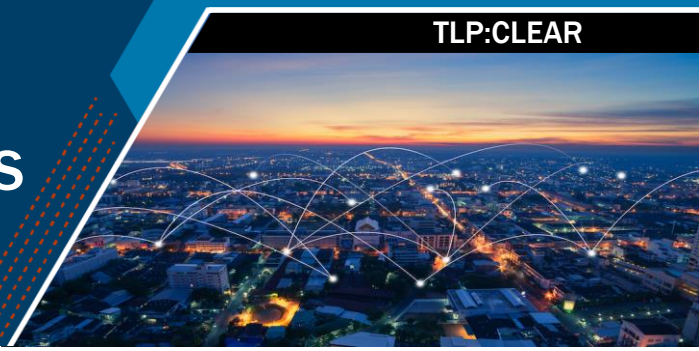
RESOURCES FOR CYBERSECURITY CLINICS



OVERVIEW

The Cybersecurity and Infrastructure Security Agency (CISA) serves as America's cyber defense agency. The agency was established in 2018 within the U.S. Department of Homeland Security and leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure. We offer a variety of resources and services to help organizations defend themselves from cyber threats.

CISA embraces new opportunities to support cybersecurity clinics at higher-education institutions. Clinics play an important role in strengthening the cybersecurity posture of small organizations at the local level. They also help address the national cyber workforce gap by training students with diverse backgrounds to enter a career in cybersecurity.

This guide outlines ways that CISA can partner with and support cybersecurity clinics and their clients.

INFORMATIONAL BRIEFINGS AND PARTNERSHIP

Partnership and collaboration are the heart of CISA's operating model. CISA regularly provides stakeholders informational briefings about cybersecurity best practices, CISA's service offerings, and unclassified and classified threat briefings. CISA's Cybersecurity Advisors are located across the country and serve as key points-of-contact for organizations interacting with CISA and as gateways to the federal government.

- **CISA Speakers:** CISA's outreach provides speakers to groups and events of all shapes and sizes, from keynoting international conferences to roundtables with small groups of stakeholders. Topics can include an overview of current threats, an introduction to CISA and its programs, commentary on current events, deep dives on specific issues, and overviews of government policy and programs. Clinics and their clients can request a speaker through our website.
  - Request a CISA Speaker | CISA

- **Cybersecurity Advisors:** Cybersecurity Advisors are a region-based source of subject-matter expertise for public and private-sector stakeholders. These subject matter experts (SMEs) advise on a range of cybersecurity activities that are aimed at improving our partners' cyber resilience postures and economic security. Advisors offer cyber security assistance to critical infrastructure owners and operators and state, local, territorial, and tribal (SLTT) officials. Advisors also help organizations develop, mature, and manage cybersecurity programs that guard sensitive information, and strengthen their overall risk management capabilities. Advisors introduce organizations to various CISA cyber security products and services, along with other public and private resources, and act as liaisons to CISA cyber programs. Advisors can provide cyber preparedness assessments and protective resources, working group support, leadership guidance, partnership in public-private development, and coordination and support in times of cyber threat, disruption, or attack. Clinics and their clients can establish relationships with their regional CISA office to learn more and take advantage of CISA resources.
  - Get in touch here: CISA Regions | CISA

GUIDANCE

CISA seeks to remain a trusted source of authoritative and actionable guidance for government, industry, and other organizations on cyber risks, vulnerabilities, and incidents. We aim to help organizations prioritize what steps to take first to minimize risk with limited resources. Tailored guidance and awareness campaigns can ensure that organizations know the best ways to protect themselves.

- **Guidance for Small Organizations:** CISA offers specialized guidance for small organizations. Clinics and their clients can use this guidance to help prioritize their cybersecurity efforts.
  - Cyber Guidance for Small Businesses | CISA
  - Partnering to Safeguard K-12 Organizations from Cybersecurity Threats | CISA
  - Healthcare and Public Health Sector | CISA

- **Cybersecurity Performance Goals (CPGs):** CISA and NIST developed baseline cybersecurity performance goals to help small- and medium-sized organizations kickstart their cybersecurity efforts. The CPGs can be leveraged to aid entities in determining the most impactful actions they can take—based on their available resources and capabilities—to meaningfully reduce cyber risk. Clinics and their clients can use this guidance to help prioritize their cybersecurity efforts.
  - Cross-Sector Cybersecurity Performance Goals | CISA

- **StopRansomware.gov:** StopRansomware.gov amasses knowledge spread across the federal government into one website that provides organizations, the general public, federal, SLTT governments, and critical infrastructure organizations free, authoritative information, resources, and tools to help prevent and mitigate ransomware attacks. The content is sourced from CISA and other governmental partners, including the Department of Health and Human Services, the Federal Bureau of Investigation, the National Institute of Standards and Technology, and the U.S. Secret Service. Clinics and their clients can reference this website for useful resources.
  - Stop Ransomware | CISA

- **Incident Response Plans:** Developing a cybersecurity incident response plan is one of the most effective steps any organization can take to protect themselves and be more resilient. CISA's Incident Response Plan Basics provides advice on what to do before, during, and after an incident.
  - Incident Response Plan Basics | CISA

TOOLS AND SERVICES

Small- and medium-sized organizations often do not have the resources to implement priority protections against ransomware attacks. To help close this gap, CISA offers a variety of services to augment and enhance an organization's existing capabilities.

- **CISA Exercises:** CISA provides a comprehensive set of resources designed to assist stakeholders in conducting their own exercises to examine their cybersecurity and physical security plans and capabilities. Organizations can use CISA Tabletop Exercise Packages (CTEPs) to facilitate discussions within organizations centered around their ability to address a variety of threat scenarios—the packages incorporate various cyber threat vectors including ransomware, insider threats, phishing, and industrial control system (ICS) compromise. There are also sector-specific cybersecurity scenarios for elections infrastructure, local governments, maritime ports, water, and healthcare.
  - Cybersecurity Scenarios | CISA

- **Vulnerability Scanning Notifications:** CISA can help infrastructure owners and operators strengthen their cyber hygiene with the aid of multiple tools, including web application scanning (WAS) and vulnerability scanning (VS). WAS and VS return raw data about potential vulnerabilities based on scans of externally facing web applications and static IPv4 addresses provided to CISA by owners and operators. This data is compared against the Common Vulnerabilities and Exposures (CVE) list and is used by CISA to assess areas of risk and gain insight on trends.
  - CYBER HYGIENE SERVICES | CISA

- **Free Commercial Services and Tools Catalog:** CISA has compiled a list of free cybersecurity tools and services to help organizations further advance their security capabilities. This living repository includes cybersecurity

services provided by CISA, widely used open-source tools, and free tools and services offered by private and public sector organizations across the cybersecurity community.
  - Free Cybersecurity Services and Tools | CISA

- **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. The CSET tool includes Ransomware Readiness Assessment (RRA), a self-assessment based on a tiered set of practices to help organizations better assess how well they are equipped to defend against and recover from a ransomware incident. Clinics and their clients can use this resource to help prioritize their cybersecurity efforts.
  - Downloading and Installing CSET | CISA

- **MS-ISAC and EI-ISAC:** CISA funds the Multi-State Information Sharing and Analysis Center (MS-ISAC) and Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) through a cooperative agreement with a non-profit organization that manages the free cybersecurity services provided to members. The MS-ISAC is open to SLTT entities of all types, including but not limited to SLTT government agencies, law enforcement, educational institutions, public utilities, and transportation authorities. This does not include private universities. The EI-ISAC is a membership-based collaborative that is open to U.S. elections entities. Members of each receive direct access to a suite of services and informational products that can help entities defend against and educate themselves about cyber intrusions. Services and products include cybersecurity advisories and alerts, a 24-7 SOC, vulnerability assessments, incident response support, secure information sharing, tabletop exercises, malicious domains/IP blocking and reports, and more.
  - MS-ISAC (cisecurity.org)
  - EI-ISAC (cisecurity.org)

GRANTS

In 2021, Congress established a four-year $1 billion grant program, managed by CISA and administered by FEMA, to help state, local, tribal, and territorial governments strengthen their cyber posture and become more resilient to cyber threats. Under the SLCGP, recipients can allocate funding towards mitigating ransomware risks, so long as expenditures directly align to their CISA-approved cybersecurity plan. The funds are passed from CISA to each state for distribution. Clinics and their clients can check with their respective state agency to understand what funds may be available to them. Additionally, some states may allow grant funds to be used by universities to strengthen their clinics or start new clinics.

  - State and Local Cybersecurity Grant Program | CISA