



**Homeland  
Security**

# **DHS Election Infrastructure Security Resource Guide**

by the National Protection and Programs Directorate  
Department of Homeland Security

*April 1, 2018*

# Table of Contents

<b>IMPORTANCE OF A SECURE ELECTION SYSTEM .....</b>	<b>3</b>
<b>ELECTION INFRASTRUCTURE’S NATIONAL LANDSCAPE .....</b>	<b>3</b>
CYBERSECURITY ADVISORS.....	4
PROTECTIVE SECURITY ADVISORS.....	4
NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.....	4
<b>AVAILABLE RESOURCES.....</b>	<b>5</b>
CYBERSECURITY ASSESSMENTS .....	5
<i>Cyber Resilience Review.....</i>	<i>5</i>
<i>External Dependencies Management Assessment .....</i>	<i>6</i>
<i>Cyber Infrastructure Survey .....</i>	<i>7</i>
<i>Phishing Campaign Assessment .....</i>	<i>8</i>
<i>Risk and Vulnerability Assessment .....</i>	<i>8</i>
<i>Vulnerability Scanning.....</i>	<i>9</i>
<i>Validated Architecture Design Review.....</i>	<i>10</i>
<i>Cybersecurity Evaluation Tool (CSET®) .....</i>	<i>10</i>
<i>Industrial Control Systems Evaluation .....</i>	<i>11</i>
DETECTION AND PREVENTION .....	12
<i>Network Protection .....</i>	<i>12</i>
<i>Incident Response, Recovery, and Cyber Threat Hunting .....</i>	<i>13</i>
<i>Malware Analysis .....</i>	<i>15</i>
INFORMATION EXCHANGE .....	15
<i>Automated Indicator Sharing .....</i>	<i>15</i>
<i>Homeland Security Information Network.....</i>	<i>16</i>
<i>Information Products: National Cyber Awareness System .....</i>	<i>16</i>
TRAINING AND CAREER DEVELOPMENT .....	17
<i>Cybersecurity Exercises.....</i>	<i>17</i>
<i>National Initiative for Cybersecurity Careers and Studies .....</i>	<i>17</i>
<i>Federal Virtual Training Environment.....</i>	<i>18</i>

# Importance of a Secure Election System

---

Americans' confidence that their vote counts – and is correctly counted – relies on secure election systems. In recent years, American citizens have become increasingly uneasy concerning potential threats to the Nation's election infrastructure. Cyber intrusions to voting machines and voter registration systems diminish the overall public confidence that 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.

Both the 2018 midterm elections and 2020 presidential election are looming. As the lead agency for securing the Nation's homeland, one of DHS's missions is to maintain public trust and confidence in America's election system. The department is working 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 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 to ensure election security, both individually and collectively, to reduce risks and sustain the integrity of their elections. Though DHS plays an important role in protecting our 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, following confirmation of the September 2016 election system hacks, the Secretary of the Department of Homeland Security designated election systems as critical infrastructure (CI). 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."<sup>1</sup>

The significance of this CI designation is that it enables DHS to prioritize cybersecurity and physical assistance to election officials who request it. The designation also emphasizes both domestically and internationally that election infrastructure possesses all the benefits and protections the Nation has to offer. The designation enabled DHS to lead the formation of a Government Coordinating Council (GCC) and the private sector's Sector Coordinating Council (SCC) to serve as collaborative forums where the Federal Government, state and local government officials, and the private sector can establish mutually recognized information sharing protocols to prevent similar instances from occurring in the future.

DHS is aggressively working with each state to improve their ability to detect and identify malicious cyber activity while also developing robust processes for coordinating mitigation efforts. The Department offers voluntary and free assistance to state and local election officials and authorities to support their infrastructure's security.

---

<sup>1</sup> USA Patriot Act of 2001 (42 U.S.C. 519c(e)).

Its partnership with the Multi-State Information Sharing and Analysis Center (MS-ISAC), DHS equips election officials with the information they need to protect themselves from similar incidents. Through this effort and other programs, DHS shares actionable information about electoral infrastructure incidents with states and local governments. Also on request, DHS will provide on-site and virtual assistance in identifying and remediating cyber incidents. DHS can guide election system owners and operators through cybersecurity evaluations and self-assessments while supporting risk management efforts on election systems. DHS is committed to helping its partners protect the Nation's election infrastructure to ensure all Americans remain confident that their election systems are secure.

Below are a few key contacts helping to secure U.S. election systems:

## Cybersecurity Advisors

DHS's Cybersecurity Advisors (CSAs) are trained personnel assigned to 10 regions 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 through DHS at no cost, along with other public and private resources, and they act as liaisons to other DHS 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](mailto:cyberadvisor@hq.dhs.gov).

## Protective Security Advisors

Serving 73 districts in 50 States and Puerto Rico, Protective Security Advisors (PSAs) are trained in the physical aspects of infrastructure protection and serve as the link to DHS infrastructure protection resources and the Federal Emergency Management Agency. PSAs share information, conduct resilience surveys and vulnerability assessments (such as the Infrastructure Survey Tool, Rapid Survey Tool, and the Regional Resiliency Assessment Program), 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, please contact [PSCDOperations@hq.dhs.gov](mailto:PSCDOperations@hq.dhs.gov).

## National Cybersecurity and Communications Integration Center

DHS's National Cybersecurity and Communications Integration Center is a 24/7 cyber situational awareness, incident response, and cyber risk management center that is 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 compromise the security and resilience of the Nation's CI, information technology (IT), and communications networks in both the public and private sectors. NCCIC also shares information to build awareness of cyber and communications vulnerabilities, threats, incidents, impacts, and mitigations.

To report an incident, contact [nccicustomerservice@hq.dhs.gov](mailto:nccicustomerservice@hq.dhs.gov).

## Available Resources

---

### Cybersecurity Assessments

#### Cyber Resilience Review

##### Description

Facilitated by DHS's Cybersecurity Advisors, the Cyber Resilience Review (CRR) is a no-cost, voluntary, interview-based assessment to evaluate an organization's operational resilience and cybersecurity practices. Through the CRR, your organization will develop an understanding of its ability to manage cyber risk during normal operations and times of operational stress and crisis.

##### Approach

The CRR is derived from the CERT Resilience Management Model (CERT-RMM), a process improvement model developed by Carnegie Mellon University's Software Engineering Institute for managing operational resilience. The CRR is based on the premise that an organization deploys its assets (people, information, technology, and facilities) to support specific critical services or products. Based on this principle, the CRR evaluates the maturity of your organization's capacities and capabilities in performing, planning, managing, measuring, and defining cybersecurity capabilities across 10 domains:

1. Asset Management
2. Controls Management
3. Configuration and Change Management
4. Vulnerability Management
5. Incident Management
6. Service Continuity Management
7. Risk Management
8. External Dependency Management
9. Training and Awareness
10. Situational Awareness

##### Outcomes

Through a CRR, your organization will gain a better understanding of your cybersecurity posture. The review provides

- an improved organization-wide awareness of the need for effective cybersecurity management;
- a review of capabilities most important to ensuring the continuity of critical services during times of operational stress and crisis;
- a catalyst for dialog between participants from different functional areas within your organization;
- a comprehensive final report that maps the relative maturity of the organizational resilience processes in each of the 10 domains, and that includes improvement options for consideration, using recognized standards; and best practices as well as references to the CERT RMM; and
- integrated peer performance comparisons for each of the 10 domains.

##### Association to the NIST Cybersecurity Framework

The principles and recommended practices within the CRR align closely with the Cybersecurity Framework (CSF) developed by the National Institute of Standards and Technology (NIST),

[www.nist.gov/cyberframework](http://www.nist.gov/cyberframework). After performing a CRR, your organization can compare the results to the criteria of the NIST CSF to identify gaps, and where appropriate, improvement efforts are needed. A reference crosswalk mapping the relationship of the CRR goals and practices to the NIST CSF categories and subcategories is included in the CRR self-assessment kit. An organization's assessment of CRR practices and capabilities may or may not indicate that the organization is fully aligned to the NIST CSF.

### **Data Privacy**

The CRR report is created exclusively for your organization's internal use. All data collected and analysis performed during a CRR assessment is afforded protection under the DHS Protected Critical Infrastructure Information (PCII) Program ([www.dhs.gov/pcii](http://www.dhs.gov/pcii)). PCII program protection means that DHS employees are trained in the safeguarding and handling of PCII, DHS cannot publicly disclose PCII, and PCII cannot be used for regulatory purposes.

### **Assessment Logistics**

- Notice required to schedule assessment: two weeks
- Time needed to complete assessment: one business day
- Personnel required to perform assessment: representatives covering the following functions: 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 self-assessment or as a facilitated assessment. For more information, or to schedule a facilitated session, contact [cyberadvisor@hq.dhs.gov](mailto:cyberadvisor@hq.dhs.gov) or visit [www.us-cert.gov/ccubedvp/assessments](http://www.us-cert.gov/ccubedvp/assessments).

## **External Dependencies Management Assessment**

### **Description**

The External Dependencies Management (EDM) assessment is a no-cost, voluntary, interview-based assessment to evaluate an organization's management of their dependencies. Through the EDM assessments, organizations can learn how to manage risks arising from external dependencies within the information and communication technology (ICT) supply chain. The ICT supply chain consists of outside parties that operate, provide, or support ICT.

### **Approach**

Risks associated with the ICT supply chain have grown dramatically with expanded outsourcing of technology and infrastructure. Failures in managing these risks have resulted in incidents affecting millions of people. The EDM Assessment focuses on the relationship between your organization's high-value services and assets (people, technology, facilities, and information) and evaluates how you manage risks incurred from using the ICT supply chain to support these high-value services. The ICT supply chain consists of outside parties that operate, provide, or support information and communications technology. Common examples include externally provided web and data hosting, telecommunications services, and data centers, as well as any service that depends on the secure use of ICT. Through the EDM assessment, the stakeholder will be able to evaluate the maturity and capacity to manage risks related to its external dependencies across three areas:

1. relationship formation,
2. relationship management and governance, and
3. service protection and sustainment.

## **Outcomes**

Through an EDM Assessment, your organization will gain a better understanding of your cybersecurity posture relating to external dependencies. The assessment provides:

- an opportunity for participants from different parts of your organization to discuss issues relating to vendors and reliance on external entities;
- options for consideration that guide improvement efforts, using recognized standards and best practices drawn from such sources as the CERT-RMM, NIST standards, and the NIST Cybersecurity Framework; and
- a comprehensive report on your third-party risk management practices and capabilities complete with peer performance comparisons.

## **Data Privacy**

The EDM report is created exclusively for your organization's internal use. All data collected and analysis performed during an EDM assessment is afforded protection under the PCII ([www.dhs.gov/pcii](http://www.dhs.gov/pcii)). PCII program protection means that DHS employees are trained in the safeguarding and handling of PCII, DHS cannot publicly disclose PCII, and PCII cannot be used for regulatory purposes. For more information, visit [www.dhs.gov/pcii-program](http://www.dhs.gov/pcii-program) or contact [PCII-Assist@hq.dhs.gov](mailto:PCII-Assist@hq.dhs.gov).

## **Assessment Logistics**

- Notice required to schedule assessment: two weeks
- Time needed to complete assessment: four hours
- Personnel required to perform assessment: representatives covering IT security planning and management, IT operations, risk management, business continuity and disaster recovery planning, IT policy and governance, business management, procurement and vendor management, and legal
- Timeframe for return assessment results: 30 days

For more information, or to schedule an EDM Assessment, contact [cyberadvisor@hq.dhs.gov](mailto:cyberadvisor@hq.dhs.gov).

## **Cyber Infrastructure Survey**

### **Description**

The Cyber Infrastructure Survey (CIS) is a no-cost, voluntary survey that evaluates the effectiveness of organizational security controls, cybersecurity preparedness, and overall resilience. CIS provides an assessment of the organization's cybersecurity practices in place for a critical service.

### **Approach**

The CIS focuses on a service-based-view versus a programmatic-view of cybersecurity. Critical services are assessed against more than 80 cybersecurity controls grouped under five top-level domains: cybersecurity management, cybersecurity forces, cybersecurity controls, cyber incident response, and cyber dependencies. Following the assessment, your organization will receive a user-friendly dashboard for reviewing and interacting with the survey findings. Your organization can use the dashboard to compare its results against industry peers, review results in the context of specific cyber and physical threat scenarios, and dynamically adjust the importance of in-place practices to see the effects on overall cyber protection.

### **Outcomes**

A CIS provides your organization with

- an effective assessment of cybersecurity controls in place for a critical service,

- a user-friendly, interactive dashboard to support cybersecurity planning and resource allocation (review results in the context of specific cyber and physical threat scenarios), and
- access to peer performance data visually depicted on the dashboard.

### **Assessment Logistics**

- Notice required to schedule assessment: two weeks
- Time needed to complete assessment: four hours
- Personnel required to perform assessment: CISO, ICS/SCADA security manager, and IT security manager
- Timeframe for return of assessment results: 30 days

### **Data Privacy**

The CIS dashboard is created exclusively for your organization’s internal use. All data collected and analysis performed during a CIS is afforded protection under the PCII Program. PCII program protection means that DHS employees are trained in the safeguarding and handling of PCII, DHS cannot publicly disclose PCII, and PCII cannot be used for regulatory purposes. For more information, visit [www.dhs.gov/pcii-program](http://www.dhs.gov/pcii-program) or contact [PCII-Assist@hq.dhs.gov](mailto:PCII-Assist@hq.dhs.gov).

For more information, or to schedule a CIS, contact [cyberadvisor@hq.dhs.gov](mailto:cyberadvisor@hq.dhs.gov).

## **Phishing Campaign Assessment**

### **Description**

The Phishing Campaign Assessment (PCA) is a no cost six-week engagement offered to SLTT governments, as well as CI and private sector companies that evaluates an organization’s susceptibility and reaction to phishing emails of varying complexity. The PCA’s results are meant to provide guidance, measure effectiveness, and justify resources needed to defend against spear-phishing and increase user training and awareness.

### **Outcomes**

After the assessment, the NCCIC will provide a PCA Report that highlights organizational click rates for varying types of phishing emails and summarizes metrics related to the proclivity of an organization to fall victim to phishing attacks

### **Assessment Logistics**

- Execution of the DHS Rules of Engagement agreement
- Pre-assessment coordination and scheduling: two weeks
- Time needed to complete the assessment: six weeks
- Personnel required to perform assessment: customer designated Point of Contact and Coordination
- Timeframe for return of assessment results: two weeks

For more information, or to get started, contact [nccicustomerservice@hq.dhs.gov](mailto:nccicustomerservice@hq.dhs.gov).

## **Risk and Vulnerability Assessment**

### **Description**

A Risk and Vulnerability Assessment (RVA) is a no-cost offering that combines national threat and vulnerability information with data collected and discovered through onsite assessment activities to provide customers with actionable remediation recommendations prioritized by risk. Engagements are

designed to determine whether and by what methods an adversary can defeat network security controls. Components of the assessment can include scenario-based network penetration testing, web application testing, social engineering testing, wireless testing, configuration reviews of servers and databases, and evaluation of an organizations detection and response capabilities.

### **Outcomes**

After the assessment, the NCCIC will provide a final RVA Report to the customer approximately 2-weeks after the engagement. The report includes business executive recommendations, specific findings and potential mitigations, as well as technical attack path details. It will also deliver an optional RVA Outbrief presentation that covers preliminary findings and observations. The briefing can be tailored for technical staff or business executives.

### **Assessment Logistics**

- Execution of the DHS Rules of Engagement agreement
- Service queue/Waitlist: customers are placed into a service queue upon their completion of the pre-requisite Rules of Engagement. The wait list evaluated on a quarterly basis and available assessment openings filled. Wait time can vary but is typically not less than 90 days.
- Pre Assessment Activities: five weeks of planning/prep (once selected from the service queue)
- Assessment Duration: two weeks of testing (one week remote and one week onsite)
- Personnel required to perform assessment: a responsible point of contact to coordinate all customer activity and (minimal) IT support to assist with technical issues such as connectivity, test accounts, etc.
- Timeframe for return of assessment results: two weeks

For more information, or to schedule an RVA, contact [nccicustomerservice@hq.dhs.gov](mailto:nccicustomerservice@hq.dhs.gov).

## **Vulnerability Scanning**

### **Description**

DHS offers Vulnerability scanning of Internet-accessible systems for known vulnerabilities on a continual basis as a no-cost service. As potential issues are identified, DHS notifies impacted customers so they may proactively mitigate risks to their systems prior to exploitation. The service incentivizes modern security practices and enables participants to reduce their exposure to exploitable vulnerabilities, which decreases stakeholder risk while increasing the Nation's overall resiliency.

### **Outcomes**

After the assessment, NCCIC will provide:

- Weekly reports - Vulnerability reports detailing current and previously mitigated vulnerabilities, high-risk hosts, and other port, device and network attributes that organizations working to improve their cybersecurity posture should examine. The report also provides recommended mitigations for each vulnerability discovered via the scanning process.
- Special reporting and notices – as certain urgent issues arise, DHS may conduct enhanced or special scans and provide special reports to help customers battle unexpected risks
- Engineering support – the NCATS team provides customer and technical support as needed.

### **Assessment Logistics**

- Execution of a signed vulnerability scanning authorization letter, to include technical points of contacts and a list of publicly accessible IPv4 addresses in CIDR notation
- Notice required to schedule assessment: 48 Hours
- Time needed to complete assessment: Fully-automated; continuous scanning

- Personnel required to perform assessment: Customer designated Point of Contact and Coordination
- Timeframe for return of assessment results: Weekly delivery; every Monday.

For more information, contact [nccicustomerservice@hq.dhs.gov](mailto:nccicustomerservice@hq.dhs.gov).

## Validated Architecture Design Review

### Description

The Validated Architecture Design Review (VADeR), (formerly known as Cyber Hygiene scanning) is a voluntary, no-cost assessment based on standards, guidelines, and best practices. The assessment encompasses architecture and design review, system configuration, and log file review, and sophisticated analysis of network traffic to develop a detailed representation of the communications, flows, and relationships between devices and most importantly to identify anomalous (and potentially suspicious) communication flows. This offering provides a sophisticated analysis of the asset owner’s network.

### Outcomes

After the review, the NCCIC will provide an in-depth VADeR Report that includes key discoveries and practical recommendations for improving an organization’s operational maturity and enhancing their cybersecurity posture.

### Assessment Logistics

- Execution of the DHS assessment agreement and submission of pre-requisite customer information (to include a network diagram)
- Pre Assessment Activities: two weeks
- Time needed to complete assessment: one week
- Personnel required to perform assessment: customer point of contact responsible for coordinating all customer activity and IT staff to answer system and network related questions
- Timeframe for return of assessment results: six weeks

For more information, contact [nccicustomerservice@hq.dhs.gov](mailto:nccicustomerservice@hq.dhs.gov).

## Cybersecurity Evaluation Tool (CSET®)

### Description

The Cyber Security Evaluation Tool (CSET®) is a no-cost, voluntary desktop stand-alone application that guides asset owners and operators through a systematic process to evaluate their operational technology and I) network security practices. Using the tool organizations are able to evaluate their cybersecurity posture against recognized standards and best practice recommendations in a systematic, disciplined, and repeatable manner.

### Outcomes

At the end of the evaluation, NCCIC will provide integrated dashboards and reports that present the assessment results in both summary and detailed form. Users are easily able to filter content or “drill down” to look at information that is more granular.

### Assessment Logistics

- Download the Tool – The CSET is immediately available for download upon request
- Select Standards – Users select one or more government and industry recognized cybersecurity standards. CSET then generates questions that are specific to those requirements.

- Determine Assurance Level – The security assurance level (SAL) is determined by responses to questions relating to the potential consequences of a successful cyber-attack on an organization, facility, system, or subsystem. It can be selected or calculated and provides a recommended level of cybersecurity rigor necessary to protect against a worst-case event.
- Create a Diagram – CSET contains a graphical user interface that allows users to diagram network topology and identify the “criticality” of the network components. Users can create a diagram from scratch, import a pre-built template diagram, or import an existing MS Visio® diagram. Users are able to define cybersecurity zones, critical components, and network communication paths. An icon palette featuring system and network components allows users to build and modify diagrams by simply dragging and dropping components into place.
- Answer the Questions – CSET then generates questions using the network topology, selected security standards, and SAL as its basis. The assessment team can select the best answer to each question using the organization’s actual network configuration and implemented security policies and procedures. Notes can be entered or files attached to individual questions, flagging them for further review or providing clarification. Each question has associated reference information that is provided for clarification. The system also displays the underlying requirements, any supplemental text, and additional resources to help address the problem identified.

For more information and to get started, visit [ics-cert.us-cert.gov/Downloading-and-Installing-CSET](https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET). To learn more about CSET or to request a physical copy of the software, contact [ncciccustomerservice@hq.dhs.gov](mailto:ncciccustomerservice@hq.dhs.gov) or visit [ics-cert.us-cert.gov](https://ics-cert.us-cert.gov).

## Industrial Control Systems Evaluation

### Description

NCCIC’s ICS subject matter experts (SMEs) provide cybersecurity assessments in partnership with CI owners and operators to strengthen the cybersecurity posture of their industrial control systems. The ICS evaluation is a voluntary, request-based assessment leveraging standards, guidelines, and best practices.

NCCIC will provide an:

- evaluation of ICS architecture,
- analysis of network traffic, and
- systems log review and analysis.

### Outcomes

Following the system analysis, the assessment team analyzes the network data traffic to identify anomalous and potentially suspicious communications sourced from, or destined for, control system assets. This offering provides a sophisticated review of the asset owner’s network traffic, collected by the asset owner, from within their control system network environment. NCCIC ICS SMEs analyze the captured network traffic using a combination of open source and commercially available tools to develop a detailed representation of the communications, flows, and relationships between devices. Lastly, the systems log analysis provides an in-depth evaluation of system log data.

Following the assessment, NCCIC compiles an in-depth report that includes an analysis of key discoveries and practical mitigations for enhancing the organization’s cybersecurity posture. NCCIC provides the report to the asset owner approximately six weeks after the assessment’s completion.

### Data protection

The DHS PCII Program categorically protects all data collected and analysis performed. By law, the PCII Program enables secure, voluntary information sharing between CI owners and operators and the Federal Government. PCII protections mean that DHS cannot publicly disclose PCII and that PCII cannot be used for regulatory purposes. For more information, visit [www.dhs.gov/pcii-program](http://www.dhs.gov/pcii-program) or contact [PCII-Assist@hq.dhs.gov](mailto:PCII-Assist@hq.dhs.gov).

For more information about the Industrial Control Systems Evaluation, contact [nccicustomerservice@hq.dhs.gov](mailto:nccicustomerservice@hq.dhs.gov).

## Detection and Prevention

### Network Protection

#### *Continuous Diagnostics and Mitigation Program*

##### **Description**

The Continuous Diagnostics and Mitigation (CDM) Program fortifies government networks and systems with capabilities and tools. These capabilities and tools identify cybersecurity risks on an ongoing basis; prioritize these risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

The CDM Tools Special Item Number (SIN) supports the DHS CDM Program. The hardware and software products and associated services under this SIN undergo a DHS product qualification process to be added to the CDM Approved Products List. The full list of CDM subcategories includes tools, associated maintenance, and other related activities, such as training. The SIN is organized by CDM capabilities into five subcategories. As shown below, the five CDM Tools SIN subcategories cover the fifteen CDM Tool Functional Areas (TFAs) and allow for future innovation.

The CDM Tools SIN on General Services Administration IT Schedule 70 is available to SLTT entities through the Cooperative Purchasing Agreement. Please reach out to [cdm.arm@hq.dhs.gov](mailto:cdm.arm@hq.dhs.gov) for further information.

##### **Approach**

###### *Manage “What is on the network”*

This subcategory identifies the existence of hardware, software, configuration characteristics, and known security vulnerabilities.

- TFA 1 – Hardware asset management
- TFA 2 – Software asset management
- TFA 3 – Configuration settings management
- TFA 4 – Vulnerability management

###### *Manage “Who is on the network”*

This subcategory identifies and determines the users or systems with access authorization, authenticated permissions, and granted resource rights.

- TFA 6 – Manage trust in people granted access
- TFA 7 – Manage security-related behavior
- TFA 8 – Manage credential and authentication
- TFA 9 – Manage account access and manage privileges

###### *Manage “How is the network protected”*

This subcategory determines the user and system actions and behavior at the network boundaries and

within the computing infrastructure.

- TFA 5 – Manage network access controls

Manage “What is happening on the network”

This subcategory prepares for events and incidents, gathers data from appropriate sources, and identifies incidents through analysis of data.

Due to the complexity to manage “What is happening on the network,” this area is covered by three focus areas:

- “What is happening on the network for Manage Events (MNGEVT)”
  - TFA 10 – Prepare for contingencies and incidents
  - TFA 11 – Respond to contingencies and incidents
- “What is happening on the network for Design and Build in Security ()”
  - TFA 12 – Design and build in requirements policy and planning
  - TFA 13 – Design and build in quality
- “What is happening on the network for Operate, Monitor and Improve ()”
  - TFA 14 – Manage audit information
  - TFA 15 – Manage operation security

Emerging Tools and Technology includes CDM cybersecurity tools and technology not in any other subcategory, such as future innovations.

For more information, visit [us-cert.gov/cdm](https://us-cert.gov/cdm) or send an email to [cdm.arm@hq.dhs.gov](mailto:cdm.arm@hq.dhs.gov) for acquisition related questions or [cdm@hq.dhs.gov](mailto:cdm@hq.dhs.gov) for program and technical questions.

## **Incident Response, Recovery, and Cyber Threat Hunting**

### **Description**

The incident response team falls under the guidance of the NCCIC Hunt and Incident Response Team (HIRT). HIRT provides incident response, management and coordination activities for cyber incidents occurring in the CI sectors as well as Government entities at the Federal, State, Local, Tribal, and Territorial levels. HIRT works with its constituents to identify and contain adversary activity and develop mitigation plans for removal and remediation of root cause. HIRT provides technical expertise and capacity to its constituents in responding to incidents. Incident response efforts focus on finding the root cause of an incident by searching for TTPs along with behaviors and associated artifacts in the victim network.

NIST defines an incident as a computer security incident, a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. HIRT further defines an individual incident as a distinct, potentially malicious event, perpetrated by a single threat actor, using a single TTP; or series of related TTPs, against a single victim. Examples include but are not limited to, malware infections, data theft, data corruption, and ransomware encryption, denial of service, control systems intrusions and threats against assets.

### **Approach**

In support of incident response, HIRT has four types of customer engagements:

- remote assistance,
- advisory deployment,
- remote deployment, and

- on-site deployment.

HIRT incident response is action taken to respond to a suspected incident and address the increased risk resulting from the incident. The goal is to manage the situation in a way that ensures safety, reduces risk, limits damage and reduces recovery time and costs. Most response actions will be technical in nature but any action taken to reduce the impact of an incident is considered part of the incident response. **Following an engagement and upon completion of analysis, the HIRT will deliver an Engagement Report (ER) to the customer within 30-60 days. The ER provides the background, scope, findings, security best practices, and conclusions relevant to the hunt.**

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.

### Approach

- 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, which are 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; 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 (IOC).
- 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 CI.

For more information, visit [www.dhs.gov/cyber](http://www.dhs.gov/cyber). To report cybersecurity incidents and vulnerabilities, call 888-282-0870 or email [nccicustomerservice@hq.dhs.gov](mailto:nccicustomerservice@hq.dhs.gov).

## Malware Analysis

The Advanced Malware Analysis Center provides 24/7 dynamic analysis of malicious code. Stakeholders submit samples via an online website and receive a technical document outlining analysis results. Experts detail recommendations for malware removal and recovery activities. This service can be performed in conjunction 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 as 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 that are extracted from infected systems and submitted to NCCIC for analysis.

To submit malware for analysis, visit [www.malware.us-cert.gov](http://www.malware.us-cert.gov). For further questions or requests, contact [ncciccustomerservice@hq.dhs.gov](mailto:ncciccustomerservice@hq.dhs.gov).

## Information Exchange 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 like malicious IP addresses or the sender's address of a phishing email. AIS is part of a DHS effort to create a cyber ecosystem where as soon as a stakeholder observes an attempted compromise, the cyber threat IOC will be shared in real time with all partners, protecting everyone from that particular threat.

Service benefits include:

- Privacy and civil liberty protection – DHS has taken careful measures to ensure that appropriate 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 provide the following functions:
  - 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 IOCs to ensure the automated processes are operating properly;
  - minimize the amount of data included in an IOC to ensure that its information is directly related to a cyber threat;
  - retain only the information needed to address cyber threats; and
  - ensure that any information collected is used only for network defense or limited law enforcement purposes.
- Sharing at machine speed – AIS enables the bidirectional sharing of IOCs between the Federal Government and AIS partners in real-time by leveraging industry standards for machine-to-

machine communication through the sharing of STIX files through the Trusted Automated eXchange of Indicator Information (TAXII™).

- 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 [www.us-cert.gov/ais](http://www.us-cert.gov/ais).

## Homeland Security Information Network

The Homeland Security Information Network (HSIN) is a trusted network for homeland security mission operations to share sensitive but unclassified information. Federal, SLTT, and private sector partners can use HSIN to manage operations, analyze data, send alerts and notices, and share the information they need to perform their duties. NCCIC-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 are used to indicate expected 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](mailto:HSIN.HelpDesk@hq.dhs.gov). NCCIC TLP:WHITE products are available through [us-cert.gov](http://us-cert.gov) and [ics-cert.gov](http://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 identity 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)
- web conferencing (HSIN Connect)

For more information, or to become a member, visit [www.dhs.gov/homeland-security-information-network-hsin](http://www.dhs.gov/homeland-security-information-network-hsin) or email [HSIN.Outreach@hq.dhs.gov](mailto:HSIN.Outreach@hq.dhs.gov).

## Information Products: National Cyber Awareness System

NCCIC offers no-cost, subscription-based information products to stakeholders through the [www.us-cert.gov](http://www.us-cert.gov) and [www.ics-cert.gov](http://www.ics-cert.gov) websites. NCCIC 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 issues 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 ICS 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 [www.us-cert.gov/ncas](http://www.us-cert.gov/ncas) and [ics-cert.us-cert.gov/](http://ics-cert.us-cert.gov/).

To subscribe to select products, visit [public.govdelivery.com/accounts/USDHSUSCERT/subscriber/new](http://public.govdelivery.com/accounts/USDHSUSCERT/subscriber/new).

## Training and Career Development

### Cybersecurity Exercises

NCCIC provides cyber exercise and incident response planning to support EI partners. NCCIC 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. These events are designed to assist organizations at all levels in the development and testing of cybersecurity prevention, protection, mitigation, and response capabilities.

Exercises range from small discussion-based exercises that last two hours to full-scale, internationally scoped, operations-based exercises that span 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 CI cyberattack.
- Exercise planning and conduct – NCCIC leverages DHS’s Homeland Security Exercise and Evaluation Program (HSEEP) model to plan and conduct a full spectrum of discussion- and operations-based cyber exercises based on stakeholder needs. This 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, NCCIC provides subject matter experts to consult on exercise design and development. NCCIC 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 – SME-run Cyber Planning Workshops are available to assist stakeholders with developing and revising integrated cyber plans.

For more information on cyber exercises, contact [ncciccustomerservice@hq.dhs.gov](mailto:ncciccustomerservice@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 leverage efforts of government, industry, and academia to provide a comprehensive, single resource to address the Nation's cybersecurity knowledge needs.

NICCS is an online resource for cybersecurity training that 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 location 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 their level of expertise, earn a certification, or transition to a new career. Strict vetting criteria for course providers ensure that the courses listed in the catalog are offered by organizations that are recognized as providing quality resources. Each course has been mapped to at least one specialty area within the National Initiative for Cybersecurity Education (NICE) 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](https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework).
- Formal Education –
  - *The National Centers of Academic Excellence (CAE) Program* – Jointly sponsored by DHS and the National Security Administration (NSA), CAE designates specific two- and four-year colleges and universities are designated based on their robust degree programs and alignment to cybersecurity related knowledge units, which have been validated by cybersecurity experts.
  - *The CyberCorps Scholarship for Service (SFS) Program* – The National Science Foundation (NSF) 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 [www.sfs.opm.gov/](http://www.sfs.opm.gov/).
- Workforce Development –
  - *The Cybersecurity Workforce Development Toolkit* – The toolkit helps organizations understand their cybersecurity workforce and staffing needs to protect their information, customers, and networks better. 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](https://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 (KSAs). The NICE Framework provides a common language to speak about cybersecurity jobs and helps with defining 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](https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework).

For more information, visit [niccs.us-cert.gov/](https://niccs.us-cert.gov/) or contact [NICCS@hq.dhs.gov](mailto: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 DHS that is available to federal and SLTT government personnel, veterans, and federal government contractors, and contains more than 800 hours of training on topics such as ethical hacking, surveillance, risk management, and malware analysis. The department's efforts focus on building a strong cyber workforce that can keep up with evolving technology and increasing cybersecurity risks.

Resource benefits include:

- Diverse courses – The program offers more than 300 demonstrations and 3,000 related materials, 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.

For more information, visit [niccs.us-cert.gov/training/federal-virtual-training-environment-fedvte](https://niccs.us-cert.gov/training/federal-virtual-training-environment-fedvte). To register for an account and for more information on available courses, visit [fedvte.usalearning.gov](https://fedvte.usalearning.gov).