CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE MONTH TOOLKIT

CONTENTS

WELCOME TO CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE MONTH 2023

Each November we celebrate Critical Infrastructure Security and Resilience Month. This year, the Cybersecurity and Infrastructure Security Agency (CISA) is calling on all Americans to ***Resolve to be Resilient***. Critical infrastructure is a shared resource as well as a shared responsibility - we all play a role in keeping it secure, and resilient.

Critical Infrastructure Security and Resilience Month is CISA's annual effort focused on educating and engaging all levels of government, infrastructure owners and operators, and the American public about the vital role critical infrastructure plays in the nation's wellbeing and why it is important to strengthen critical infrastructure security and resilience.

This month CISA is focusing on building resilience. Resilience means doing the work up front to prepare for a disruption, anticipating that it will in fact happen, and exercising not just for response but with a deliberate focus on continuity and recovery, improving the ability to operate in a degraded state, and significantly reducing downtime when an incident occurs.

CISA partners with critical infrastructure owners and operators nationwide to help them reduce risk and build their security capacity to withstand new threats and disruptions, whether from natural hazards or other physical and cyber threats. In the following pages we offer a number of resources to help you and your organization get involved in Critical Infrastructure Security and Resilience Month. Be sure to follow us on social media and take part in the hashtag #BeResilient conversation!

THIS NOVEMBER, TAKE ACTION ON INFRASTRUCTURE SECURITY

Start by visiting cisa.gov/CISR to learn more about critical infrastructure and available resources, training and tips.

RESOLVE TO BE RESILIENT

Resolve to be Resilient, so that, as a nation, we can recover quickly in the event of an incident tomorrow. Everyone plays a role in the nation's security and resilience, and we must understand and accept our mutual responsibilities in managing our shared risks.

THE CURRENT THREAT ENVIRONMENT

Critical infrastructure faces a wide range of threats and risks, from naturally occurring events, to human-induced disruptions of both accidental and malicious origins. Catastrophic natural hazards and climate change has increased the frequency and intensity of natural disasters, which have adverse effects on physical critical infrastructure such as transportation networks, telecommunications systems and energy infrastructure. The threat of terrorism and targeted violence unfortunately remains elevated and is increasingly local and often aimed at public gatherings, like houses of worship. The diversity, complexity, and sheer expanse of our nation's physical infrastructure poses its own unique challenges.

Additionally, critical infrastructure assets and systems have become highly interconnected and interdependent, both domestically and internationally, increasing the likelihood of cascading failures across multiple sectors. Increased digitization of the systems and processes that underpin the functioning of critical infrastructure amplify the risk for assets and systems' exposure to heighten physical and cyber threats from state-sponsored and non-state actors, as well as cybercriminals. The impact of cyberattacks are costly in nature, as governments and owners and operators of critical infrastructure spend millions of dollars rectifying the damage caused to their assets, systems and reputation.

A shifting geopolitical landscape has intensified national security concerns and has shown how targeting critical infrastructure can be a primary attack vector for weakening a country's ability to protect itself, and its citizens. This can occur both in a conflict setting, as well as through indirect, long-term foreign interference campaigns. These concerns have highlighted that domestic investment in infrastructure security and resilience can both strengthen national security and serve as a strategic deterrent. All of these factors demand a greater focus on resilience.

WHAT YOU CAN DO

No matter what line of work we are engaged in or where we live, nearly everything we do relies on critical infrastructure. Fortunately, there are steps we can take to help keep these systems running smoothly. We invite you to join this effort in whatever capacity is right for your role or organization. Below are some quick actions different stakeholders can take to help make critical infrastructure more resilient. Visit CISA.gov to learn more.

Recommended Actions for the Private Sector

- ✓ Improve security through a series of steps, including:
  - *Assess Your Risk.* Organizations must identify your most critical functions and assets, define dependencies that enable the continuity of these functions, and consider the full range of threats that could undermine functional continuity.
  - *Make a Plan and Exercise It.* Organizations should perform dedicated resilience planning, determine the maximum downtime acceptable for customers, develop recovery plans to regain functional capabilities within the maximum downtime, and test those plans under real-life conditions.
  - *Continuously Improve and Adapt.* Organizations must be prepared to regularly adapt to changing conditions and threats. This starts with fostering a culture of continuous improvement, based on lessons learned from exercises and real-world incidents and evolving cross-sector risks.
- ✓ Add your voice to social media conversations by using the hashtag #BeResilient to critical infrastructure issues and how they relate to your mission and to the security environment of your office.
- ✓ Encourage clients, stakeholders, and state, local, tribal, and territorial government counterparts to learn about critical infrastructure, dependencies, and the importance of a whole-of-community effort throughout the month by visiting cisa.gov/CISR.
- ✓ Integrate cybersecurity into facility and operational protective measures.
- ✓ Build resilience into facility design and operations.

Recommended Actions for Sector Risk Management Agencies

- ✓ Educate members of your sector about critical infrastructure issues and how they relate to the sector's security environment and business operations during this time of transition.
- ✓ Discuss the evolution of focus on critical infrastructure—from protection to security and resilience—and dependencies requiring innovation and investment of infrastructure in newsletters, mailings and websites.
- ✓ Highlight your partnership with CISA, other federal agencies and the national critical infrastructure community to make these vital assets and systems secure and resilient.
- ✓ Host a virtual town hall to discuss local critical infrastructure issues.
- ✓ Promote training and exercise opportunities to owners, operators and internal staff.

Recommended Actions for State, Local, Tribal, and Territorial Government Officials

- ✓ Conduct or participate in a training or exercise to improve security and resilience.
- ✓ Election officials can go to Election Security | Cybersecurity and Infrastructure Security Agency CISA for election security and disinformation/misinformation resources.
- ✓ Access the multitude of resources available through the Interagency Security Committee to enhance the security of federal government facilities: Interagency Security Committee | CISA.
- ✓ See if you qualify for the FY23 State and Local Cybersecurity Grant Program: State and Local Cybersecurity Grant Program | CISA.

- ✓ Connect public safety officials with private sector businesses.
- ✓ Meet with local business owners to discuss dependencies on critical infrastructure and distribute relevant materials.
- ✓ Include a message about the importance of infrastructure security and resilience in newsletters, mailings and websites.
- ✓ Meet with CISA representatives in your state or district to better understand your local infrastructure and the risks it faces.
- ✓ Host a town hall meeting to discuss local critical infrastructure issues.
- ✓ Write an opinion editorial in the local paper about the importance of critical infrastructure security and resilience.

Recommended Actions for Members of Congress

- ✓ Meet with CISA representatives in your state or district to better understand your local infrastructure and the risks it faces.
- ✓ Promote training and exercise opportunities to owners and operators.
- ✓ Engage state and local officials on current initiatives to improve security and resilience.
- ✓ Meet with local business owners to discuss dependencies and interdependencies of critical infrastructure.
- ✓ Include a message about the importance of infrastructure security and resilience in newsletters, mailings and websites.
- ✓ Write an opinion editorial in your local paper about the importance of critical infrastructure.

Communication Tips

In addition, partners can reference the tips below for engaging with various audiences:

- ✓ *Understand Your Audience*—Know what groups of people you are trying to reach. Knowing who is receiving your message is important to what you say and do.
- ✓ *Know the Specific Risks in Your Area*—By tailoring messages to the specific risks in your area, you can make your outreach more effective and help your community prepare for the most likely events.
- ✓ *Make It Meaningful*—Tailor your message to each audience, whether this is owners or operators, individuals or families, employees, professionals in specific fields (such as education or medicine), young people, or those with special access and functional needs.
- ✓ *Make It Accessible*—Create messages and tools that are accessible to all audiences. Visit Digital.gov — Guidance on building better digital services in government for more information on accessibility.
- ✓ *Engage Your Audience*—Create activities that engage your community and promote interaction.

RESOURCES

CISA provides several resources that support security capacity building efforts, including those focused on active shooter preparedness, vehicle ramming mitigations, unmanned aircraft systems, school safety, chemical security, and bombing prevention. CISA also conducts exercises to help stakeholders assess their plans and can provide free site visits to assess current security posture and identify any vulnerabilities and areas for improvement. Below are CISA's resources across different infrastructure security topics.

Active Shooter Preparedness

- CISA provides active shooter resources focused on behavioral indicators denoting a potential attack, emergency action plan creation, actions that may be taken during an incident to reduce consequences, and how to quickly recover from an incident. Resources are available in multiple languages for first responders, human resources, security professionals, and private citizens: Active Shooter Preparedness | CISA.
- CISA provides an Emergency Action Plan template, guide, and video on considerations for the plan from survivors of active shooter incidents at *Active Shooter Emergency Action Plan*.
    - CISA also conducts Active Shooter Preparedness webinars to directly support organizations in developing emergency action plans through live instructor-based training.

Bombing Prevention and Countering Improvised Explosive Devices

- CISA's Office for Bombing Prevention (OBP) develops and delivers a diverse curriculum of training and awareness products to help build nationwide counter-improvised explosive device (IED) core capabilities and enhance awareness of terrorist threats. Download and use the *Security and Resiliency Guide: Counter-Improvised Explosive Device Concepts, Common Goals, and Available Assistance*.
- Download and use the *Public Venue Security Screening Guide* to protect venues from bombings and the *Security and Resiliency Guide for Public Assembly*.
- Learn from others different techniques and tactics on how to counter and prevent IED incidents. Register at the Technical Resource for Incident Prevention (TRIPwire) Portal | CISA - a free, 24/7, online, collaborative information-sharing resource hub that provides information on evolving IED tactics, techniques, incident lessons learned, and counter-IED preparedness.
- CISA also offers many valuable resources to identify and report suspicious activity related to bomb threats, including:
    - CISA's Bomb-Making Materials Awareness Program (BMAP) | CISA which offers tools to help companies and their employees serve as the nation's first line of defense to identify and report suspicious purchasing behavior for products used to make bombs.
    - CISA's "HOT RAIN" card provide people with easy-to-remember tips on how to recognize suspicious or unattended items.
    - CISA's *Be Vigilant video series* highlights how bombs can be made from everyday items and enables the public to recognize and report suspicious activity.

Chemical Security

- Request a ChemLock On-Site Assessment and Assistance so CISA chemical security experts can identify specific security risks that your on-site chemicals present and offer scalable, tailored suggestions for security measures that will best enhance your organization's security posture based on your unique circumstances and business model.
- If you have dangerous chemicals at your facility, conduct an inventory to ensure that you are aware of all the chemicals that you have on-site. Use ChemLock Resources | CISA to enhance the security of those dangerous chemicals to ensure that they are not weaponized.
- CISA offers live, on-demand training to assist owners, operators, facility personnel, and retailers with understanding the threats that chemicals pose and what security measures can be put into place to

reduce the risk of dangerous chemicals being weaponized. Learn more about CISA's ChemLock | CISA.

Insider Threat

- CISA provides Insider Threat Mitigation workshops at the request of stakeholders to their Protective Security Advisors that define an insider and insider threat, how to build an Insider Threat Mitigation Team, and how to mitigate and recover from insider threat incidents.
    - Visit Insider Threat Mitigation Resources and Tools | CISA for more materials to help you recognize, prepare for, and recover from insider threat incidents.
- Public reports of suspicious activities to the authorities have helped prevent attacks. Know how to report suspicious behavior locally.
- Non-security professionals at any organization can also augment security through non-confrontational techniques that can thwart a potential attack or escalating situation.
- The Employee Vigilance Through the Power of Hello slick-sheet and placemat provide information to assist in identifying and effectively responding to suspicious behavior. Additionally, these resources have been translated into 17 languages including Dari and Pashto and can be found here: *Power of Hello Translations*.
- Learn how to identify potential signs that someone is on a *pathway to violence*.
- Be prepared on what to say and do when faced with behaviors that raise concern or an incident that is escalating with CISA's four-product De-escalation Series.
    - These products help stakeholders assess if the situation or person of concern is escalating; de-escalate the situation currently taking place through purposeful actions; and report the situation through organizational reporting to enable assessment and management of an evolving threat and 9-1-1 for immediate threats.
- Facilities with dangerous chemicals can ensure their personnel are aware of how and when to report suspicious activity by downloading and using the *ChemLock: Reporting Suspicious Activities and Significant Activities fact sheet*.

School Safety

- CISA develops and deploys capacity building products and tools to support and enhance school safety and security. Resources include CISA's K-12 School Security Guide Suite, which provides K-12 districts and campuses with information, tools, and strategies to assess vulnerabilities, improve physical security, and better protect school communities.
- CISA and the U.S. Secret Service National Threat Assessment Center partnered to develop the K-12 Bystander Reporting Toolkit | CISA which offers simple strategies and guidance K-12 schools and school districts can use to implement and enhance safety reporting programs and encourage bystander reporting among students and other members of the school community.
- CISA developed *Protecting Our Future: Partnering to Safeguard K–12 Organizations from Cybersecurity Threats* which provides recommendations and resources to help K-12 schools and school districts address systemic cybersecurity risk. It also provides insight into the current threat landscape specific to the K-12 community and offers actionable steps school leaders can take to strengthen their cyber posture.
    - Visit CISA'S K-12 page: Cybersecurity for K-12 Education | CISA for more cybersecurity resources for the K-12 education community.
- School administrators, security personnel, parents, and educators can visit SchoolSafety.gov which houses a comprehensive repository of federal and state resources, programs, tools, and evidence-based practices on a range of school safety topics, including physical security, cybersecurity, and targeted violence.
- Visit CISA's School Safety page: School Safety | CISA for more school safety and security resources for the K-12 community.

Resilience Planning and Supply Chain Security

- The Security Assessment at First Entry | CISA tool is a high-level resource for facilities that have

limited or no security measures or planning in place. It is designed to assess current security posture and produce a report in under two hours.

- State and local governments as well as critical infrastructure operators can use CISA's *Infrastructure Resilience Planning Framework (IRPF)* to better identify critical infrastructure, assess related risks, and develop and implement resilience solutions.
- Using the Mitigating ICT Supply Chain Risks with Qualified Bidder and Manufacturer Lists and Vendor Supply Chain Risk Management (SCRM) Template can help ensure the Internet Communication Technology (ICT) products you buy from vendors meet industry standards. Both tools are great resources for IT or cyber security personnel, acquisitions and procurement professionals, those who manage vendor and supplier lists, among others.
- The Regional Resiliency Assessment Program | CISA is a voluntary, cooperative assessment of specific critical infrastructure that identifies a range of security and resilience issues that could have regionally or nationally significant consequences. The goal of the program is to generate greater understanding and action among public and private sector partners to improve the resilience of a region's critical infrastructure.

Securing Public Gatherings and Other Physical Security Resources

- Learn about the multitude of resources available to augment security of public gathering locations in a manner that does not impede daily operations Securing Public Gatherings | Cybersecurity and Infrastructure Security Agency CISA.
- CISA provides security resources specific to Faith Based Organizations that assist houses of worship in securing physical and cyber infrastructure.
- Learn about the actions that may be taken within legal parameters to mitigate implications of unauthorized overflights of unmanned aircraft systems. Visit Unmanned Aircraft Systems Resources | CISA.
- Visit Physical Security | CISA for free tools and resources for small- and medium-sized businesses related to security and resilience.

Self-Assessment and Exercises

- Participate in, or conduct, a training or exercise to improve security and resilience. (CISA offers a whole suite of tabletop exercise scenarios that organizations can use to run their own exercise.)
- Review and revise business continuity and emergency plans and processes to address the evolving threat we face today and to align with updated sector-specific plans.
- CISA provides ready-to-use *exercise packages* for our security partners working with public gatherings and crowded places to use in initiating training within their organizations. Each package can be customized and includes templates with exercise objectives, scenarios, and discussion questions.
- Learn about CISA's vehicle ramming mitigation solutions, including a *self-assessment tool* that contains a series of questions allowing users to evaluate potential facility vulnerabilities to an attack. Based on responses, the tool recommends protective measures/actions and provides users with information on related available resources to inform decision-making.
- Use CISA's *Insider Risk Mitigation Self-Assessment Tool* to assess your organization's vulnerability to an insider threat.
- Learn about resources available for vulnerability assessments and continuity plans, including Critical Infrastructure Assessments | CISA.

Resources for All

- Report suspicious activity to local law enforcement to public safety officials to discuss security and resilience enhancements.
- Within each CISA region are local and regional Protective Security Advisors (PSAs), Cyber Security Advisors (CSAs), Emergency Communications Coordinators (ECCs), and Chemical Security Inspectors (CSIs). Contact your regional representative today for a complimentary assessment:

Security Advisors | CISA.

- The Cross-Sector Cybersecurity Performance Goals | CISA were developed in close partnership with organizations across government and the private sector. They provide voluntary guidance to critical infrastructure and other organizations to help them prioritize security investments toward areas that will have the greatest impact on their cybersecurity.
- CISA offers three priority telecommunications services that enable essential personnel to communicate when networks are degraded or congested. Enroll in all three services here: Priority Telecommunications Services | CISA.
- Visit Telework Guidance and Resources | CISA for guidance on teleworking securely.
- Learn about the legal protections for information shared with CISA under the Protected Critical Infrastructure Information (PCII) Program at Protected Critical Infrastructure Information (PCII) Program | CISA.

TEMPLATES

Press Release Template

If you choose to use this template, you must include the following language attributing the authorship to CISA: "The message contained in this newsletter/blog was authored by CISA."

(Month, Day)
(Contact Name)
(Phone/Email)

CITY, STATE - (ORGANIZATION) Joins National Effort to Promote Infrastructure Security and Resilience November is Critical Infrastructure Security and Resilience Month.

(ORGANIZATION) has committed to participate in Critical Infrastructure Security and Resilience Month to focus on the importance of our nation's critical infrastructure. We all share the responsibility to keep our critical infrastructure and our communities secure and resilient. Public-private partnerships leverage our shared commitment by identifying vulnerabilities and mitigating risks through protective programs and training.

(INSERT QUOTE FROM YOUR ORGANIZATION SPOKESPERSON HERE)

This year's theme is Resolve to be Resilient. Weather is becoming more extreme, physical and cyberattacks are a persistent threat, and technology is advancing in ways that will change our future very quickly. We must prepare by accepting that it's our responsibility to strengthen critical infrastructure and protect the vital services it provides. We can do this by embracing resiliency and building it into our preparedness planning—and then exercising those plans. The safety and security of the nation depends on the ability of critical infrastructure to be able to prepare for and adapt to changing conditions and to withstand and recover rapidly from disruptions. This starts with building resilience into infrastructure investment.

America's national security and economic prosperity are increasingly dependent upon critical infrastructure that is at risk from a variety of hazards, including both physical and cyber. Critical infrastructure security and resilience require a clear understanding of the risks we face and a whole-of-community effort that involves partnership between public, private, and non-profit sectors.

Just as we all rely on critical infrastructure, we all play a role in keeping it strong, secure, and resilient.

(ORGANIZATION) is (INSERT EVENT AND MORE DETAILS HERE AS TO HOW YOUR ORGANIZATION IS PARTICIPATING OR HOW YOUR ORGANIZATION IS WORKING TO PROTECT AND SECURE INFRASTRUCTURE AND MAKE IT MORE RESILIENT).

For more information about Infrastructure Security Month, visit [INSERT ORGANIZATION WEBPAGE IF APPLICABLE] or cisa.gov/CISR.

(ORGANIZATION NAME)
(ORGANIZATION BOILERPLATE/DESCRIPTION OF ORGANIZATION)

Newsletter/Blog Post Template

If you choose to use this template, you must include the following language attributing the authorship to CISA: "The message contained in this newsletter/blog was authored by CISA."

Please consider highlighting Critical Infrastructure Security and Resilience Month in your organization by

including a brief article in your newsletter or a post on your blog, if you have one. To help get you started, here is an example of what you might want to include.

Resolve to be Resilient

November is Critical Infrastructure Security and Resilience month a nationwide effort to raise awareness and reaffirm the commitment to keep our nation's critical infrastructure secure and resilient. (ORGANIZATION) has committed to building awareness of the importance of critical infrastructure.

[INSERT QUOTE FROM ORGANIZATION LEADERSHIP ON THE ROLE THEY PLAY IN SECURING CRITICAL INFRASTRUCTURE AND THE MESSAGE THEY WANT TO CONVEY TO THEIR PARTNERS/CUSTOMERS/CONSTITUTENTS.]

This year's theme is ***Resolve to be Resilient***. Weather is becoming more extreme, physical and cyberattacks are a persistent threat, and technology is advancing in ways that will change our future very quickly. We must prepare by accepting that it's our responsibility to strengthen critical infrastructure and protect the vital services it provides. We can do this by embracing resiliency and building it into our preparedness planning—and then exercising those plans. The safety and security of the nation depends on the ability of critical infrastructure to be able to prepare for and adapt to changing conditions and to withstand and recover rapidly from disruptions. This starts with building resilience into infrastructure investment.

The safety and security of the nation depends on the ability of critical infrastructure to be able to prepare for and adapt to changing conditions and to withstand and recover rapidly from disruptions. Attacks cannot be completely prevented from happening, but we can minimize their impact by building resilience into our infrastructure and into our society.

For more information, visit CISA's Critical Infrastructure Security and Resilience Month web page for more information and resources: cisa.gov/CISR.

The message contained in this press release was authored by the Cybersecurity and Infrastructure Security Agency (CISA).

SLTT Proclamation Template

If you choose to use this template, you much include the following language attributing the authorship to CISA: "This Message contained in this newsletter/blog was authored by CISA."

PROCLAMATION

Critical Infrastructure Security and Resilience Month November 2023

WHEREAS, "Critical Infrastructure Security and Resilience Month" creates an important opportunity for every resident of [REGION, TOWN, or STATE] to recognize that infrastructure provides essential goods and services and that of protecting our nation's infrastructure resources and enhancing our national security and resilience is a national imperative; and

WHEREAS, the nation's critical infrastructure spurs our economy and supports our wellbeing, keeping infrastructure secure, functioning, and resilient requires a unified whole-of-nation, whole-of-community effort; and

WHEREAS, managing and mitigating risks to infrastructure from physical threats and cyber vulnerabilities requires shared responsibility and coordinated commitment; and

WHEREAS, partnerships between state, local, tribal and territorial governments, federal agencies, and the private sector makes good business sense; and

WHEREAS, making critical infrastructure secure and resilient is a shared national responsibility that all citizens of [REGION, TOWN or STATE] can get involved in and do their part, along with the many businesses and industries that make up the critical infrastructure community, and in their local communities by learning about risks to the critical infrastructure in their areas and taking steps to build resilience. THEREFORE, BE IT RESOLVED that the [GOVERNING BODY] hereby proclaims November 2023 as Critical Infrastructure Security and Resilience Month and encourages communities to support the national effort to strengthen critical infrastructure security by engaging in partnerships together toward creating a more resilient society.

DATED this _____ Day of _____ 2023 by the [GOVERNING BODY]

_____

NAME, TITLE

The message contained in this press release was authored by CISA.

SOCIAL MEDIA AND ONLINE RESOURCES

Social Media

CISA will use social media to share news and updates about Infrastructure Security Month. *Visit CISA.gov for more information and follow us on Twitter, Facebook, LinkedIn, Instagram* and use the hashtag #BeResilient to join the conversation. Also, be sure to check our page for updates at cisa.gov/CISR.

Useful Videos

Critical infrastructure-related videos are available through the DHS YouTube page. These links can be used in messaging materials or through Twitter and Facebook postings.

- ✓ "Options for Consideration Active Shooter Training Video" series demonstrates possible actions to take if confronted with an active shooter scenario: Options for Consideration Active Shooter Training Video Series - YouTube.
- ✓ PCII Program Introduction Video (4:13 duration): PCII Program Introduction Video - YouTube
- ✓ "What to Do" videos provide guidance to security officials, the general public and many other stakeholders about the steps they should take to protect themselves and others from bomb incidents: What to Do: Bomb Threats - YouTube.
- ✓ "Vehicle Ramming Attack Mitigation" provides insightful analysis and recommendations aimed at protecting organizations and individuals against a potential vehicle ramming incident (12:52 duration): Vehicle Ramming Attack Mitigation - YouTube.
- ✓ "Pathway to Violence" discusses behavioral indicators that assailants often demonstrate before a violent act (11:23 duration): Pathway to Violence - YouTube.
- ✓ Cybersecurity Performance Goals (2:15 duration): Intro to CISA Cybersecurity Performance Goals - YouTube.

Downloadable Graphics

These graphics can be used messaging materials or through social media (LinkedIn, Twitter, and Facebook: 1200x627 and Instagram: 1080x1080 and 1920x1080) postings. We have also included a signature block graphic. Click here to download: cisa.gov/cisr.

FREQUENTLY ASKED QUESTIONS (FAQS)

What is critical infrastructure?

The nation's critical infrastructure provides the essential services that underpin American society. Ensuring delivery of essential services and functions is important to sustaining the American way of life.

There are 16 critical infrastructure sectors whose assets, systems and networks—both physical and virtual—are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or a combination of any of these. They include the chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities, which includes the election infrastructure subsector; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems sectors.

America's national security and economic prosperity increasingly depend on critical infrastructure that is at risk from a variety of hazards and threats. Threats including aging or failing infrastructure, extreme weather, cyberattacks, or evolving terrorism threats, can profoundly impact our economy and communities. Critical infrastructure security and resilience require a clear understanding of the risks we face and a whole-of-community effort that involves partnership between public, private and nonprofit sectors. Learn more at Critical Infrastructure Sectors | CISA.

Who is the critical infrastructure community?

The critical infrastructure community includes the owners and operators of critical infrastructure, officials across all levels of government, and ultimately, all of us who benefit from the critical infrastructure around us. Just as we all rely on critical infrastructure, we all play a role in keeping it strong, secure, and resilient. Securing and making critical infrastructure resilient is a shared responsibility—shared by federal, state, local, tribal, and territorial governments; private companies; and individual citizens.

The American public can do their part at home, at work, and in their local communities by being prepared for all hazards, reporting suspicious activities to local law enforcement, and learning more about critical infrastructure security and resilience.

Why is it important to focus on the critical infrastructure needs of the country?

Critical infrastructure provides essential services that we use every day. Due to the various dependencies and interdependencies between infrastructure sectors, a disruption or breakdown in any one sector could create cascading effects that impact other sectors, which, in turn, affects still more sectors.

Most of the nation's critical infrastructure is privately owned and operated, and both the government and private sector have a shared responsibility to prevent and reduce the risks of disruptions to critical infrastructure. Investments in infrastructure protection are crucial to the resilience of the public and private sectors.

Together, public and private efforts to strengthen critical infrastructure show a correlated return on investment. Not only do these efforts help the public sector enhance security and rapidly respond to and recover from all hazards, but they also help the private sector restore business operations and minimize losses in the face of an event.

How do cyber interdependencies affect infrastructure security?

Critical infrastructure is highly interconnected, and any single system may rely on other critical infrastructure to run at normal operations. The integration of cyber-physical technologies and systems that deliver our critical functions — from manufacturing to healthcare to transportation and beyond — means that single

events can manifest in the loss or degradation of service across multiple industries. Operational technology and industrial control systems pose unique risks that demand particular focus due to the heightened consequences of disruption and challenges related to deploying certain security controls at scale. While new and emerging technologies are vital drivers of innovation and opportunity, they can also present unanticipated risks. Similarly, unforeseen interdependencies can lead to systemic risk conditions and cascading impacts. Such an evolving environment requires a more unified approach than ever before.

CISA makes available several resources that further inform actions organizations can take to integrate security, including:

- **Cybersecurity and Physical Security Convergence Guide**: An informational guide about convergence and the benefits of a holistic security strategy that aligns cybersecurity and physical security functions with organizational priorities and business objectives. The guide describes the risks associated with siloed security functions, a description of convergence in the context of organizational security functions, benefits of convergence, a flexible framework for aligning security functions, and several case studies. To learn more, visit Cybersecurity and Physical Security Convergence Action Guide | CISA.
- **Energy Sector Spotlight: Cyber-Physical Security Considerations for the Electricity Sub-Sector**: A co-branded product with the Department of Energy that provides small and mid-sized municipalities, utility owner operators, and the broader critical infrastructure community with a quick-hit product that highlights key cyber-physical attack vectors facing the electricity sub-sector, best practices for mitigating risk, and recommendations for maintaining resilience. To access the document, visit Sector Spotlight: Cyber-Physical Security Considerations for the Electricity Sub-Sector | CISA.
- **Stadium Spotlight: Connected Devices and Integrated Security Consideration**: A co-branded product with the National Center for Spectator Sports Safety and Security that provides stadium owner operators and security professionals with a snapshot of the connected stadium environment, key vulnerabilities and consequences, and recommended enterprise- and asset-level risk mitigations. To access the document, visit Stadium Spotlight: Connected Devices and Integrated Security Considerations | CISA.

It is also important to understand not only how critical infrastructure relies on secure cyber systems, but also how to protect our critical infrastructure against cyberattacks. Through Critical Infrastructure Security and Resilience Month, CISA promotes shared awareness and understanding of the diverse hazards affecting critical infrastructure resilience. For tools and tips on cybersecurity visit Cybersecurity Best Practices | CISA.