**CISA mission**: Lead the collaborative national effort to strengthen the security and resilience of America’s critical infrastructure

In support of that mission: Cybersecurity Advisors (CSAs):

- **Assess**: Evaluate critical infrastructure cyber risk.
- **Promote**: Encourage best practices and risk mitigation strategies.
- **Build**: Initiate, develop capacity, and support cyber communities-of-interest and working groups.
- **Educate**: Inform and raise awareness.
- **Listen**: Collect stakeholder requirements.
- **Coordinate**: Bring together incident support and lessons learned.
CISA assists the public and private sectors secure its networks and focuses on organizations in the following 16 critical infrastructure sectors.
Cyber Security Evaluation Tool (CSET)

**Purpose:** Provides a detailed, effective, and repeatable tool for assessing systems security against established industry standards and guidance.

**Facilitated:** Self-Administered, undertaken independently

**Benefits:**
- Immediately available for download upon request
- Understanding of operational technology and information technology network security practices
- Ability to drill down on specific areas and issues
- Helps to integrate cybersecurity into current corporate risk management strategy

**Time to Execute / Availability:**
- Varies greatly (min 2 Hours) / N/A (self-assessment)
CSET Ransomware Readiness Assessment (RRA)

CSET is a desktop software tool that guides network defenders through a step-by-step process to evaluate their cybersecurity practices on their networks. CSET—applicable to both information technology (IT) and industrial control system (ICS) networks—enables users to perform a comprehensive evaluation of their cybersecurity posture using many recognized government and industry standards and recommendations.

To understand your cybersecurity posture and assess how well your organization is equipped to defend and recover from a ransomware incident, take the Ransomware Readiness Assessment (RRA). The RRA is a self-assessment based on a tiered set of practices to help organizations better assess how well they are equipped to defend and recover from a ransomware incident. The RRA:

- Helps organizations evaluate their cybersecurity posture, with respect to ransomware, against recognized standards and best practice recommendations in a systematic, disciplined, and repeatable manner.
- Guides asset owners and operators through a systematic process to evaluate their operational technology (OT) and information technology (IT) network security practices against the ransomware threat.
- Provides an analysis dashboard with graphs and tables that present the assessment results in both summary and detailed form.

https://github.com/cisagov/cset/releases/tag/v10.3.0.0
Overview: In 2016, DHS launched the External Dependencies Management (EDM) Assessment, focusing specifically on ensuring the protection and sustainment of services and assets that are dependent on the actions of third-party entities.

Background: External Dependencies Management is a domain covered by the CRR. However, EDM and associated issues (e.g., supply-chain management, vendor management) are not addressed at a comprehensive level within the CRR, resulting in the creation of a separate assessment.

Linkages to CRR: Despite operating at a more granular level than the CRR, the EDM Assessment borrows heavily from the CRR’s methodological architecture and scoring system but remains a DHS-facilitated assessment.
To provide the organization with an understandable and useful structure for the evaluation, the EDM Assessment is divided into three distinct areas (domains):

1. **RELATIONSHIP FORMATION** – how the organization considers third party risks, selects external entities, and forms relationships with them so that risk is managed from the start

2. **RELATIONSHIP MANAGEMENT AND GOVERNANCE** – how the organization manages ongoing relationships with external entities to support and strengthen its critical services at a managed level of risk and cost

3. **SERVICE PROTECTION AND SUSTAINMENT** – how the organization plans for, anticipates, and manages disruption or incidents related to external entities
Phishing Campaign Assessment (PCA)

Objectives:
• Increase cybersecurity awareness within stakeholder organizations
• Decrease risk of successful malicious phishing attacks, limit exposure, reduce rates of exploitation

Benefits:
• Receive actionable metrics
• Highlight need for improved security
Training

Scope:
• 6-week engagement period
• Phishing emails capture click-rate only, no payloads will be used
• Varying Levels of Complexity -- Levels 1 - 6 (Easy to Difficult)
Phishing Campaign Assessment (PCA)

<table>
<thead>
<tr>
<th>Week</th>
<th>Campaign</th>
<th>Date Sent</th>
<th>Complexity Level</th>
<th>User Click Rate</th>
<th># Emails Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Please Help!</td>
<td>3/18/16</td>
<td>1</td>
<td>0.17%</td>
<td>401</td>
</tr>
<tr>
<td>2</td>
<td>Reveal Your Past</td>
<td>3/31/16</td>
<td>2</td>
<td>2.54%</td>
<td>402</td>
</tr>
<tr>
<td>3</td>
<td>Password Expire Alert</td>
<td>4/6/16</td>
<td>3</td>
<td>12.62%</td>
<td>401</td>
</tr>
<tr>
<td>4</td>
<td>Severe Weather Checklist</td>
<td>4/15/16</td>
<td>4</td>
<td>7.41%</td>
<td>402</td>
</tr>
<tr>
<td>5</td>
<td>Federal Employee Survey</td>
<td>4/20/16</td>
<td>5</td>
<td>15.57%</td>
<td>401</td>
</tr>
<tr>
<td>6</td>
<td>Salary Guidelines</td>
<td>4/27/16</td>
<td>6</td>
<td>32.03%</td>
<td>402</td>
</tr>
</tbody>
</table>

Click-Rate by Complexity

- Level of Complexity: 1, 2, 3, 4, 5, 6
- User Click Rate: 0.17%, 2.54%, 12.62%, 7.41%, 15.57%, 32.03%
Vulnerability Scanning Service (CyHy)

Assess Internet accessible systems for known vulnerabilities and configuration errors

Work with organization to proactively mitigate threats and risks to systems

**Activities include:**

- **Network Mapping**
  - Identify public IP address space
  - Identify hosts that are active on IP address space
  - Determine the O/S and Services running
  - Re-run scans to determine any changes
  - Graphically represent address space on a map

- **Network Vulnerability & Configuration Scanning**
  - Identify network vulnerabilities and weakness
Web Application Scanning (WAS)

An Internet based scanning service to assess the “health” of your publicly accessible web applications by checking for known vulnerabilities and weak configurations.

SCANNING OBJECTIVES

• Maintain enterprise awareness of your publicly accessible web-based assets
• Provide insight into how systems and infrastructure appear to potential attackers
• Drive proactive mitigation of vulnerabilities to help reduce overall risk

SCANNING PHASES

• Discovery Scanning: Identify active, internet-facing web applications
• Vulnerability Scanning: Initiate non-intrusive checks to identify potential vulnerabilities and configuration weaknesses
Remote Penetration Test (RPT)

Utilizes a dedicated remote team to assess and identify vulnerabilities and work with customers to eliminate exploitable pathways.

- Focuses on externally accessible systems

SCENARIOS:

- **External Penetration Test**: Verifying if the stakeholder network is accessible from the public domain by an unauthorized user by assessing open ports, protocols, and services.

- **External Web Application Test**: Evaluating web applications for potential exploitable vulnerabilities; the test can include automated scanning, manual testing, or a combination of both methods.

- **Phishing Assessment**: Testing through carefully crafted phishing emails containing a variety of malicious payloads to the trusted point of contact.
Additional Cyber Resources
The MS-ISAC is designated by the U.S. Department of Homeland Security as the focal point for cyber threat prevention, protection, response and recovery for the nation’s state, local, tribal and territorial (SLTT) governments including chief information security officers, homeland security advisors and fusion centers.

- Includes representatives from all 50 states, U.S. territories, hundreds of local governments (including all 50 state capital cities), and tribal governments.

- Operates a 24-hour Integrated Intelligence Center that provides real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation and incident response for the nation’s SLTT governments.
The Homeland Security Information Network (HSIN) provides you with a central, online location for information sharing and collaboration.

A network designed by users, for users

A trusted, secure, virtual platform to work with homeland security partners in real-time

A platform that supports daily operations, planned events and exercises, and incident response

Access HSIN 24x7 through your:

Use HSIN if you want to:
- Utilize a trusted, secure network to get information about incidents, plan security for large-scale events or conduct daily operations
- Share information with trusted colleagues and partners for mission support
- Use geospatial tools to map materials, resources and intelligence information
- Chat securely during emergencies or training exercises
- Send alerts and notifications to your qualified colleagues

For more information, contact the HSIN Outreach Team at HSIN.Outreach@hq.dhs.gov or visit our website at www.dhs.gov/hsin.

- If there is a suspected or confirmed cyber attack or incident that:
  - Affects core government or critical infrastructure functions;
  - Results in the loss of data, system availability; or control of systems;
  - Indicates malicious software is present on critical systems

Advanced Malware Analysis Center:

- Provides 24x7 dynamic analyses of malicious code. Stakeholders submit samples via an online website and receive a technical document outlining the results of the analysis. Experts will detail recommendations for malware removal and recovery activities.
- Web Submission: [https://malware.us-cert.gov](https://malware.us-cert.gov)