2022 INFRASTRUCTURE SECURITY MONTH

INFRASTRUCTURE SECURITY IS NATIONAL SECURITY: DRIVE DOWN RISK, BUILD RESILIENCE.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

CONTENTS

WELCOME TO INFRASTRUCTURE SECURITY MONTH 2022 2
HELP DRIVE DOWN CRITICAL INFRASTRUCTURE RISK AND BUILD RESILIENCE 3
WHAT YOU CAN DO 8
TEMPLATES 11
SOCIAL MEDIA AND ONLINE RESOURCES 14
FREQUENTLY ASKED QUESTIONS (FAQS) 16

WELCOME TO INFRASTRUCTURE SECURITY MONTH 2022

Each November we celebrate Infrastructure Security Month. This year, the Cybersecurity and Infrastructure Security Agency (CISA) reminds everyone that *Infrastructure Security is National Security. Together We Can Drive Down Risk, Build Resilience*. Keeping the nation's critical infrastructure secure is important to our national security. Critical infrastructure spans everything from healthcare, water and education to chemical, transportation, and energy systems—and much more. It is interdependent with other critical infrastructure and supporting systems and encompasses all the essential services and critical functions that keep our country and our economy running.

Not only do we need to protect critical infrastructure and people in and around those facilities from physical threats, but we also need to be aware of new cyber vulnerabilities that emerge as our critical infrastructure systems increasingly integrate information technology (IT) and operational technology (OT) into operations. Adversaries are eager to disrupt critical infrastructure by any means possible, which is why this November, as we celebrate Infrastructure Security Month, we ask everyone to join us in focusing on ways to reduce risk and build resilience on both the physical and cyber fronts.

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 Infrastructure Security Month. Be sure to follow us on social media and take part in the hashtags #infrastructure and #InfrastructureResilience conversation!

THIS NOVEMBER, TAKE ACTION ON INFRASTRUCTURE SECURITY

Start by visiting Infrastructure Security Month | CISA to learn more about critical infrastructure and available resources, training, and tips.

HELP DRIVE DOWN CRITICAL INFRASTRUCTURE RISK AND BUILD RESILIENCE

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 and enhancing resilience.

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.

Critical infrastructure is a shared resource as well as a shared responsibility - we all play a role in keeping it secure, and resilient.

THE CURRENT THREAT ENVIRONMENT

Today's risks and threats are complex, geographically dispersed, and affect a diverse array of stakeholders, including federal civilian government agencies, private sector companies, state, local, tribal, and territorial (SLTT) governments, and ultimately the American people. Our increasingly interconnected, global cyberspace presents profound challenges in which we face 24/7/365 asymmetric, cyber threats with large scale real-world effects. For example, in May 2021, a major pipeline in the U.S. was hit with a ransomware attack causing them to them to halt all pipeline operations for several days, disrupting the routines of millions of Americans as well as the economy.

The diversity, complexity, and sheer expanse of our nation's physical infrastructure also poses unique challenges. Securing critical infrastructure, public gatherings, schools and universities, and key facilities from the threats of terrorist attacks and targeted violence remains a key priority. The risks posed by a changing climate are equally daunting. As climate events grow more extreme, we can expect natural hazards, scarcities, and system stresses to place further strain on the nation's infrastructure. All of these factors demand a greater focus on resilience.

CROSS-CUTTING RESOURCES

- The CISA Services Catalog is all of CISA, all in one place – a single resource that provides users with access to information on services across all of CISA's mission areas that are available to federal government; SLTT; private industry; academia; and NGO and non-profit stakeholders.
- The Cross-Sector Cybersecurity Performance Goals were developed in close partnership with organizations across government and the private sector. It 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 provides security resources specific to Faith-Based Organizations at Faith Based Organizations - Houses of Worship | CISA, including a Houses of Worship Security Self-Assessment at Houses of Worship | CISA that many states accept as part of Nonprofit Security Grant Program applications.
- School administrators can visit SchoolSafety.gov which houses a comprehensive repository of federal and state resources, programs, tools, and actionable recommendations on a variety of school safety threats and topics, including physical security, cybersecurity, and targeted violence.

ADDITIONAL RESOURCES

CISA provides several resources that support security capacity building efforts, including those focused on active shooter preparedness, vehicle ramming mitigations, unmanned aircraft systems (sUAS), 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 security and vulnerability.

Understand the Risks

- 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 Qualified Bidder and Manufacturer Lists Report and Vendor Supply Chain Risk Management 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; and others.
- Use CISA's Insider Risk Mitigation *Self-Assessment Tool* to assess your organization's vulnerability to an insider threat.
- Learn about the *Drought and Infrastructure: A Planning Guide (Drought Guide)* which introduces the nature of drought, how it can affect infrastructure operations, and federal agency sources of information and drought mitigation planning tools. The guide is used by CISA Regional staff, local, tribal, territorial, and regional governments, communities, infrastructure providers, and other stakeholders to anticipate and reduce the potential consequences of droughts on critical water, transportation, dams, power, and other services.
- CISA develops and deploys capacity building training and tools to support and enhance school safety and security. Resources include CISA's *K-12 School Security Guide Suite*, which provides K-12 schools and districts with guidance, strategies, and recommendations to assess for vulnerabilities and implement layered elements of physical security.
- 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.
- Download and use the *Counter-IED Security and Resiliency Guide* and accompanying *fact sheet*.
- 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 training courses.

- Request a ChemLock on-site chemical security assessment so that CISA chemical security experts can identify the specific security risks that your on-site chemicals present and offer scalable, tailored suggestions for security measures that will best enhance their security posture based on your unique circumstances and business model.
- Make sure you know whether you need to report any dangerous chemicals under the Chemical Facility Anti-Terrorism Standards (CFATS) program. Check out the list of chemicals of interest at Chemical Facility Anti-Terrorism Standards webpage.
- As the holiday season approaches, review the *CISA Protecting Patrons During the Holiday Shopping Season document*. Although there are currently no credible or imminent threats, places where the public gathers can benefit from assessing existing security practices to ensure effective procedures are in place.
- CISA developed two infographics on Cyber Risks and Resources for the Water and Wastewater Systems Sector to provide water and wastewater systems managers and SLTT partners with an overview of the cyber risks they may face and to highlight resources available to help them enhance their cybersecurity. Each infographic focuses on a specific National Critical Function (NCF): Supply Water and Manage Wastewater. Compromise to these NCFs could lead to an incident resulting in public health and safety concerns, environmental damage, and/or economic disruption. These infographics identify risks under three categories—Information Technology (IT), Operational Technology (OT), and IT/OT convergence—and demonstrate some of the potential risks (i.e., steal sensitive data, disable network components, and compromise operations) that can be caused by malicious cyber-attacks.
    - *Cyber Risks & Resources for the Supply Water National Critical Function Infographic*
    - *Cyber Risks & Resources for the Manage Wastewater National Critical Function Infographic*
    - *Additional Resource Link: National Critical Functions (NCF) Fact Sheet*

Train and prepare for potential incidents.

- 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.
- 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 Guide | CISA*.
    - CISA also conducts Active Shooter Preparedness webinars to directly support organizations in developing emergency action plans through live instructor-based training.
- Learn about the actions that may be taken within legal parameters to mitigate implications of unauthorized overflights of unmanned aircraft systems. Visit UAS - Critical Infrastructure | CISA.
- 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. Sign up today: Counter-IED Training and Awareness | CISA.
    - For additional information on Counter-IED training, assessment, and planning, read *OBP's fact sheet*.
- Download and use the *Outdoors Event and Public Assembly products* 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 - 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 provides Insider Threat Mitigation workshops at the request of stakeholders to their Protective Security Advisor (PSA) that define an insider and insider threat, how to build and Insider Threat Mitigation Team, and how to mitigate and recover from insider threat incidents.
    - Visit CISA's Insider Threat Resources page for more materials on how to recognize, prepare for, and recover from insider threat incidents.
- CISA's ChemLock Exercises offers CISA Tabletop Exercise Packages (CTEPs), drills, and general materials to help facilities conduct exercises that are tailored specifically for chemical security.
- More than 96 percent of manufactured goods involve chemicals in some way—and many of these chemicals could be exploited in a terrorist attack. CISA has developed voluntary and regulatory chemical security programs and resources to help stakeholders—private industry, public sector, and law enforcement—enhance the security of facilities that possess dangerous chemicals from many threats: cyberattacks, biohazards, insider threats, and theft and diversion for use in chemical or explosive weapons.

Report suspicious activity.

- There have been numerous examples of the public identifying something suspicious and reporting that to police. Such information has helped prevent attacks.
- 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 stakeholders with 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 *path to violence*.
- Be prepared to know 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 for Critical Infrastructure Owners and Operators*.
    - 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.
- 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) 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" *poster and postcard* 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.
- The CISA *Insider Threat Mitigation Guide* provides information to create or enhance an organization's insider threat mitigation program. It highlights behavioral indicators and suspicious activity stakeholders should identify and report to their organization's multi-disciplinary threat management team for further assessment.

- 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*. Facilities with dangerous chemicals regulated by the Chemical Facility Anti-Terrorism Standards (CFATS) program must comply with 18 Risk-Based Performance Standards (RBPS). Two of these RBPS address reporting significant security incidents and suspicious activities.

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 organization. A number of our resources are listed below for quick reference, and we encourage you to visits CISA.gov for more.

Private Sector

- ✓ Improve security through a series of steps, including:
  - *Understand risk*: from a national (e.g., DHS National Terrorism Advisory System Bulletin) and local (e.g., connecting with the local fusion center) perspectives. Also conduct a vulnerability assessment of your facility as each face unique challenges.
  - *Implement measures*: based on potential threats and results of the vulnerability assessment, implement measures to mitigate vulnerabilities by leveraging the suite of resources that CISA makes available.
  - *Develop and exercise a plan*: through a security and/or emergency action plan, document the processes that personnel/volunteers should take to enhance security before and respond following an incident. Exercise plan(s) build muscle memory.
  - *Build soft skills:* augment security beyond traditional protective measures by positioning personnel/volunteers to be able to identify potential suspicious behavior and to take appropriate action to thwart a potential attack.
- ✓ Additionally, there are many other ways you can take action to drive down risk and build resilience:
  - 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.
- ✓ Visit Telework | CISA for guidance on teleworking securely.
- ✓ Visit Hometown Security | CISA for free tools and resources for small- and medium-sized businesses related to security and resilience.
- ✓ 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 | CISA.
- ✓ Learn about resources available for vulnerability assessments and continuity plans, including Critical Infrastructure Vulnerability Assessments | CISA.
- ✓ Learn about the legal protections for information shared with CISA under the Protected Critical Infrastructure Information (PCII) Program at PCII Program | CISA.
- ✓ Integrate cybersecurity into facility and operational protective measures.
- ✓ Build resilience into facility design and operations.
- ✓ Report suspicious activity to local law enforcement to public safety officials to discuss security and resilience enhancements.
- ✓ 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 Infrastructure Security Month | CISA.
- ✓ 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 and tools to enhance the security of those dangerous chemicals to ensure that they are not weaponized.
- ✓ Make sure you know whether you need to report any dangerous chemicals under the Chemical Facility Anti-Terrorism Standards (CFATS) program. Check out the list of chemicals of interest on the Chemical Facility Anti-Terrorism Standards webpage.
- ✓ Add your voice to social media conversations by using the hashtags #infrastructure and #InfrastructureResilience about critical infrastructure issues and how they relate to your mission and to the security environment of your office.

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.

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 Infrastructure Security | 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 (ISC) | 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 op-ed in the local paper about the importance of critical infrastructure security and resilience.

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 op-ed 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.

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."

PRESS RELEASE

(Date – Month, Day), 2022
Contact: (Contact Name), (Phone/Email)

(ORGANIZATION) Joins National Effort to Promote Infrastructure Security and Resilience

CITY, STATE – November is Infrastructure Security Month.

(ORGANIZATION) has committed to participate in Infrastructure Security 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 *Infrastructure Security is National Security: Together we can Drive Down Risk, Build Resilience*. Keeping the nation's critical infrastructure secure is important to our national security. Critical infrastructure spans everything from healthcare, water and education to chemical, transportation, and energy systems—and much more. It is interdependent with other critical infrastructure and supporting systems and encompasses all the essential services and critical functions that keep our country and our economy running.

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 Infrastructure Security Month | CISA.

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

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

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 Infrastructure Security 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.

Infrastructure Security is National Security: Together We Can Drive Down Risk, Build Resilience

November is Infrastructure Security 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 *Infrastructure Security is National Security: Together We Can Drive Down Risk, Build Resilience*, which covers the spectrum of infrastructure security. The threats to our critical infrastructure range from severe weather events to technological hazards and complex incidents. It includes physical threats originating here at home, as well as cybersecurity activities launched from across the globe by adversaries seeking ways to disrupt or destroy the essential services we rely on for health and economic and national security.

Keeping the nation's critical infrastructure secure is important to our national security. Critical infrastructure spans everything from healthcare, water and education to chemical, transportation, and energy systems—and much more. It is interdependent with other critical infrastructure and supporting systems and encompasses all the essential services and critical functions that keep our country and our economy running.

As our critical infrastructure systems increasingly take advantage of benefits offered by integrating information technology (IT) and operational technology (OT), new vulnerabilities are exposed. Adversaries are eager to disrupt critical infrastructure by any means possible, which is why this November as we recognize Infrastructure Security Month, we ask everyone to focus on ways they can reduce risk and build resilience on both the cyber and physical fronts.

To learn more, visit Infrastructure Security Month.

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

Infrastructure Security Month
November 2022

WHEREAS, "Infrastructure Security 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 2022 as Infrastructure Security 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 _____ 2022 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 hashtags #infrastructure and #InfrastructureResilience to join the conversation. Also, be sure to check our page for updates at Infrastructure Security Month | CISA.

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.

- ✓ "Critical Infrastructure Protection" (1:18 duration): Critical Infrastructure Protection - YouTube
- ✓ "Protected Critical Infrastructure Information (PCII) Program" (3:22 duration): Protected Critical Infrastructure Information (PCII) Program - YouTube
- ✓ "Options for Consideration Active Shooter Training Video" demonstrates possible actions to take if confronted with an active shooter scenario (7:52 duration): Options for Consideration Active Shooter Training Video - YouTube
- ✓ Three "Be Vigilant" videos provide guidance about the steps the public and businesses should take to recognize and report suspicious activity in order to prevent a bombing incident: Be Vigilant - YouTube
- ✓ Three "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" - YouTube
- ✓ "Vehicle Ramming Attack Mitigation" provides insightful analysis and recommendations aimed at protecting organizations and individuals against a potential vehicle ramming incident (12:39 duration): Vehicle Ramming Attack Mitigation - YouTube
- ✓ "Understanding the Insider Threat" uses security and behavior experts to discuss how insider threats manifest in a variety of ways, including terrorism, workplace violence, and breaches of cybersecurity (30:36 duration): Understanding The Insider Threat Video - YouTube
- ✓ "UAS and Critical Infrastructure—Understanding the Risk" contains information on critical infrastructure security challenges associated with the UAS threat, counter-UAS security practices, actions to consider for risk mitigation, and messaging for facility and organizational preparedness related to UAS incidents (11:00 duration): UAS and Critical Infrastructure – Understanding the Risk - YouTube
- ✓ "Pathway to Violence" discusses behavioral indicators that assailants often demonstrate before a violent act (11:07 duration): Pathway to Violence - YouTube
- ✓ "Active Shooter Emergency Action Plan" guides viewers through important considerations of EAP development utilizing the firsthand perspectives of active shooter survivors, first responder personnel, and other subject matter experts who share their unique insight (1:36:24 duration): Active Shooter Emergency Action Plan - YouTube
- ✓ "K 12 Education Leaders' Guide to Ransomware Prevention, Response, and Recovery" is a webinar on the steps #K12 schools can take to prevent, respond to, and recover from #ransomware attacks (12:39 duration): K 12 Education Leaders' Guide to Ransomware Prevention, Response, and Recovery - YouTube

- ✓ “What Is CFATS?” is a brief informational video that provides an introductory overview of the Chemical Facility Anti-Terrorism Standards (CFATS) program: What is CFATS? - YouTube

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 (SLTT) 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.

What are some of the challenges facing critical infrastructure today?

Risks to critical infrastructure can come from natural or weather related events; they can also come from a diverse group of threat actors including nation states, as well as cybercriminals, terrorist groups, and other malicious actors seeking to take advantage of our open society and the proliferation of technology to do us

harm.

Aging, outdated, and under-resourced infrastructures are also a challenge across the country. During any emergency, communication between first responders and between decision-makers is at risk from disruption or lack of interoperability.

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 (OT) and industrial control systems (ICS) 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 | 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 Infrastructure Security Month, CISA promotes shared awareness and understanding of the diverse hazards affecting critical infrastructure resilience. For tools and tips on cybersecurity visit CYBERSECURITY | CISA.