusion prevention service offerings. Domain Name System Sinkholing blocks access to specified malicious domain names. Email (SMTP) Filtering blocks email with specified malicious criteria from reaching an organization's email services and email filtering. These services block possible malware communications and spear phishing campaigns targeting networks.

Participating in ECS affords organizations with a quick and efficient way to receive protections based on classified information to thwart possible malicious communications and spear phishing campaigns without having the burdensome requirements of maintaining secure facilities and cleared personnel.

Potential ECS customers can directly contact accredited ECS service providers to learn pricing and technical requirements. Accredited ECS services providers are AT&T (ecs-prmo@list.att.com), CenturyLink (ecs@centurylink.com), and Verizon (vz-ecs@one.verizon.com). The ECS service provider does not have to be the organization's Internet provider.

Program participation cost is potentially reduced or free to state and local organizations who may be eligible to apply for FEMA Homeland Security Grant Program funds (through respective state grant administrative agencies), to pay for ECS.

For more information about the ECS program, visit dhs.gov/ecs.

## Incident Response, Recovery, and Cyber Threat Hunting

The Hunt and Incident Response Team (HIRT) provides incident response, incident management, and coordination activities for cyber incidents in critical infrastructure sectors as well as government entities at the federal and SLTT levels. HIRT works with customers to identify and contain adversary activity and develop mitigation plans for removal and remediation of the root cause of the incident.

HIRT provides technical expertise and capacity in responding to incidents. Incident response efforts focus on finding the root cause of an incident by searching for tactics, techniques and procedures, along with behaviors and associated artifacts (i.e., malicious code) in the victim network.

HIRT responds to incidents such as malware infections, data theft, data corruption and ransomware encryption, denial of service, control systems intrusions, and threats against assets.

HIRT has four types of customer engagements:

- Remote assistance,
- Advisory deployment,
- Remote deployment, and
- On-site deployment.

In addition to responding to a suspected incident, HIRT addresses the increased risk resulting from the incident. The goal is to manage the situation to ensure safety, reduce risk, limit damage, and reduce recovery time and costs. Most response actions will be technical in nature but any action taken to reduce incident impact is considered incident response.

Following an engagement and upon completion of analysis, HIRT delivers an Engagement Report to the customer within 60 days. The report provides the background, scope, findings, security best practices, and conclusions relevant to the incident.

Tools, techniques, and artifacts used include:

- Existing documentation, including policies, procedures, and processes,
- System owner interviews,
- Existing customer documentation,
- Host-based analysis,
- Reviews of existing customer logs,
- Network traffic analysis,
- Network infrastructure analysis, and
- Data mapping and other diagrams.

Incident response activities include:

- Incident triage – Process taken to scope the severity of an incident and determine required resources for action.
- Network topology review – Assessment of network ingress, egress, remote access, segmentation, and interconnectivity, with resulting recommendations for security enhancements.
- Infrastructure configuration review – Analysis of core devices on the network, used, or can be used for network security (e.g., prevention, monitoring, or enforcement functions).
- Log analysis – Examination of logs from network and security devices to illuminate possible malicious activity.
- Incident specific risk overview – Materials and in-person briefings for technical, program manager, or senior leadership audience to cover current cyber risk landscape, including classified briefings to cleared staff when appropriate.
- Hunt analysis – Deployment of host and network hunting tools to detect indicators of compromise.
- Malware analysis – Reverse engineering of malware artifacts to determine functionality and discover indicators.
- Mitigation – Actionable guidance to improve the organization's security posture, including incident-specific recommendations, security best practices, and recommended tactical measures.
- Digital media analysis – Technical forensic examination of digital artifacts to detect malicious activity and develop further indicators.
- Control systems incident analysis -- Analysis of supervisory control and data acquisition devices, process control, distributed control, and any other systems that control, monitor, and manage critical infrastructure.

For more information, visit dhs.gov/cisa/cyber-incident-response. To report cybersecurity incidents and vulnerabilities, call 888-282-0870 or email nccicustomerservice@hq.dhs.gov.

## Malware Analysis

The Advanced Malware Analysis Center provides 24/7 dynamic analysis of malicious code. Stakeholders submit samples through an online website and receive a technical document outlining analysis results. Experts detail recommendations for malware removal and recovery activities. Malware analysis can be conducted jointly with incident response services if required.

Service benefits include:

- Isolated network – A standalone, closed computer network system ensures containment.
- Classified capability – A Sensitive Compartmented Information Facility (SCIF) is used for coordination with members of the intelligence community, law enforcement, and trusted third parties. It is the only accredited federal malware lab of its kind.
- Analytical capabilities – Experts analyze the current state of computer systems, storage mediums, and physical memory of computer systems.
- Extrication of malicious code – Analysts conduct static analysis and behavior analysis of malicious code types (e.g., worms, Trojans, spyware, botnets, and rootkits) using standard reverse engineering and debugging tools for malicious artifacts extracted from infected systems and submitted to NCCIC for analysis.

To submit malware for analysis, email malware.us-cert.gov or go to malware.us-cert.gov/MalwareSubmission/pages/submission.jsf.
For questions or requests, contact nccicccustomerservice@hq.dhs.gov.

# Information Sharing and Awareness

## Automated Indicator Sharing

Automated Indicator Sharing (AIS) enables the exchange of cyber threat indicators between the Federal Government, SLTT governments, and the private sector at machine speed. Threat indicators are pieces of information such as malicious IP addresses or the sender's address of a phishing email. AIS is part of CISA's effort to create a cyber ecosystem where as soon as a stakeholder observes an attempted compromise, the cyber threat indicator of compromise is shared in real time with all partners, enabling people to act to protect themselves from that particular threat.

AIS benefits include:

- Privacy and civil liberty protection – CISA has taken careful measures to ensure privacy and civil liberty protections are implemented in AIS and are regularly tested. To ensure that Personally Identifiable Information (PII) is protected, AIS has processes that:
    - Perform automated analyses and technical mitigations to delete PII that is not directly related to a cyber threat.
    - Incorporate elements of human review on select fields of certain indicators of compromise to ensure the automated processes are operating properly.
    - Minimize the amount of data included in an indicator of compromise (IOC) to ensure that its information is directly related to a cyber threat.
    - Retain only the information needed to address cyber threats.
    - Ensure any information collected is used only for network defense or limited law enforcement purposes.
- Sharing at machine speed – AIS enables two-way sharing of IOCs between the Federal Government and AIS partners in near real-time by using industry standards for machine-to-machine communication.
- Non-attributional sharing – Participants who share indicators through AIS will not be identified as the source of those indicators unless they affirmatively consent to the disclosure of their identity.

For more information, or to sign up to participate in AIS, visit us-cert.gov/ais.

## Homeland Security Information Network

The Homeland Security Information Network (HSIN) is a trusted network for sharing sensitive but unclassified information. This secure network serves all of Homeland Security—federal, SLTT, international, and private sector organizations—and is relied on for daily operations, major national and international events, disaster planning and response, public safety, and incident management. Partners can use HSIN to manage operations, analyze data, send alerts and notices, and share information to perform their duties.

CISA-developed products are available to registered stakeholders in authorized communities of interest. These products include Traffic Light Protocol (TLP) GREEN and AMBER indicator bulletins and analysis reports. TLP is a set of designations used to facilitate greater sharing of sensitive information with the appropriate audience. Four colors show allowable sharing boundaries from most restricted to least restricted public disclosure: RED, AMBER, GREEN, and WHITE, respectively.

For information on applying for a HSIN account, contact HSIN at 866-430-0162 or HSIN.HelpDesk@hq.dhs.gov. NCCIC TLP:WHITE products are available through us-cert.gov and ics-cert.gov.

HSIN uses enhanced security measures, including verifying the identity of all users the first time they register, and ensuring users use two-factor authentication each time they log on. HSIN leverages the trusted identities of its users to provide simplified access to a number of law enforcement, operations, and intelligence information-sharing portals.

Service benefits include:

- Alerts and notifications,
- Basic Learning Management System,
- Comprehensive HSIN training,
- Document repository,
- Geographic information system mapping,
- Instant messaging (HSIN chat),
- Managed workflow capabilities,
- Secure messaging (HSIN Box), and
- Web conferencing (HSIN Connect).

For more information, or to become a member, visit dhs.gov/homeland-security-information-network-hsin or email HSIN.Outreach@hq.dhs.gov.

## National Cyber Awareness System

CISA offers no-cost, subscription-based information products to stakeholders through the us-cert.gov and ics-cert.gov websites. CISA designed these products—part of the National Cyber Awareness System (NCAS)—to improve situational awareness among technical and non-technical audiences by providing timely information about cybersecurity threats and general security topics.

Products include technical alerts, control systems advisories and reports, weekly vulnerability bulletins, and tips on cyber hygiene best practices. Subscribers can select to be notified when products of their choosing are published.

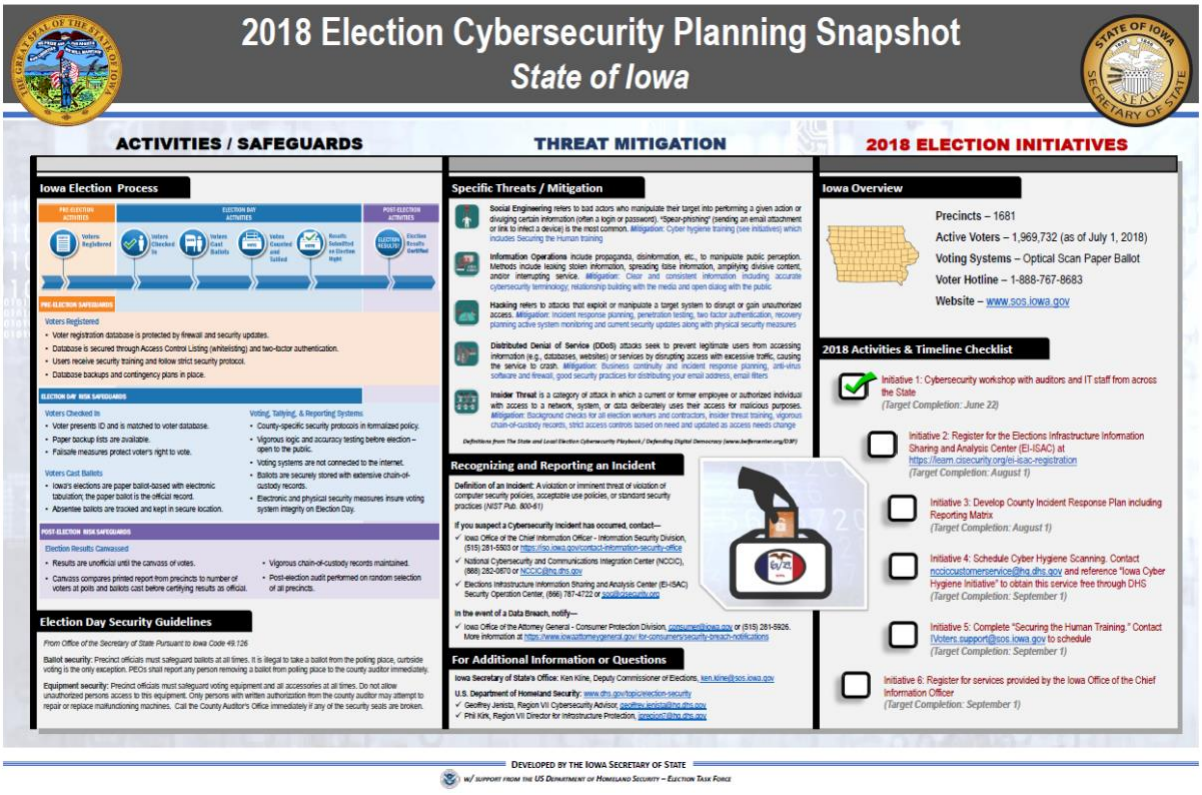
Service benefits include:

- Current Activity provides up-to-date information about high-impact security activity affecting the community at-large.
- Alerts provide timely information about current security issues, vulnerabilities, and exploits.
- Advisories provide timely information about current Industrial Control Systems security issues, vulnerabilities, and exploits.
- Bulletins provide weekly summaries of new vulnerabilities. Patch information is provided when available.
- Tips provide guidance on common security issues.

For more information on available information products, visit us-cert.gov/ncas and ics-cert.gov. To subscribe, visit public.govdelivery.com/accounts/USDHSUSCERT/subscriber/new.

## Last Mile Posters

CISA collaborates with state and local election officials to create informative posters highlighting efforts to strengthen election security. Leading up to the 2018 midterm elections, election official presented the Last Mile Posters to voters, lawmakers, and their own personnel to bolster confidence in the security of their election systems. State election offices also found the posters useful for engaging with and promoting state security initiatives to local election offices.




CISA works closely with stakeholders to tailor posters to their needs. CISA also creates and sends 20” x 30” poster copies directly to stakeholders at no cost.

For more information or to request this free service, contact electiontaskforce@hq.dhs.gov.

# Training and Career Development

## Cybersecurity Exercises

CISA provides cyber exercise and incident response planning to support election infrastructure partners. CISA delivers a full spectrum of cyber exercise planning workshops and seminars, and conducts tabletop, full-scale, and functional exercises, as well as the biennial National Cyber Exercise--Cyber Storm and the annual Cyber Guard Prelude exercise. Events are designed to assist organizations at all levels in the development and testing of cybersecurity, protection, mitigation, and response capabilities.

Exercises range from small discussion-based drills lasting two hours to full-scale, internationally scoped, operations-based exercises spanning multiple days.

- Cyber Storm – Cyber Storm is DHS's flagship, biennial exercise series, which provides an opportunity for the Federal Government, SLTT organizations, and the private sector to address cyber incident response as a community. Now on its sixth iteration, each exercise in the series has simulated the discovery of, and response to a coordinated critical infrastructure cyberattack.
- Exercise planning and conduct – CISA leverages DHS's Homeland Security Exercise and Evaluation Program model to plan and conduct a full spectrum of discussion- and operations-based cyber exercises centered on stakeholder needs. Support includes the development of exercise scenarios and supporting materials, meeting facilitation, exercise facilitation and control, and exercise evaluation.
- Cyber exercise consulting – For entities that prefer to develop their own exercises, CISA provides subject matter experts to consult on exercise design and development. CISA also makes off-the-shelf resources available for stakeholder use, which includes a scenario library, the Cyber Tabletop Exercise Package, Cyber Virtual Tabletop Exercises, and cyber incident response planning templates.
- Cyber planning support – Run by subject matter experts, Cyber Planning Workshops assist stakeholders with developing and revising integrated cyber plans.

For more information on cyber exercises, contact nccicustomerservice@hq.dhs.gov.

## National Initiative for Cybersecurity Careers and Studies

The National Initiative for Cybersecurity Careers and Studies (NICCS) was developed in close partnership between DHS, NIST, the Office of the Director of National Intelligence, and the Department of Defense, along with other government agencies, to combine efforts of government, industry, and academia to provide a comprehensive, single resource to address the Nation's cybersecurity knowledge needs.

NICCS, an online resource for cybersecurity training, connects government employees, students, educators, and industry with cybersecurity training providers throughout the Nation.

Resource benefits include:

- NICCS Education and Training Catalog – The catalog is a central repository of over 3,000 cybersecurity-related courses from over 125 different providers. The catalog can be searched by course location, preferred delivery method (i.e., online or in-person), specialty area, and proficiency level.
- Courses are designed for participants to add a skillset, increase expertise level, earn a certification, or transition to a new career. Strict vetting criteria for course providers ensure courses listed in the catalog are offered by organizations recognized as providing quality resources.
- Each course has been mapped to at least one specialty area within the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework. For more information on NICCS and the National Cybersecurity Workforce Framework, visit niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework.
- Formal Education –
    - **The National Centers of Academic Excellence (CAE) Program** – Jointly sponsored by CISA and the National Security Agency, the CAE Program designates specific two- and four-year colleges and universities as Centers of Academic Excellence based on their robust degree programs and alignment to cybersecurity-related knowledge units, validated by cybersecurity experts.
    - **The CyberCorps Scholarship for Service (SFS) Program** – The National Science Foundation provides scholarships for students at select colleges and universities in return for service in federal or SLTT governments upon graduation. For more information on SFS, visit sfs.opm.gov.
- Workforce Development –
    - **The Cybersecurity Workforce Development Toolkit** – The toolkit helps organizations understand their cybersecurity workforce and staffing needs to better protect their information, customers, and networks. The toolkit includes cybersecurity career-path templates and recruitment resources to recruit and retain top cybersecurity talent. For more information on NICCS and the Cybersecurity Workforce Development Toolkit, visit niccs.us-cert.gov/workforce-development/cybersecurity-workforce-development-toolkit.
    - **The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework** – The NICE Framework provides a blueprint to describe cybersecurity work into categories, specialty areas, work roles, tasks, and knowledge, skills, and abilities. The NICE Framework provides a common language to speak about cybersecurity jobs and helps define personal requirements for cybersecurity positions. For more information on NICCS and the National Cybersecurity Workforce Framework, visit niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework.

For more information, visit niccs.us-cert.gov or contact NICCS@hq.dhs.gov.

## Federal Virtual Training Environment

The Federal Virtual Training Environment (FedVTE) is a free, online, on-demand cybersecurity training system managed by CISA available to federal and SLTT government personnel, veterans, and federal government contractors. FedVTE contains more than 800 hours of training on topics such as ethical hacking, surveillance, risk management, and malware analysis. CISA's efforts focus on building a strong cyber workforce to keep up with evolving technology and increasing cybersecurity risks.

Election officials may find a new course of particular interest, "The Election Official as IT Manager," developed specifically for them. The course includes a review of election systems, election night reporting, and Interconnected election systems vulnerabilities and liabilities. Social media and website best practices, vulnerabilities, and liabilities are also discussed. A review of CISA resources available to the election community is included.

FedVTE resource benefits include:

- Diverse courses – More than 300 demonstrations and 3,000 related materials are available, including online lectures and hands-on virtual labs.
- Certification offerings – Offerings include Network +, Security +, Certified Information Systems Security Professional (CISSP), Windows Operating System Security, and Certified Ethical Hacker.
- Experienced instructors – All courses are taught by experienced cybersecurity subject matter experts.

To register for an account, visit niccs.us-cert.gov/training/federal-virtual-training-environment-fedvte. For more information, contact fedvte@hq.dhs.gov.

CISA
CYBER+INFRASTRUCTURE

# #PROTECT2020

CISA.gov