

CYBERSECURITY + INFRASTRUCTURE SECURITY AGENCY

SERVICES



Fall 2022

SERVICES DIRECTORY

Select the option that best describes your organization:



SERVICES



ACADEMIA



Cybersecurity

BROWSE BY TYPE



Capacity Building Services



Capacity Building Level: ● ○ ○

CISA Tabletop Exercise Packages

CISA Tabletop Exercise Packages (CTEP) assist stakeholders in conducting their own tabletop exercises by providing exercise planners with tools, scenarios, question sets, and guidance to support the development of discussion-based exercises.

CISA.Exercises@cisa.dhs.gov

Capacity Building Level: ● ○ ○

Multi-State Information Sharing and Analysis Center

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a membership-based collaborative that serves as the central cybersecurity resource for the nation's state, local, tribal, and territorial governments.

info@msisac.org

Capacity Building Level: ● ○ ○

Stakeholder Exercises

Planning with a range of stakeholders to develop and conduct preparedness exercises.

CISA.Exercises@cisa.dhs.gov



Incident Response Services



Incident Response Level: ● ○ ○

Multi-State Information Sharing and Analysis Center

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a membership-based collaborative that serves as the central cybersecurity resource for the nation's state, local, tribal, and territorial governments.

info@msisac.org



Information Sharing Services



Information Sharing Level: ● ○ ○

Multi-State Information Sharing and Analysis Center

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a membership-based collaborative that serves as the central cybersecurity resource for the nation's state, local, tribal, and territorial governments.

info@msisac.org



Risk Assessment Services



Risk Assessment Level: ● ○ ○

Multi-State Information Sharing and Analysis Center

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a membership-based collaborative that serves as the central cybersecurity resource for the nation's state, local, tribal, and territorial governments.

info@msisac.org

Risk Assessment Level: ● ○ ○

Vulnerability Scanning

CISA offers organizations continual vulnerability scanning of internet-accessible systems.

vulnerability@cisa.dhs.gov



Partnership Development Services



Partnership Development Level: ● ○ ○

Multi-State Information Sharing and Analysis Center

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a membership-based collaborative that serves as the central cybersecurity resource for the nation's state, local, tribal, and territorial governments.

info@msisac.org

Many CISA services involve the close coordination and sharing of sensitive information between CISA and the organization receiving the service. To facilitate these partnerships, such organizations receive protections under the Protected Critical Infrastructure Information (PCII) Program. For more information on the PCII Program, visit <https://www.cisa.gov/pcii-program>.



BROWSE BY TYPE



Capacity Building Services



Capacity Building Level: ● ○ ○

Active Shooter Preparedness Webinar

A webinar that provides information and resources to more effectively prepare for, mitigate the impacts of, and respond to an active shooter incident.

ASworkshop@hq.dhs.gov

Capacity Building Level: ● ○ ○

ChemLock Exercises

CISA's ChemLock exercises and drills can help a facility with dangerous chemicals that has a security plan in place identify best practices, lessons learned, and areas for improvement in plans and procedures.

ChemLock@cisa.dhs.gov

Capacity Building Level: ● ○ ○

ChemLock On-Site Assessments and Assistance

CISA's ChemLock on-site assessments and assistance can help facilities assess the risk of dangerous chemicals at the facility and then develop a security plan that addresses those risks.

ChemLock@cisa.dhs.gov

Capacity Building Level: ● ○ ○

ChemLock Training

CISA's ChemLock offers training to assist with understanding the risks that chemicals pose and what security measures can be put into place to reduce the risk of dangerous chemicals being weaponized.

ChemLock@cisa.dhs.gov

Capacity Building Level: ● ○ ○

CISA Tabletop Exercise Packages

CISA Tabletop Exercise Packages (CTEP) assist stakeholders in conducting their own tabletop exercises by providing exercise planners with tools, scenarios, question sets, and guidance to support the development of discussion-based exercises.

CISA.Exercises@cisa.dhs.gov

Capacity Building Level: ● ○ ○

Stakeholder Exercises

Planning with a range of stakeholders to develop and conduct preparedness exercises.

CISA.Exercises@cisa.dhs.gov



Incident Response Services



Incident Response Level: ● ○ ○

Active Shooter Preparedness Webinar

A webinar that provides information and resources to more effectively prepare for, mitigate the impacts of, and respond to an active shooter incident.

ASworkshop@hq.dhs.gov

Incident Response Level: ● ○ ○

Explosive Blast Modeling Assessment

A detailed technical assessment that provides stakeholders with a visual model of their facility's structural vulnerabilities and soft-targets against improvised explosive devices.

OBP@cisa.dhs.gov

Incident Response Level: ● ● ○

Special Event and Domestic Incident Tracker Tool

Special Event and Domestic Incident Tracker (SEDIT) Tool is a planning capability that integrates security and resilience data to create scenarios to make decisions regarding the impact, protection, mitigation, response, and recovery efforts.

CISA-GatewayHelpDesk@cisa.dhs.gov



Information Sharing Services



Information Sharing Level: ● ○ ○

CISA Gateway

The CISA Gateway provides various data collection, analysis, and response tools in one integrated system, streamlining access to CISA tools and datasets by leveraging a single user registration, management, and authentication process.

CISA-GatewayHelpDesk@cisa.dhs.gov

Information Sharing Level: ● ○ ○

Explosive Blast Modeling Assessment

A detailed technical assessment that provides stakeholders with a visual model of their facility's structural vulnerabilities and soft-targets against improvised explosive devices.

OBP@cisa.dhs.gov



Risk Assessment Services



Risk Assessment Level: ● ○ ○

ChemLock On-Site Assessments and Assistance

CISA's ChemLock on-site assessments and assistance can help facilities assess the risk of dangerous chemicals at the facility and then develop a security plan that addresses those risks.

ChemLock@cisa.dhs.gov

Risk Assessment Level: ● ○ ○

Explosive Blast Modeling Assessment

A detailed technical assessment that provides stakeholders with a visual model of their facility's structural vulnerabilities and soft-targets against improvised explosive devices.

OBP@cisa.dhs.gov



Partnership Development Services



Partnership Development Level: ● ○ ○

Active Shooter Preparedness Webinar

A webinar that provides information and resources to more effectively prepare for, mitigate the impacts of, and respond to an active shooter incident.

ASworkshop@hq.dhs.gov

Partnership Development Level: ● ○ ○

Explosive Blast Modeling Assessment

A detailed technical assessment that provides stakeholders with a visual model of their facility's structural vulnerabilities and soft-targets against improvised explosive devices.

OBP@cisa.dhs.gov

Many CISA services involve the close coordination and sharing of sensitive information between CISA and the organization receiving the service. To facilitate these partnerships, such organizations receive protections under the Protected Critical Infrastructure Information (PCII) Program. For more information on the PCII Program, visit <https://www.cisa.gov/pcii-program>.



SERVICES



FEDERAL



Communications

BROWSE BY TYPE



Capacity Building Services



Capacity Building Level: ● ○ ○

Interoperable Communications Technical Assistance Program

A portfolio of no-cost technical assistance available to all 56 states and territories and federally recognized tribes to help solve communications interoperability issues.

ECD@cisa.dhs.gov



Incident Response Services



Incident Response Level: ● ○ ○

Government Emergency Telecommunications Service

Provides national security and emergency preparedness personnel with end-to-end priority on landline networks.

ECD@cisa.dhs.gov

Incident Response Level: ● ○ ○

Telecommunications Service Priority Program

Provides national security and emergency preparedness organizations with priority repair and installation of vital voice and data circuits.

ECD@cisa.dhs.gov

Incident Response Level: ● ○ ○

Wireless Priority Service

Provides national security and emergency preparedness personnel with priority access and processing on cellular networks.

ECD@cisa.dhs.gov

Many CISA services involve the close coordination and sharing of sensitive information between CISA and the organization receiving the service. To facilitate these partnerships, such organizations receive protections under the Protected Critical Infrastructure Information (PCII) Program. For more information on the PCII Program, visit <https://www.cisa.gov/pcii-program>.



BROWSE BY TYPE



Capacity Building Services



Capacity Building Level: ● ● ●

Assessment Evaluation and Standardization

The Assessment Evaluation and Standardization (AES) training is a free, in-person and virtual training program during which participants learn how to conduct CISA cyber assessments.

CSD_VM_Methodology@cisa.dhs.gov

Capacity Building Level: ● ○ ○

CISA Tabletop Exercise Packages

CISA Tabletop Exercise Packages (CTEP) assist stakeholders in conducting their own tabletop exercises by providing exercise planners with tools, scenarios, question sets, and guidance to support the development of discussion-based exercises.

CISA.Exercises@cisa.dhs.gov

Capacity Building Level: ● ○ ○

Continuous Diagnostics and Mitigation

The CDM Program delivers cybersecurity tools, integration services, and dashboards that help federal civilian agencies, as well as non-Chief Financial Officer (CFO) Act agencies through the Shared Services Platform, improve their cybersecurity posture.

CDM@cisa.dhs.gov

Capacity Building Level: ● ● ○

Cyber Storm

CISA-sponsored cybersecurity exercise that simulates a large-scale, coordinated cyber-attack impacting critical infrastructure.

cyberstorm@hq.dhs.gov

Capacity Building Level: ● ○ ○

CyberStat Workshops

Workshops during which participants will build tangible solutions to address common problems across the Federal enterprise.

cyberstat@cisa.dhs.gov

Capacity Building Level: ● ● ●

EINSTEIN 3 Accelerated Capability Training

Provides introductory and ongoing training and mentoring on the EINSTEIN 3 capability of securing civilian Federal networks.

Central@cisa.gov

Capacity Building Level: ● ○ ○

Federal Virtual Training Environment

The Federal Virtual Training Environment (FedVTE) offers free online, on-demand cybersecurity training system that contains more than 800 hours of training for state, local, tribal, and territorial government personnel and veterans.

education@cisa.dhs.gov

Capacity Building Level: ● ● ●

High Value Asset Assessment

A risk based evaluation of the security posture of a federal High Value Asset in accordance with OMB M-19-03.

HVAPMO@cisa.dhs.gov

Capacity Building Level: ● ○ ○

Protective Domain Name System Resolver

CISA's Protective Domain Name System (DNS) Resolver Service is the evolution and successor to the DNS egress protection capability currently being delivered through E3A DNS Sinkhole.

Christopher.Villas@cisa.dhs.gov

Capacity Building Level: ● ○ ○

Stakeholder Exercises

Planning with a range of stakeholders to develop and conduct preparedness exercises.

CISA.Exercises@cisa.dhs.gov

Capacity Building Level: ● ○ ○

Vulnerability Disclosure Policy Platform

CISA's Vulnerability Disclosure Policy (VDP) Platform provides participating agencies with a centrally managed system to intake vulnerability reports and information from, and collaborate with, security researchers from the general public to improve the security of internet-accessible systems.

QSMO@cisa.dhs.gov



Incident Response Services



Incident Response Level: ● ○ ○

Cyber Incident Response

For cybersecurity incidents that have a national security interest and align with national priorities, CISA provides incident response augmentation, artifact analysis, and coordination assistance.

<https://us-cert.cisa.gov/forms/report>

Incident Response Level: ● ○ ○

Malware Analysis

CISA's Malware Analysis service provides stakeholders a dynamic analysis of malicious code, including recommendations for malware removal and recovery activities.

<https://www.malware.us-cert.gov/>

Incident Response Level: ● ● ○

National Cybersecurity Protection System

System-of-systems with a range of capabilities that enables CISA to secure and defend the Federal Government's IT infrastructure.

Central@cisa.gov

Incident Response Level: ● ○ ○

Vulnerability Disclosure Policy Platform

CISA's Vulnerability Disclosure Policy (VDP) Platform provides participating agencies with a centrally managed system to intake vulnerability reports and information from, and collaborate with, security researchers from the general public to improve the security of internet-accessible systems.

QSMO@cisa.dhs.gov



Information Sharing Services



Information Sharing Level: ● ● ○

Automated Indicator Sharing

Enables the exchange of cyber threat indicators with SLTT governments and the private sector at machine speed.

cyberservices@cisa.dhs.gov

Information Sharing Level: ● ○ ○

Homeland Security Information Network: CISA Cyber Portal

Department of Homeland Security's official system for sharing sensitive but unclassified information.

HSIN.Helpdesk@cisa.dhs.gov

Information Sharing Level: ● ○ ○

National Cyber Awareness System

Situational awareness tool for technical and non-technical audiences that provides timely information about cybersecurity threats and issues.

<https://us-cert.cisa.gov/mailing-lists-and-feeds>

Information Sharing Level: ● ○ ○

Shared Cybersecurity Services

Commercial cyber threat feed subscriptions for Federal Civilian Agencies, State Fusion Centers, the MS-ISAC, and the EI-ISAC

CISA_CTIS.SCS_Info@cisa.dhs.gov

Information Sharing Level: ● ○ ○

Vulnerability Disclosure Policy Platform

CISA's Vulnerability Disclosure Policy (VDP) Platform provides participating agencies with a centrally managed system to intake vulnerability reports and information from, and collaborate with, security researchers from the general public to improve the security of internet-accessible systems.

QSMO@cisa.dhs.gov

Risk Assessment Services

Risk Assessment Level: ● ○ ○

Cyber Infrastructure Survey

An assessment that evaluates the effectiveness of organizational security controls, cybersecurity preparedness, and overall resilience.

iodregionaloperations@cisa.dhs.gov

Risk Assessment Level: ● ● ●

Cyber Resilience Review

An assessment that evaluates an organization's operational resilience and cybersecurity practices.

iodregionaloperations@cisa.dhs.gov

Risk Assessment Level: ● ○ ○

Cyber Threat Hunting

CISA provides cyber hunting services focused on specific threat actors and their associated tactics, techniques, and procedures.

Central@cisa.gov

Risk Assessment Level: ● ● ○

External Dependencies Management Assessment

An assessment for organizations to learn how to manage risks arising from external dependencies within the supply chain.

cyberadvisor@cisa.dhs.gov

Risk Assessment Level: ● ○ ○

Federal Incident Response Evaluation

Evaluates an organization's cybersecurity incident management and response capabilities.

CyberLiaison@hq.dhs.gov

Risk Assessment Level: ● ○ ○

Vulnerability Scanning

CISA offers organizations continual vulnerability scanning of internet-accessible systems.

vulnerability@cisa.dhs.gov

Many CISA services involve the close coordination and sharing of sensitive information between CISA and the organization receiving the service. To facilitate these partnerships, such organizations receive protections under the Protected Critical Infrastructure Information (PCII) Program. For more information on the PCII Program, visit <https://www.cisa.gov/pcii-program>.



BROWSE BY TYPE



Capacity Building Services



Capacity Building Level: ● ○ ○

Active Shooter Preparedness Webinar

A webinar that provides information and resources to more effectively prepare for, mitigate the impacts of, and respond to an active shooter incident.

ASworkshop@hq.dhs.gov

Capacity Building Level: ● ○ ○

CISA Tabletop Exercise Packages

CISA Tabletop Exercise Packages (CTEP) assist stakeholders in conducting their own tabletop exercises by providing exercise planners with tools, scenarios, question sets, and guidance to support the development of discussion-based exercises.

CISA.Exercises@cisa.dhs.gov

Capacity Building Level: ● ● ○

Counter-Improvised Explosive Device and Risk Mitigation Training

Training courses to educate on strategies to prevent, protect against, respond to, and mitigate bombing incidents.

OBPTraining@cisa.dhs.gov

Capacity Building Level: ● ● ○

Interagency Security Committee Compliance Assistance

Assistance includes both technical training on the Interagency Security Committee's (ISC) Compliance System as well as continuing education on the ISC's policies and standards.

isccs-support@hq.dhs.gov

Capacity Building Level: ● ○ ○

Interagency Security Committee Risk Management Process Training

This half-day, instructor-led course is a prerequisite for Facility Security Committee membership and covers the Risk Management Process.

rmp_fsctrng@cisa.dhs.gov

Capacity Building Level: ● ○ ○

Stakeholder Exercises

Planning with a range of stakeholders to develop and conduct preparedness exercises.

CISA.Exercises@cisa.dhs.gov



Incident Response Services



Incident Response Level: ● ○ ○

Active Shooter Preparedness Webinar

A webinar that provides information and resources to more effectively prepare for, mitigate the impacts of, and respond to an active shooter incident.

ASworkshop@hq.dhs.gov

Incident Response Level: ● ○ ○

Explosive Blast Modeling Assessment

A detailed technical assessment that provides stakeholders with a visual model of their facility's structural vulnerabilities and soft-targets against improvised explosive devices.

OBP@cisa.dhs.gov

Incident Response Level: ● ● ○

Special Event and Domestic Incident Tracker Tool

Special Event and Domestic Incident Tracker (SEdit) Tool is a planning capability that integrates security and resilience data to create scenarios to make decisions regarding the impact, protection, mitigation, response, and recovery efforts.

CISA-GatewayHelpDesk@cisa.dhs.gov



Information Sharing Services



Information Sharing Level: ● ○ ○

CISA Gateway

The CISA Gateway provides various data collection, analysis, and response tools in one integrated system, streamlining access to CISA tools and datasets by leveraging a single user registration, management, and authentication process.

CISA-GatewayHelpDesk@cisa.dhs.gov

Information Sharing Level: ● ○ ○

Explosive Blast Modeling Assessment

A detailed technical assessment that provides stakeholders with a visual model of their facility's structural vulnerabilities and soft-targets against improvised explosive devices.

OBP@cisa.dhs.gov

Information Sharing Level: ● ○ ○

Homeland Security Information Network - Critical Infrastructure

The Homeland Security Information Network's Critical Infrastructure (HSIN-CI) network is the Department of Homeland Security's online platform for collaboration in protecting the nation's critical infrastructure.

HSINCI@hq.dhs.gov

Information Sharing Level: ● ○ ○

Technical Resource for Incident Prevention

A cross-sector, resource-sharing portal to increase awareness of evolving improvised explosive device tactics, techniques, and procedures.

TRIPwireHelp@cisa.dhs.gov



Risk Assessment Services



Risk Assessment Level: ● ○ ○

Explosive Blast Modeling Assessment

A detailed technical assessment that provides stakeholders with a visual model of their facility's structural vulnerabilities and soft-targets against improvised explosive devices.

OBP@cisa.dhs.gov

Risk Assessment Level: ● ● ○

Infrastructure Visualization Platform

Data collection and presentation tool that supports critical infrastructure security, special event planning, and responsive operations.

isdassessments@cisa.dhs.gov

Risk Assessment Level: ● ● ○

National Counter-Improvised Explosive Device Capabilities Analysis Database

An assessment program that analyzes the capabilities of bomb squads; explosives detection canine teams; dive teams; and special weapons and tactics teams.

NCCAD@cisa.dhs.gov

Risk Assessment Level: ● ○ ○

Regional Resiliency Assessment Program

Provides voluntary collaborative assessments to improve the resilience of a region's critical infrastructure.

resilience@cisa.dhs.gov

Partnership Development Services

Partnership Development Level: ● ○ ○

Active Shooter Preparedness Webinar

A webinar that provides information and resources to more effectively prepare for, mitigate the impacts of, and respond to an active shooter incident.

ASworkshop@hq.dhs.gov

Partnership Development Level: ● ○ ○

Explosive Blast Modeling Assessment

A detailed technical assessment that provides stakeholders with a visual model of their facility's structural vulnerabilities and soft-targets against improvised explosive devices.

OBP@cisa.dhs.gov



SERVICES



INDUSTRY



Communications

BROWSE BY TYPE



Incident Response Services



Incident Response Level: ● ○ ○

Government Emergency Telecommunications Service

Provides national security and emergency preparedness personnel with end-to-end priority on landline networks.

ECD@cisa.dhs.gov

Incident Response Level: ● ○ ○

Telecommunications Service Priority Program

Provides national security and emergency preparedness organizations with priority repair and installation of vital voice and data circuits.

ECD@cisa.dhs.gov

Incident Response Level: ● ○ ○

Wireless Priority Service

Provides national security and emergency preparedness personnel with priority access and processing on cellular networks.

ECD@cisa.dhs.gov

Many CISA services involve the close coordination and sharing of sensitive information between CISA and the organization receiving the service. To facilitate these partnerships, such organizations receive protections under the Protected Critical Infrastructure Information (PCII) Program. For more information on the PCII Program, visit <https://www.cisa.gov/pcii-program>.



BROWSE BY TYPE



Capacity Building Services



Capacity Building Level: ● ● ●

Assessment Evaluation and Standardization Training

In-person and virtual training program during which participants learn how to conduct CISA cyber assessments.

CSD_VM_Methodology@cisa.dhs.gov

Capacity Building Level: ● ○ ○

CISA Tabletop Exercise Packages

CISA Tabletop Exercise Packages (CTEP) assist stakeholders in conducting their own tabletop exercises by providing exercise planners with tools, scenarios, question sets, and guidance to support the development of discussion-based exercises.

CISA.Exercises@cisa.dhs.gov

Capacity Building Level: ● ● ○

Cyber Storm

CISA-sponsored cybersecurity exercise that simulates a large-scale, coordinated cyber-attack impacting critical infrastructure.

cyberstorm@hq.dhs.gov

Capacity Building Level: ● ● ○

Enhanced Cybersecurity Services

Partnership between CISA and commercial service providers to detect and block malicious traffic entering or exiting customer networks (Note: Cost may apply).

ECS_Program@hq.dhs.gov

Capacity Building Level: ● ○ ○

Federal Virtual Training Environment

The Federal Virtual Training Environment (FedVTE) offers free online, on-demand cybersecurity training system that contains more than 800 hours of training for state, local, tribal, and territorial government personnel and veterans.

education@cisa.dhs.gov

Capacity Building Level: ● ○ ○

Stakeholder Exercises

Planning with a range of stakeholders to develop and conduct preparedness exercises.

CISA.Exercises@cisa.dhs.gov



Incident Response Services



Incident Response Level: ● ○ ○

Cyber Incident Response

For cybersecurity incidents that have a national security interest and align with national priorities, CISA provides incident response augmentation, artifact analysis, and coordination assistance.

<https://us-cert.cisa.gov/forms/report>

Incident Response Level: ● ○ ○

Malware Analysis

CISA's Malware Analysis service provides stakeholders a dynamic analysis of malicious code, including recommendations for malware removal and recovery activities.

<https://www.malware.us-cert.gov/>



Information Sharing Services



Information Sharing Level: ● ● ○

Automated Indicator Sharing

Enables the exchange of cyber threat indicators with SLTT governments and the private sector at machine speed.

cyberservices@cisa.dhs.gov

Information Sharing Level: ● ○ ○

Homeland Security Information Network CISA Cyber Portal

Department of Homeland Security's official system for sharing sensitive but unclassified information.

HSIN.Helpdesk@hq.dhs.gov

Information Sharing Level: ● ○ ○

National Cyber Awareness System

Situational awareness tool for technical and non-technical audiences that provides timely information about cybersecurity threats and issues.

<https://us-cert.cisa.gov/mailing-lists-and-feeds>



Risk Assessment Services



Risk Assessment Level: ● ○ ○

Cyber Infrastructure Survey

An assessment that evaluates the effectiveness of organizational security controls, cybersecurity preparedness, and overall resilience.

iodregionaloperations@cisa.dhs.gov

Risk Assessment Level: ● ● ●

Cyber Resilience Review

An assessment that evaluates an organization's operational resilience and cybersecurity practices.

iodregionaloperations@cisa.dhs.gov

Risk Assessment Level: ● ○ ○

Cyber Threat Hunting

CISA provides cyber hunting services focused on specific threat actors and their associated tactics, techniques, and procedures.

Central@cisa.gov

Risk Assessment Level: ● ● ○

External Dependencies Management Assessment

An assessment for organizations to learn how to manage risks arising from external dependencies within the supply chain.

cyberadvisor@cisa.dhs.gov

Risk Assessment Level: ● ○ ○

Vulnerability Scanning

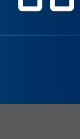
CISA offers organizations continual vulnerability scanning of internet-accessible systems.

vulnerability@cisa.dhs.gov

Many CISA services involve the close coordination and sharing of sensitive information between CISA and the organization receiving the service. To facilitate these partnerships, such organizations receive protections under the Protected Critical Infrastructure Information (PCII) Program. For more information on the PCII Program, visit <https://www.cisa.gov/pcii-program>.



SERVICES



INDUSTRY



Infrastructure

BROWSE BY TYPE



Capacity Building Services



Capacity Building Level: ● ○ ○

Active Shooter Preparedness Webinar

A webinar that provides information and resources to more effectively prepare for, mitigate the impacts of, and respond to an active shooter incident.

ASworkshop@hq.dhs.gov

Capacity Building Level: ● ○ ○

ChemLock Exercises

CISA's ChemLock exercises and drills can help a facility with dangerous chemicals that has a security plan in place identify best practices, lessons learned, and areas for improvement in plans and procedures.

ChemLock@cisa.dhs.gov

Capacity Building Level: ● ○ ○

ChemLock On-Site Assessments and Assistance

CISA's ChemLock on-site assessments and assistance can help facilities assess the risk of dangerous chemicals at the facility and then develop a security plan that addresses those risks.

ChemLock@cisa.dhs.gov

Capacity Building Level: ● ○ ○

ChemLock Training

CISA's ChemLock offers training to assist with understanding the risks that chemicals pose and what security measures can be put into place to reduce the risk of dangerous chemicals being weaponized.

ChemLock@cisa.dhs.gov

Capacity Building Level: ● ○ ○

CISA Tabletop Exercise Packages

CISA Tabletop Exercise Packages (CTEP) assist stakeholders in conducting their own tabletop exercises by providing exercise planners with tools, scenarios, question sets, and guidance to support the development of discussion-based exercises.

CISA.Exercises@cisa.dhs.gov

Capacity Building Level: ● ○ ○

Counter-Improvised Explosive Device and Risk Mitigation Training

Training courses to educate on strategies to prevent, protect against, respond to, and mitigate bombing incidents.

OBPTraining@cisa.dhs.gov

Capacity Building Level: ● ● ○

Cyber Storm

CISA-sponsored cybersecurity exercise that simulates a large-scale, coordinated cyber-attack impacting critical infrastructure.

cyberstorm@hq.dhs.gov

Capacity Building Level: ● ○ ○

Stakeholder Exercises

Planning with a range of stakeholders to develop and conduct preparedness exercises.

CISA.Exercises@cisa.dhs.gov



Incident Response Services



Incident Response Level: ● ○ ○

Active Shooter Preparedness Webinar

A webinar that provides information and resources to more effectively prepare for, mitigate the impacts of, and respond to an active shooter incident.

ASworkshop@hq.dhs.gov

Incident Response Level: ● ○ ○

Explosive Blast Modeling Assessment

A detailed technical assessment that provides stakeholders with a visual model of their facility's structural vulnerabilities and soft-targets against improvised explosive devices.

OBP@cisa.dhs.gov

Incident Response Level: ● ● ○

Special Event and Domestic Incident Tracker Tool

Special Event and Domestic Incident Tracker (SEDIT) Tool is a planning capability that integrates security and resilience data to create scenarios to make decisions regarding the impact, protection, mitigation, response, and recovery efforts.

CISA-GatewayHelpDesk@cisa.dhs.gov



Information Sharing Services



Information Sharing Level: ● ○ ○

CISA Gateway

The CISA Gateway provides various data collection, analysis, and response tools in one integrated system, streamlining access to CISA tools and datasets by leveraging a single user registration, management, and authentication process.

CISA-GatewayHelpDesk@cisa.dhs.gov

Information Sharing Level: ● ○ ○

Explosive Blast Modeling Assessment

A detailed technical assessment that provides stakeholders with a visual model of their facility's structural vulnerabilities and soft-targets against improvised explosive devices.

OBP@cisa.dhs.gov

Information Sharing Level: ● ○ ○

Homeland Security Information Network - Critical Infrastructure

The Homeland Security Information Network's Critical Infrastructure (HSIN-CI) network is the Department of Homeland Security's online platform for collaboration in protecting the nation's critical infrastructure.

HSINCI@hq.dhs.gov

Information Sharing Level: ● ○ ○

Technical Resource for Incident Prevention

A cross-sector, resource-sharing portal to increase awareness of evolving improvised explosive device tactics, techniques, and procedures.

TRIPwireHelp@cisa.dhs.gov

Risk Assessment Services

Risk Assessment Level: ● ○ ○

ChemLock On-Site Assessments and Assistance

CISA's ChemLock on-site assessments and assistance can help facilities assess the risk of dangerous chemicals at the facility and then develop security plans that address those risks.

ChemLock@cisa.dhs.gov

Risk Assessment Level: ● ○ ○

Explosive Blast Modeling Assessment

A detailed technical assessment that provides stakeholders with a visual model of their facility's structural vulnerabilities and soft-targets against improvised explosive devices.

OBP@cisa.dhs.gov

Risk Assessment Level: ● ● ○

Infrastructure Survey Tool

Voluntary assessment to identify and document the overall security and resilience of critical infrastructure facilities.

Central@cisa.dhs.gov

Risk Assessment Level: ● ● ○

Infrastructure Visualization Platform

Data collection and presentation tool that supports critical infrastructure security, special event planning, and responsive operations.

isdassessments@cisa.dhs.gov

Risk Assessment Level: ● ○ ○

Regional Resiliency Assessment Program

Provides voluntary collaborative assessments to improve the resilience of a region's critical infrastructure.

resilience@cisa.dhs.gov

Risk Assessment Level: ● ○ ○

Security Assessment at First Entry

Rapid voluntary physical security assessment designed to quickly identify vulnerabilities and evaluate options to mitigate them.

isdassessments@cisa.dhs.gov

Partnership Development Services

Partnership Development Level: ● ○ ○

Active Shooter Preparedness Webinar

A webinar that provides information and resources to more effectively prepare for, mitigate the impacts of, and respond to an active shooter incident.

ASworkshop@hq.dhs.gov

Partnership Development Level: ● ○ ○

Explosive Blast Modeling Assessment

A detailed technical assessment that provides stakeholders with a visual model of their facility's structural vulnerabilities and soft-targets against improvised explosive devices.

OBP@cisa.dhs.gov

Many CISA services involve the close coordination and sharing of sensitive information between CISA and the organization receiving the service. To facilitate these partnerships, such organizations receive protections under the Protected Critical Infrastructure Information (PCII) Program. For more information on the PCII Program, visit <https://www.cisa.gov/pcii-program>.



SERVICES



NON-PROFITS



Cybersecurity

BROWSE BY TYPE



Capacity Building Services



Capacity Building Level: ● ○ ○

CISA Tabletop Exercise Packages

CISA Tabletop Exercise Packages (CTEP) assist stakeholders in conducting their own tabletop exercises by providing exercise planners with tools, scenarios, question sets, and guidance to support the development of discussion-based exercises.

CISA.Exercises@cisa.dhs.gov

Capacity Building Level: ● ● ○

Cyber Storm

CISA-sponsored cybersecurity exercise that simulates a large-scale, coordinated cyber-attack impacting critical infrastructure.

cyberstorm@hq.dhs.gov

Capacity Building Level: ● ○ ○

Stakeholder Exercises

Planning with a range of stakeholders to develop and conduct preparedness exercises.

CISA.Exercises@cisa.dhs.gov



Risk Assessment Services



Risk Assessment Level: ● ○ ○

Vulnerability Scanning

CISA offers organizations continual vulnerability scanning of internet-accessible systems.

vulnerability@cisa.dhs.gov

Many CISA services involve the close coordination and sharing of sensitive information between CISA and the organization receiving the service. To facilitate these partnerships, such organizations receive protections under the Protected Critical Infrastructure Information (PCII) Program. For more information on the PCII Program, visit <https://www.cisa.gov/pcii-program>.



BROWSE BY TYPE



Capacity Building Services



Capacity Building Level: ● ○ ○

Active Shooter Preparedness Webinar

A webinar that provides information and resources to more effectively prepare for, mitigate the impacts of, and respond to an active shooter incident.

ASworkshop@hq.dhs.gov

Capacity Building Level: ● ○ ○

CISA Tabletop Exercise Packages

CISA Tabletop Exercise Packages (CTEP) assist stakeholders in conducting their own tabletop exercises by providing exercise planners with tools, scenarios, question sets, and guidance to support the development of discussion-based exercises.

CISA.Exercises@cisa.dhs.gov

Capacity Building Level: ● ● ○

Cyber Storm

CISA-sponsored cybersecurity exercise that simulates a large-scale, coordinated cyber-attack impacting critical infrastructure.

cyberstorm@hq.dhs.gov

Capacity Building Level: ● ○ ○

Stakeholder Exercises

Planning with a range of stakeholders to develop and conduct preparedness exercises.

CISA.Exercises@cisa.dhs.gov



Incident Response Services



Incident Response Level: ● ○ ○

Active Shooter Preparedness Webinar

A webinar that provides information and resources to more effectively prepare for, mitigate the impacts of, and respond to an active shooter incident.

ASworkshop@hq.dhs.gov

Incident Response Level: ● ○ ○

Explosive Blast Modeling Assessment

A detailed technical assessment that provides stakeholders with a visual model of their facility's structural vulnerabilities and soft-targets against improvised explosive devices.

OBP@cisa.dhs.gov

Incident Response Level: ● ● ○

Special Event and Domestic Incident Tracker Tool

Special Event and Domestic Incident Tracker (SEDIT) Tool is a planning capability that integrates security and resilience data to create scenarios to make decisions regarding the impact, protection, mitigation, response, and recovery efforts.

CISA-GatewayHelpDesk@cisa.dhs.gov



Information Sharing Services



Information Sharing Level: ● ○ ○

CISA Gateway

The CISA Gateway provides various data collection, analysis, and response tools in one integrated system, streamlining access to ISD's tools and datasets by leveraging a single user registration, management, and authentication process.

CISA-GatewayHelpDesk@cisa.dhs.gov

Incident Response Level: ● ○ ○

Explosive Blast Modeling Assessment

A detailed technical assessment that provides stakeholders with a visual model of their facility's structural vulnerabilities and soft-targets against improvised explosive devices.

OBP@cisa.dhs.gov

Information Sharing Level: ● ○ ○

Technical Resource for Incident Prevention

A cross-sector, resource-sharing portal to increase awareness of evolving IED tactics, techniques, and procedures.

TRIPwireHelp@cisa.dhs.gov



Risk Assessment Services



Incident Response Level: ● ○ ○

Explosive Blast Modeling Assessment

A detailed technical assessment that provides stakeholders with a visual model of their facility's structural vulnerabilities and soft-targets against improvised explosive devices.

OBP@cisa.dhs.gov

Risk Assessment Level: ● ● ○

Infrastructure Visualization Platform

Data collection and presentation tool that supports critical infrastructure security, special event planning, and responsive operations.

isdassessments@cisa.dhs.gov



Partnership Development Services



Partnership Development Level: ● ○ ○

Active Shooter Preparedness Webinar

A webinar that provides information and resources to more effectively prepare for, mitigate the impacts of, and respond to an active shooter incident.

ASworkshop@hq.dhs.gov

Incident Response Level: ● ○ ○

Explosive Blast Modeling Assessment

A detailed technical assessment that provides stakeholders with a visual model of their facility's structural vulnerabilities and soft-targets against improvised explosive devices.

OBP@cisa.dhs.gov

Many CISA services involve the close coordination and sharing of sensitive information between CISA and the organization receiving the service. To facilitate these partnerships, such organizations receive protections under the Protected Critical Infrastructure Information (PCII) Program. For more information on the PCII Program, visit <https://www.cisa.gov/pcii-program>.



BROWSE BY TYPE



Capacity Building Services



Capacity Building Level: ● ○ ○

.gov Top-Level Domain

It should be easy to identify governments on the internet. .gov is the top-level domain for U.S.-based government organizations.

Cameron.Dixon@cisa.dhs.gov

Capacity Building Level: ● ● ●

Assessment Evaluation and Standardization

The Assessment Evaluation and Standardization (AES) training is a free, in-person and virtual training program during which participants learn how to conduct CISA cyber assessments.

CSD_VM_Methodology@cisa.dhs.gov

Capacity Building Level: ● ○ ○

Cyber Storm

CISA-sponsored cybersecurity exercise that simulates a large-scale, coordinated cyber-attack impacting critical infrastructure.

cyberstorm@hq.dhs.gov

Capacity Building Level: ● ○ ○

Cybersecurity Fundamentals Workshops

Fundamentals Workshop for local officials to learn about common cybersecurity threats as well as basic security practices.

cyberadvisor@cisa.dhs.gov

Capacity Building Level: ● ● ○

Enhanced Cybersecurity Services

Partnership between CISA and commercial service providers to detect and block malicious traffic entering or exiting customer networks (Note: Cost may apply).

ECS_Program@hq.dhs.gov

Capacity Building Level: ● ○ ○

Federal Virtual Training Environment

The Federal Virtual Training Environment (FedVTE) offers free online, on-demand cybersecurity training system that contains more than 800 hours of training for state, local, tribal, and territorial government personnel and veterans.

education@cisa.dhs.gov

Capacity Building Level: ● ○ ○

Multi-State Information Sharing and Analysis Center

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a membership-based collaborative that serves as the central cybersecurity resource for the nation's state, local, tribal, and territorial governments.

info@msisac.org

Capacity Building Level: ● ○ ○

Stakeholder Exercises

Planning with a range of stakeholders to develop and conduct preparedness exercises.

CISA.Exercises@cisa.dhs.gov



Incident Response Services



Incident Response Level: ● ○ ○

Cyber Incident Response

For cybersecurity incidents that have a national security interest and align with national priorities, CISA provides incident response augmentation, artifact analysis, and coordination assistance.

<https://us-cert.cisa.gov/forms/report>

Incident Response Level: ● ○ ○

Malware Analysis

CISA's Malware Analysis service provides stakeholders a dynamic analysis of malicious code, including recommendations for malware removal and recovery activities.

<https://www.malware.us-cert.gov/>

Capacity Building Level: ● ○ ○

Multi-State Information Sharing and Analysis Center

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a membership-based collaborative that serves as the central cybersecurity resource for the nation's state, local, tribal, and territorial governments.

info@msisac.org



Information Sharing Services



Information Sharing Level: ● ● ○

Automated Indicator Sharing

Enables the exchange of cyber threat indicators with SLTT governments and the private sector at machine speed.

cyberservices@hq.dhs.gov

Information Sharing Level: ● ○ ○

Homeland Security Information Network: CISA Cyber Portal

Department of Homeland Security's official system for sharing sensitive but unclassified information.

HSIN.Helpdesk@hq.dhs.gov

Capacity Building Level: ● ○ ○

Multi-State Information Sharing and Analysis Center

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a membership-based collaborative that serves as the central cybersecurity resource for the nation's state, local, tribal, and territorial governments.

info@msisac.org

Information Sharing Level: ● ○ ○

National Cyber Awareness System

Situational awareness tool for technical and non-technical audiences that provides timely information about cybersecurity threats and issues.

<https://us-cert.cisa.gov/mailing-lists-and-feeds>

Information Sharing Level: ● ○ ○

Shared Cybersecurity Services

Commercial cyber threat feed subscriptions for Federal Civilian Agencies, State Fusion Centers, MS-ISAC, and EI-ISAC.

CISA.CTIS.SCS_Info@cisa.dhs.gov



Risk Assessment Services



Risk Assessment Level: ● ○ ○

Cyber Infrastructure Survey

An assessment that evaluates the effectiveness of organizational security controls, cybersecurity preparedness, and overall resilience.

iodregionaloperations@cisa.dhs.gov

Risk Assessment Level: ● ● ●

Cyber Resilience Review

An assessment that evaluates an organization's operational resilience and cybersecurity practices.

iodregionaloperations@cisa.dhs.gov

Risk Assessment Level: ● ○ ○

Cyber Threat Hunting

CISA provides cyber hunting services focused on specific threat actors and their associated tactics, techniques, and procedures.

Central@cisa.gov

Risk Assessment Level: ● ● ●

External Dependencies Management Assessment

An assessment for organizations to learn how to manage risks arising from external dependencies within the supply chain.

cyberadvisor@cisa.dhs.gov

Capacity Building Level: ● ○ ○

Multi-State Information Sharing and Analysis Center

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a membership-based collaborative that serves as the central cybersecurity resource for the nation's state, local, tribal, and territorial governments.

info@msisac.org

Risk Assessment Level: ● ○ ○

Vulnerability Scanning

CISA offers organizations continual vulnerability scanning of internet-accessible systems.

vulnerability@cisa.dhs.gov



Partnership Development Services



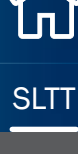
Capacity Building Level: ● ○ ○

Multi-State Information Sharing and Analysis Center

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a membership-based collaborative that serves as the central cybersecurity resource for the nation's state, local, tribal, and territorial governments.

info@msisac.org

Many CISA services involve the close coordination and sharing of sensitive information between CISA and the organization receiving the service. To facilitate these partnerships, such organizations receive protections under the Protected Critical Infrastructure Information (PCII) Program. For more information on the PCII Program, visit <https://www.cisa.gov/pcii-program>.



BROWSE BY TYPE



Capacity Building Services



Capacity Building Level: ● ○ ○

Active Shooter Preparedness Webinar

A webinar that provides information and resources to more effectively prepare for, mitigate the impacts of, and respond to an active shooter incident.

ASworkshop@hq.dhs.gov

Capacity Building Level: ● ○ ○

CISA Tabletop Exercise Packages

CISA Tabletop Exercise Packages (CTEP) assist stakeholders in conducting their own tabletop exercises by providing exercise planners with tools, scenarios, question sets, and guidance to support the development of discussion-based exercises.

CISA.Exercises@cisa.dhs.gov

Capacity Building Level: ● ● ○

Counter-Improvised Explosive Device and Risk Mitigation Training

Training courses to educate on strategies to prevent, protect against, respond to, and mitigate bombing incidents.

OBPTraining@cisa.dhs.gov

Capacity Building Level: ● ● ○

Interagency Security Committee Risk Management Process Training

This half-day, instructor-led course is a prerequisite for Facility Security Committee membership and covers the Risk Management Process.

rmp_fsctrng@cisa.dhs.gov

Capacity Building Level: ● ● ○

Multi-Jurisdiction Improvised Explosive Device Security Planning

A series of tabletop exercises that assists participants in identifying roles and capabilities gaps within a multi-jurisdictional planning area for countering improvised explosive devices.

MJIEDSP@cisa.dhs.gov

Capacity Building Level: ● ○ ○

Stakeholder Exercises

Planning with a range of stakeholders to develop and conduct preparedness exercises.

CISA.Exercises@cisa.dhs.gov



Incident Response Services



Incident Response Level: ● ○ ○

Active Shooter Preparedness Webinar

A webinar that provides information and resources to more effectively prepare for, mitigate the impacts of, and respond to an active shooter incident.

ASworkshop@hq.dhs.gov

Incident Response Level: ● ○ ○

Explosive Blast Modeling Assessment

A detailed technical assessment that provides stakeholders with a visual model of their facility's structural vulnerabilities and soft-targets against improvised explosive devices.

OBP@cisa.dhs.gov

Incident Response Level: ● ● ○

Special Event and Domestic Incident Tracker Tool

Special Event and Domestic Incident Tracker (SEDIT) Tool is a planning capability that integrates security and resilience data to create scenarios to make decisions regarding the impact, protection, mitigation, response, and recovery efforts.

CISA-GatewayHelpDesk@cisa.dhs.gov



Information Sharing Services



Information Sharing Level: ● ○ ○

CISA Gateway

The CISA Gateway provides various data collection, analysis, and response tools in one integrated system, streamlining access to CISA tools and datasets by leveraging a single user registration, management, and authentication process.

CISA-GatewayHelpDesk@cisa.dhs.gov

Incident Response Level: ● ○ ○

Explosive Blast Modeling Assessment

A detailed technical assessment that provides stakeholders with a visual model of their facility's structural vulnerabilities and soft-targets against improvised explosive devices.

OBP@cisa.dhs.gov

Information Sharing Level: ● ○ ○

Homeland Security Information Network - Critical Infrastructure

The Homeland Security Information Network's Critical Infrastructure (HSIN-CI) network is the Department of Homeland Security's online platform for collaboration in protecting the nation's critical infrastructure.

HSINCI@hq.dhs.gov

Information Sharing Level: ● ○ ○

Technical Resource for Incident Prevention

A cross-sector, resource-sharing portal to increase awareness of evolving improvised explosive device tactics, techniques, and procedures.

TRIPwireHelp@cisa.dhs.gov



Risk Assessment Services



Incident Response Level: ● ○ ○

Explosive Blast Modeling Assessment

A detailed technical assessment that provides stakeholders with a visual model of their facility's structural vulnerabilities and soft-targets against improvised explosive devices.

OBP@cisa.dhs.gov

Risk Assessment Level: ● ● ○

Infrastructure Visualization Platform

Data collection and presentation tool that supports critical infrastructure security, special event planning, and responsive operations.

isdassessments@cisa.dhs.gov

Risk Assessment Level: ● ● ○

National Counter-Improvised Explosive Device Capabilities Analysis Database

An assessment program that analyzes the capabilities of bomb squads; explosives detection canine teams; dive teams; and special weapons and tactics teams.

NCCAD@cisa.dhs.gov

Risk Assessment Level: ● ○ ○

Rapid Survey

Rapid voluntary security and resilience assessment available for use by state and local partners.

Central@cisa.gov

Risk Assessment Level: ● ○ ○

Regional Resiliency Assessment Program

Provides voluntary collaborative assessments to improve the resilience of a region's critical infrastructure.

resilience@hq.dhs.gov

Partnership Development Services

Partnership Development Level: ● ○ ○

Active Shooter Preparedness Webinar

A webinar that provides information and resources to more effectively prepare for, mitigate the impacts of, and respond to an active shooter incident.

ASworkshop@hq.dhs.gov

Incident Response Level: ● ○ ○

Explosive Blast Modeling Assessment

A detailed technical assessment that provides stakeholders with a visual model of their facility's structural vulnerabilities and soft-targets against improvised explosive devices.

OBP@cisa.dhs.gov



SERVICES



SLTT



Communications

BROWSE BY TYPE



Capacity Building Services



Capacity Building Level: ● ○ ○

Interoperable Communications Technical Assistance Program

A portfolio of technical assistance available to all 56 states and territories and federally recognized tribes to help solve communications interoperability issues.

ECD@cisa.dhs.gov



Incident Response Services



Incident Response Level: ● ○ ○

Government Emergency Telecommunications Service

Provides national security and emergency preparedness personnel with end-to-end priority on landline networks.

ECD@cisa.dhs.gov

Incident Response Level: ● ○ ○

Telecommunications Service Priority Program

Provides national security and emergency preparedness organizations with priority repair and installation of vital voice and data circuits.

ECD@cisa.dhs.gov

Incident Response Level: ● ○ ○

Wireless Priority Service

Provides national security and emergency preparedness personnel with priority access and processing on cellular networks.

ECD@cisa.dhs.gov

Many CISA services involve the close coordination and sharing of sensitive information between CISA and the organization receiving the service. To facilitate these partnerships, such organizations receive protections under the Protected Critical Infrastructure Information (PCII) Program. For more information on the PCII Program, visit <https://www.cisa.gov/pcii-program>.