CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

On November 16, 2018, the Cybersecurity and Infrastructure Security Agency Act of 2018 was signed into law and elevates the mission of the former National Protection and Programs Directorate (NPPD) within DHS and establishes the Cybersecurity and Infrastructure Security Agency (CISA).

- CISA leads the national effort to *defend* critical infrastructure against the threats of *today*, while working with partners across all levels of government and in the private sector to *secure* against the evolving risks of *tomorrow*.
- The name CISA brings recognition to the work being done, improving it's ability to engage with partners and stakeholders, and recruit top cybersecurity talent.

What Does CISA Do?

CISA is responsible for protecting the Nation's critical infrastructure from physical and cyber threats. This mission requires effective coordination and collaboration among a broad spectrum of government and private sector organizations.

Comprehensive Cyber Protection:

- The CISA Central provides 24x7 cyber situational awareness, analysis, incident response and cyber defense capabilities to the Federal government; state, local, tribal and territorial governments; the private sector and international partners.
- CISA provides cybersecurity tools, incident response services and assessment capabilities to safeguard the networks that support the essential operations of federal civilian departments and agencies.

Infrastructure Resilience:

- CISA coordinates security and resilience efforts using trusted partnerships across the private and public sectors, and delivers training, technical assistance, and assessments to federal stakeholders as well as to infrastructure owners and operators nationwide.
- CISA provides consolidated all-hazards risk analysis for U.S. critical infrastructure through the National Risk Management Center.

Emergency Communications:

- CISA enhances public safety interoperable communications at all levels of government, providing training, coordination, tools and guidance to help partners across the country develop their emergency communications capabilities.
- Working with stakeholders across the country, CISA conducts extensive, nationwide outreach to support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters.

Organizational Changes Related to the CISA Act

The CISA Act establishes three divisions in the new agency: Cybersecurity, Infrastructure Security and Emergency Communications.

- The Act transfers the Office of Biometrics Identity Management (OBIM) to DHS's Management Directorate. Placement within the DHS Headquarters supports expanded collaboration and ensures OBIM's capabilities are available across the DHS enterprise and the interagency.
- The bill provides the Secretary of Homeland Security the flexibility to determine an alignment of the Federal Protective Service (FPS) that best supports its critical role of protecting federal employees and securing federal facilities across the nation and territories.

CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

CISA ASSESSMENTS

The CISA Assessments team supports Federal, State, Local, Tribal and Territorial Governments and Critical Infrastructure partners by providing proactive testing and assessment services. The team also provides an objective third-party perspective of stakeholder operational cybersecurity posture and identifies security control strengths and weaknesses. CISA Assessments aggregates these insights into actionable reports that champion the implementation of mitigations and controls capable of positive impact toward overall risk reduction.

OBJECTIVES

- Reduce Stakeholder Risk
- Enable Data-Driven Decision
- Influence Operational Behaviors
- Increase National Resilience

SERVICE OFFERINGS

- **Vulnerability Scanning** is the persistent scanning of internet-accessible systems for vulnerabilities, configuration errors, and suboptimal security practices.
- **Phishing Campaign Assessments** measure propensity to click on email phishing lures which increases organizational training and awareness.
- **Remote Penetration Testing** focuses on testing a stakeholder's internet exposure.
- **Risk and Vulnerability Assessments** combine national threat information with data collected and vulnerabilities identified through on-site assessment activities to provide tailored risk analysis reports.
- **Red Team Assessments** closely mirror an attack by an advanced adversary to test operational capabilities and maturity.
- **Validated Architecture Design Review** evaluates the resiliency of a stakeholder's systems, networks and security services.
- **Third-Party Qualification** qualifies third-party organizations to perform assessments and technical services following CISA Assessments standards, process and procedures.
- **Critical Product Evaluations** assess, within an isolated environment, the "out-of-the-box" security of products and solutions relevant to critical infrastructure operations and national resilience.
- **Cyber Resilience Review** identifies and evaluates cyber security management capabilities, maturity, and capacity to manage cyber risk during normal operations and times of operational stress.
- **External Dependency Management** assesses the activities and practices utilized by an organization to manage risks arising from external dependencies.
- **Cyber Infrastructure Survey** identifies cybersecurity controls and protective measures in place and provides an interactive dashboard for comparative analysis and valuation.

ABOUT

Our Team

The CISA Assessments team is a group of highly trained information security experts. Our mission is to measurably reduce cybersecurity risks to our Nation.

CISA leads the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

Our Services provide:

- **A proactive, risk-based approach** to analyzing stakeholder systems
- **Expertise** in identification of vulnerabilities, risk evaluation, and prioritized mitigation guidance
- **Comprehensive services that empower stakeholders** to increase speed and effectiveness of their cyber response capabilities.

Additional Information

CISA assessments' security services are available at no cost. Stakeholders include Federal, State, Local, Tribal and Territorial governments, as well as Critical Infrastructure private sector companies. CISA does not share attributable information without written and agreed consent from the stakeholder. CISA uses anonymized data to develop non-attributed reports for trending and analysis purposes.

GET STARTED

Capabilities and service delivery timelines are available upon request. Service availability is limited. Contact us at **Central@cisa.dhs.gov** to get started. Service delivery queues are prioritized on a continuous basis to ensure no stakeholder or sector receives a disproportionate amount of resources and that the data collected is a diverse representation of the nation.

MISSION AND VISION

Mission: *Providing cybersecurity assessments to facilitate the identification of risk for the purpose of protecting the Nation's cyber infrastructure.*

Vision: *To be the preeminent government leader providing comprehensive, innovative, and dynamic cybersecurity assessments for the purpose of facilitating and protecting the federal, state, private sector and critical infrastructure networks of the United States, reducing attack surfaces, eliminating threats, and fostering partnerships across the government landscape.*

CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

CYBERSECURITY ASSESSMENTS SUMMARY

Name	Cyber Resilience Review (CRR)	External Dependency Management (EDM) Assessment	Cyber Infrastructure Survey (CIS)	Onsite Cyber Security Evaluation Tool (CSET) Assessment
Purpose and Value Proposition	Identifies and evaluates cyber security management capabilities, maturity, and capacity to manage cyber risk during normal operations and times of operational stress.	Assesses the activities and practices utilized by an organization to manage risks arising from external dependencies.	Identifies cybersecurity controls and protective measures in place and provides an interactive dashboard for comparative analysis and valuation.	Provides a detailed, effective, and repeatable tool for assessing systems security against established industry standards and guidance
Scope	Critical Service view	Critical Service view	Critical Service view	Information Technology and Operational Technology systems
Time to Execute/ Availability	5 to 6 Hours / Within 2 – 4 weeks	3 – 4 Hours / Within 2 – 4 weeks	2 ½ to 4 Hours / Within 2 – 4 weeks	Varies greatly (min 2 Hours) / N/A (self-assessment)
Information Sought	Capabilities and maturity indicators in 10 security domains	Capabilities and maturity indicators across third party relationship management lifecycle domains	Protective measures in-place	Architecture diagrams, infrastructure, policies, and procedures documents
Preparation	Planning call to scope evaluation	Planning call to scope evaluation	Planning call to scope evaluation	Self-assessment available from web site and utilized locally
Participants	IT/Security Manager, Continuity Planner, and Incident Responders	IT/Security Manager, Continuity Planner, with Contract Management	IT/Security Manager	Operators, engineers, IT staff, policy/ management personnel, and subject matter experts

CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

CYBERSECURITY ASSESSMENTS SUMMARY

Name	Validated Architecture Design Review (VADR)	Phishing Campaign Assessment (PCA)	Vulnerability Scanning (Formally Cyber Hygiene)	Remote Penetration Test (RPT)	Network Risk and Vulnerability Assessment (RVA)
Purpose	Provide analysis and representation of asset owner's network traffic, data flows, and device relationships and identifies anomalous communications flows.	Measure the susceptibility of an organization's personnel to social engineering attacks, specifically email phishing attacks.	Identify public-facing Internet security risks, through service enumeration and vulnerability scanning	Perform external penetration testing and security services to identify risks and externally exploitable pathways into systems, networks and applications.	Perform penetration testing and security services to identify risks and vulnerabilities within IT systems, networks and applications
Scope	Industrial Control Systems / Network Architecture/ Network Traffic	Organization / Business Unit / Email Service	Public-Facing, Network-Based IT Service	Organization / Business Unit / Network-Based IT Service	Organization / Business Unit / Network-Based IT Service
Time to Execute / Availability	Variable (Hours to Days) / Case by case	Approximately 6 Weeks / Within 2-6 months	Continuous / Within 2-3 days	Up to 6 weeks / 3 – 6 months	Two weeks of testing / 9 – 15 months
Information Sought	Network design, system configurations, log files, interdependencies, and its applications	Phishing "click rate" metrics compared to attach sophistication	Network service and vulnerability information	Network, Database, Application scope and/or access to be tested with various security tools	Network, Database, Application scope and/or access to be tested with various security tools
Preparation	Coordinated via Email. Planning calls	Formal rules of engagement and pre-planning	Signed agreement letter and IP address scope to be tested	Formal rules of engagement and extensive pre-planning	Formal rules of engagement and extensive pre-planning
Participants	Control system operators/ engineers, IT personnel, and OT personnel	IT/Security Manager, Network Administrators, end users	IT/Security Manager and Network Administrators	Management stakeholders, IT/Security Manager, Network Administrators & System Owners.	Management stakeholders, IT/Security Manager, Network Administrators, and System Owners.