2021 INFRASTRUCTURE SECURITY MONTH

INFRASTRUCTURE SECURITY AND RESILIENCE: BUILD IT IN

November 2021

cisa.gov

CONTENTS

INFRASTRUCTURE SECURITY MONTH TOOLKIT

Welcome to Infrastructure Security Month 2021

Each November we recognize Infrastructure Security Month. This year's theme is *Infrastructure Security: Build It In* to remind all audiences how important it is to consider infrastructure security and resilience from design concept all the way through development and implementation. This annual campaign provides opportunities to shine a light on key resources and actions that organizations and individuals can take, as well as initiatives impacting the future of critical infrastructure security and resilience, such as new legislation, policy, and doctrine.

As the nature of the threat to critical infrastructure evolves and as CISA's work and partnership with the private sector matures, the agency is shifting its focus from asset protection to building in resilience to the wide range of threats and hazards from the start.

Each week throughout November, the agency will spotlight a different way to think about how we build in critical infrastructure security and resilience:

- **Week 1 (November 1-7):** Interconnected and Interdependent Critical Infrastructure: Shared risk means building in shared responsibility.
- **Week 2 (November 8-14):** Secure Public Gatherings: Build in security for mass gatherings starting with your planning.
- **Week 3 (November 15-21):** Build Security and Resilience into Critical Infrastructure
- **Week 4 (November 22-30):** Secure Elections: Building resilience into our democratic processes.

KEY MESSAGES

- November is Infrastructure Security Month. All month we are asking stakeholders to "Build it In" as a reminder of how important it is to consider infrastructure security and resilience from design concept all the way through development and implementation.
- Much of the nation's critical infrastructure is interconnected and interdependent, which means an incident in one area can have impacts across multiple sectors, creating disruptions for many communities. We saw examples earlier this year when major cyberattacks caused issues up and down the supply chain.
- Because our nation relies on critical infrastructure for health, energy, communications, and other vital services, it is equally important that everyone understand their role and take action to ensure our critical infrastructure remains strong, secure, and functional.
- Some of the ways we can work toward this goal include:
    - Strengthening preparedness plans for a variety of security risks to public gatherings, such as insider threats and active shooters.
    - Sharing information about best practices, conducting assessments to identify vulnerabilities, building partnerships across the critical infrastructure community, and offering training and providing tools to critical infrastructure stakeholders.
    - Helping to secure democracy by building more resiliency into the election process.
    - Recognizing the unique expertise and capabilities of the government, private, and nonprofit sectors and integrating them into the national effort to build more resiliency into the country's critical infrastructure.

HOW TO PROMOTE INFRASTRUCTURE SECURITY AND RESILIENCE AWARENESS

INTRODUCTION

- November is Infrastructure Security Month, a time to shine a light on the vital role that critical cyber and physical infrastructure plays in keeping the nation and our communities safe, secure, and prosperous.
- We are promoting four sub-themes for Infrastructure Security Month 2021, under the overarching theme of *Infrastructure Security and Resilience: Build it In*. These include:
    - Week 1 (November 1-7): Interconnected and Interdependent Critical Infrastructure: Shared risk means building in shared responsibility.
    - Week 2 (November 8-14): Secure Public Gatherings: Build in security for mass gatherings starting with your planning.
    - Week 3 (November 15-21): Build Security and Resilience into Critical Infrastructure.
    - Week 4 (November 22-30): Secure Elections: Building resilience into our democratic processes.
- Infrastructure Security Month is a time to think about how each of us can contribute to the security and resilience of the nation's most essential services and functions, such as:
    - Instant access to information and communications
    - Safe, clean drinking water
    - Reliable transportation
    - Agriculture that supplies plentiful year-round food
    - Chemical security for plastics, electronics, medicine, and fuel
    - Election systems and infrastructure
- Everyone plays a role in the nation's security and resilience, and we must understand and accept our shared responsibility in managing our shared risk.
- During this year's Infrastructure Security Month, we ask every organization to:
    - Remember if you share risk, you must also share the responsibility to reduce that risk.
    - Reevaluate your preparedness plans on securing public gatherings and make sure they are up to date with the latest techniques and tactics.
    - Consider ways to make resilience part of the design when upgrading or building new critical infrastructure.
    - Help people understand and identify misinformation, disinformation, and conspiracies appearing online related to COVID-19, 5G, election security, or other infrastructure related issues.

THE THREAT ENVIRONMENT

Events in 2021 have highlighted the interconnectedness of the nation's critical infrastructure and the need to build in security and resilience from the earliest point possible.

Many of the threats we face now build on issues that emerged in 2020. For example, the massive shift to virtual and hybrid environments that started in response to COVID-19 pandemic restrictions have become more prevalent, opening additional vulnerabilities in our online environment. The start of the year was marked by the violent January 6 riots at the nation's Capital, which made national news and impacted government critical infrastructure due to widespread misinformation and disinformation campaigns about the Presidential election results.

Threats to mass gatherings persist. Facilities housing dangerous chemicals continue to be targeted by terrorist groups both domestic and abroad.

Significant cyber intrusions, beginning with the SolarWinds compromise discovered at the end of 2020 and continuing with Kaseya and ransomware attacks on critical infrastructure like oil and agriculture, have highlighted the very real physical impacts that cyber intrusions can have on interconnected and interdependent critical infrastructure.

In 2021, climate change has also become increasingly prominent in the headlines as the nation endured increasingly extreme weather and wildfires. Critical infrastructure like dams and water were impacted by extreme drought, and communities (and their infrastructure) have been impacted by massive and prolonged wildfires in the West, while the nation's southern and eastern states saw widespread flooding.

Despite the threats, there is ample opportunity to mitigate or even avoid much of the risk. The monthly theme and supporting weekly messages will highlight ways that we can "build in" security and 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 cyber and physical infrastructure. Fortunately, there are steps we can take to help keep these systems running smoothly. Below we have outlined this year's themes with a spotlight on the issue behind the theme and how you can get involved.

Week 1: Interconnected and Interdependent Critical Infrastructure: Shared Risk Means Building in Shared Responsibility

THE ISSUE

- In today's globally interconnected world, our critical infrastructure and American way of life face a wide array of risks with significant real-world consequences.
- This is something we have known for years but is now being felt by the public with every cyber breach and ransomware attack.
- Today, the critical functions within our society are built as "systems of systems" – complex designs with numerous interdependencies and systemic risks that can have cascading effects.
- And as we've witnessed over the past year, as these networked systems and devices further weave into our lives and businesses, their vulnerabilities provide additional attack vectors and a larger attack surface for nation-state adversaries and cyber criminals to exploit.
- Many of the risks we face today are complex, dispersed both geographically and across a variety of stakeholders. They are challenging to understand and even harder to address.
- In today's system-of-systems world, no single private or government entity has all the information necessary to manage systemic risk. A breach on one system can also impact multiple cyber and physical systems that are connected or dependent on it to operate.
- Information and communications technology (ICT) have accelerated digital transformations in almost every part of society. However, when a supply chain incident occurs, everyone suffers: buyers, suppliers, and users. In a world of shared risks, securing the global ICT supply chain requires an ongoing, unified effort between government and industry.
- With most of the nation's critical infrastructure privately-owned, sector expertise is necessary to understand, as complete as possible, the systemic risk picture that the consequences of a threat— cyber, physical, technological, or natural— can have on operations or functions in multiple sectors and on the National Critical Functions.
- The ubiquitous use of the Global Positioning Navigation (GPS) as the primary source of positioning, navigation, and timing information makes many sectors and National Critical Functions vulnerable to adversaries seeking to cause harm by disrupting or manipulating the GPS signal.

HOW TO GET INVOLVED

- We invite you to join this effort in whatever capacity is right for your organization.

    - Take advantage of our free training and information to get more informed.
    - Take the free, online Cyber Supply Chain Risk Management course which provides an introduction of what a supply chain is, how adversaries target supply chains, and steps that individuals and organizations can take to improve supply chain security.
    - Learn about your organization's risks by participating in one of our assessments.
    - Reach out to CISA at Central@cisa.gov to begin participating in one of our information sharing programs and share information to help fill gaps in knowledge and understanding across the community.
    - Learn from other practitioners, through events like CISA's Chemical Security Seminars. This year's seminars focus on cyber and physical aspects of chemical security – and registration is open now.
    - 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.
    - Share CISA's Information and Communications Technology (ICT) Toolkit to emphasize the role we all have in securing ICT supply chains.
    - CISA's Supply Chain Risk Management (SCRM) Essentials is a guide for leaders and staff with actionable steps on how to start implementing organizational SCRM practices to improve their overall security resilience.
    - Learn how Positioning, Navigation, and Timing (PNT) impacts critical infrastructure operations. CISA published the *Understanding Vulnerabilities of Positioning, Navigation, and Timing (PNT) fact sheet* to provide critical infrastructure owners/operators and equipment manufacturers an overview of critical infrastructure dependencies on PNT services and the need to strengthen the nation's security and resilience from the impact of PNT disruptions on critical operations and services.
- There are many ways you and your organization can take part in our collective defense. Start today by visiting cisa.gov or reaching out to your CISA regional office.

Week 2: Secure Public Gatherings: Build in security for mass gatherings starting with your planning.

THE ISSUE

- Our nation has experienced too many violent attacks against the places in our communities where we should feel safest. These attacks have targeted crowded places and community members in public venues where they gather to learn, socialize, worship, and patronize local businesses.
- Terrorists and violent extremist actors target infrastructure that have the potential to inflict significant personal harm to individuals, to intimidate or coerce a government, the civilian population, or any segments of this population, to further their political or social objectives.
- Public gatherings, such as sports venues, schools, and transportation systems, are locations that are easily accessible to large numbers of people and that have limited security or protective measures in place making them vulnerable to attack.
- Enhancing the security of public gathering areas continues to be a priority for CISA. The agency works with partners in the public and private sectors to identify, develop, and implement innovative measures to mitigate risks to public gatherings and crowded places in a manner that does not negatively impact operations.
- While not all attacks can be stopped, many can be prevented through focused security and preparedness efforts.

HOW TO GET INVOLVED

- CISA provides several resources, including those focused on active shooter preparedness, vehicle ramming mitigations, and bombing prevention. We also conduct exercises to help stakeholders assess their plans, and we provide free site visits to assess security and vulnerability.
    - Use CISA's Insider Risk Mitigation *Self Assessment Tool* to assess your organization's vulnerability to an insider threat.
    - Learn about CISA's vehicle ramming mitigation solutions.
    - CISA provides active shooter resources in multiple languages for first responders, human resources, security professionals, and private citizens: Active Shooter Preparedness | CISA
    - 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.
    - School administrators can visit SchoolSafety.gov which houses a comprehensive repository of federal and state school resources, programs, tools, and actionable recommendations and resources on a variety of school safety threats and topics, including physical security and targeted violence.
    - Download and use the Outdoors Event and Public Assembly products to protect venues from bombings and the Security and Resiliency Guide for Public Assembly.
- Report suspicious activity. The public plays an important role in the safety and security of our communities across the country.
    - There have been numerous examples of the public identifying something suspicious and reporting that to police. Such information has helped prevent attacks.
    - The *Employee Vigilance Through the Power of Hello* slick-sheet and placemat provides stakeholders with information to assist in identifying and effectively responding to suspicious behavior. Additionally, these resources have been translated into 16 languages including Dari and Pashto and can be found here: Power of Hello Translations.
    - 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.
    - 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, or if an emergency response is needed immediately; de-escalate the situation currently taking place through purposeful actions, verbal communication, and body language; and report the situation through organizational reporting to enable assessment and management of an evolving threat and 9-1-1 for immediate threats.
    - 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.
    - CISA's *Personal Security Considerations fact sheet* encourages stakeholders to remain vigilant and report suspicious behavior. It also provides easily implementable security measures that can mitigate threats to personal safety.

- Plan and prepare for potential incidents ranging from active shooters to bomb threats to Unmanned Aircraft Systems (UAS).
    - The CISA Securing Public Gatherings webpage houses resources to help organizations mitigate potential risks.
    - CISA created a guide to support stakeholders in mitigating potential risks associated with the dynamic threat environment: *Security of Soft Targets and Crowded Places – Resource Guide*.
    - Our Active Shooter Preparedness webpage provides resources to help stakeholders prepare for and respond to and active shooter incident.
    - The *Insider Threat Mitigation Guide* provides comprehensive information on how to establish or enhance an insider threat prevention and mitigation program.
    - The Unmanned Aircraft Systems (UAS) Frequently Ask Questions (FAQs) webpage provides information and resources on the lawful use of UAS as well as the threat UAS pose to critical infrastructure.
    - The *National Interoperability Field Operations Guide (NIFOG)* is our principal reference for interoperability during key planned events, major public safety incidents, or disasters.
- 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 discussions within their organizations. Each package can be customized and includes templates with exercise objectives, scenarios, and discussion questions.
    - 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*.
    - 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.
    - Visit CISA's Insider Threat Resources page for more materials on how to recognize, prepare for, and recover from insider threat incidents.
    - CISA also provides materials on how to identify potential signs that someone is on a path to violence.
    - CISA develops and deploys capacity training and tools to support and enhance school safety and security. Resources, like CISA's *K-12 School Security: A Guide for Preventing and Protecting Against Gun Violence (2nd Edition)*, provide preventive and protective measures to address the threat of gun violence in schools.

Week 3: Build Security and Resilience into Critical Infrastructure

THE ISSUE

- The critical infrastructure upon which communities rely faces an array of ever-evolving threats, from terrorist attacks and cyber intrusions to extreme weather and deferred maintenance.
- Investing in critical infrastructure that can withstand and quickly recover from all threats is essential to maintaining our nation's economy, security, and health.
- For the private sector, this investment includes building security into your everyday business practices and decisions and helping to ensure that it becomes part of your organization's culture. The best security planning is tailored to your operating environment and becomes part of your routine.
- Building strong security means understanding the risks you face. For example, every day, thousands of American businesses interact with chemicals that terrorists could use as weapons, with

devastating consequence. For those who use, manufacture, and transport these materials, understanding the risk allows security planning to be integrated into safety and business protocols.
- Adversaries target organizations of all sizes and in every industry, so cybersecurity is not just a large business problem. It's no longer enough for organizations to focus on securing their own data and information systems; they must also encourage enhanced cybersecurity practices of their managed service providers (MSPs).

HOW TO GET INVOLVED

- 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.
- Download and use the *Counter-IED Security and Resiliency Guide* and accompanying *fact sheet*.
- If your organization works with chemicals, make sure you understand the risk. CISA will be launching the ChemLock program to help ensure you understand the potential concerns and offer assistance and solutions to address security in your specific operating environment.
- Register for the 2021 Chemical Security Seminars to come together to discuss threats to the chemical industry, hear case studies from industry experts with real-world experience, and share best practices to enhance chemical security.
- 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 | CISA
- A *CISA Insights* titled "Risk Considerations for Managed Service Providers" provides a framework with an actionable checklist for organizations that choose to outsource their IT services. The resource provides guidance on how to proactively manage cybersecurity risk and collaborate with managed service providers to jointly reduce overall risk.
- 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.

Week 4: Secure Our Elections: Build resilience into our democratic processes

THE ISSUE

- While the 2020 election was the most secure in modern history, we shouldn't expect our adversaries to back off of these tactics in upcoming election cycles and we shouldn't expect election officials to combat sophisticated, state-sponsored threat actors on their own.
- CISA is expanding outreach to state, local, tribal, and territorial (SLTT) election officials, and enhancing our engagement with the private sector, to ensure that our partners have awareness of our extensive cyber and physical security tools, services, and resources.
- CISA is also working to increase public confidence in the integrity of the electoral system and has expanded efforts to help Americans recognize and avoid Mis/Dis/Mal-information (MDM).
    - This year we released *Bug Bytes*, the second graphic novel in our resilience series. The intent of this series is to help the American public understand the risks from foreign influence operations on our society and democracy.
    - It may be hard to visualize what MDM looks like. We're working to make that easier.

HOW TO GET INVOLVED

- State, local, tribal and territorial election officials and our private sector partners are encouraged to take advantage of CISA's extensive cyber and physical security services, tools, and resources.
- You can find out more on the items below by visiting our Election Security website.
    - Work with CISA's regional cybersecurity advisors (CSAs) to sign up for CISA's cyber hygiene scanning, which evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities and provides weekly reports to participants. Additional cybersecurity services include phishing assessments, remote penetration testing, and other services that can reduce the risk of a successful cyber intrusion.
    - Work with CISA's regional protective security advisors (PSAs) to do an assessment of your physical infrastructure.
    - CISA can also help state and local election officials transition your government websites to the .gov top-level domain (TLD), which is now free of charge. Using a .gov domain helps voters to identify legitimate election information quickly and accurately and can help prevent the spread of election-related MDM.
    - Take advantage of CISA's training and exercise offerings. CISA offers a suite of trainings to the Election Infrastructure Sector, which provide an overview of the Agency's resources and services; best practices to protect, detect, respond, and recover from phishing and ransomware attacks; and best practices to build public trust in elections to help combat MDM.
    - CISA also hosts exercises, such as tabletops, to provide the Election Infrastructure sector with the means to identify areas for improvement, share plans and procedures, and enhance preparedness against threats to election infrastructure.
- SLTT officials and the private sector are encouraged to join the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), a voluntary, collaborative partnership between the Center for Internet Security (CIS), CISA, and the Election Infrastructure Subsector Government Coordinating Council (EIS GCC).
    - The EI-ISAC is funded through DHS grants and offers state and local election officials a suite of elections-focused cyber defense tools, including threat intelligence products, incident response and forensics, threat and vulnerability monitoring, cybersecurity awareness and training products.
- Check out the resources that CISA has developed to help the American public recognize and combat MDM and foreign influence activities targeting elections and critical infrastructure by visiting www.cisa.gov/mdm.
- Read *Bug Bytes,* the second graphic novel in CISA's Resilience Series, which communicates the dangers and risks associated with threat actors using social media and other communication platforms to spread MDM for the sole purpose of planting doubt in the minds of targeted audiences to steer their opinions.

THIS NOVEMBER, TAKE ACTION ON INFRASTRUCTURE SECURITY

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

FREQUENTLY ASKED QUESTIONS (FAQS)

About Infrastructure Security Month

What is Infrastructure Security Month?

Each November, CISA recognizes Infrastructure Security Month. This is an annual effort to educate and engage the public and private sectors, as well as the American public, about the vital role critical infrastructure plays in our nation's wellbeing and why it is important to strengthen critical infrastructure security and resilience.

This year's theme is *Infrastructure Security: Build It In* to remind all audiences how important it is to consider infrastructure security and resilience from design concept all the way through development and implementation. This annual campaign provides opportunities to shine a light on key resources and actions that organizations and individuals can take, as well as initiatives impacting the future of critical infrastructure security and resilience, such as new legislation, policy, and doctrine.

Each week throughout November, the agency will spotlight a different way to think about how we build in critical infrastructure security and resilience:

- **Week 1 (November 1-7):** Interconnected and Interdependent Critical Infrastructure: Shared risk means building in shared responsibility.
- **Week 2 (November 8-14):** Secure Public Gatherings: Build in security for mass gatherings starting with your planning.
- **Week 3 (November 15-21):** Build Security and Resilience into Critical Infrastructure.
- **Week 4 (November 22-30):** Secure Elections: Building resilience into our democratic processes.

About the significance of critical infrastructure

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, both natural and man-made. These hazards and threats include aging or failing infrastructure, extreme weather, cyberattacks, or evolving terrorism threats, which can 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.

The majority of our 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?

Many of the threats we face now build on issues that emerged in 2020. For example, the massive shift to virtual and hybrid environments that started in response to COVID-19 pandemic restrictions have become more prevalent, opening additional vulnerabilities in our online environment. The start of the year was marked by the violent January 6 riots at the nation's Capital, which made national news and impacted government critical infrastructure due to widespread misinformation and disinformation campaigns about the Presidential election results. Threats to mass gatherings persist. Facilities housing dangerous chemicals continue to be targeted by terrorist groups both domestic and abroad.

Significant cyber intrusions, beginning with the supply chain compromise discovered at the end of 2020 and continuing with Kaseya and ransomware attacks on critical infrastructure like oil and agriculture, have highlighted the very real physical impacts that cyber intrusions can have on interconnected and interdependent critical infrastructure.

In 2021, climate change has become increasingly prominent in the headlines as the nation endured increasingly extreme weather and wildfires. Critical infrastructure like dams and water were impacted by extreme drought, and communities (and their infrastructure) have been impacted by massive and prolonged wildfires in the West, while the nation's southern and eastern states saw increased flooding.

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. Nearly all critical infrastructure relies heavily on network and other cyber support to operate essential systems. Today's critical infrastructure functions are inseparable from the information technology and control systems that support them.

Many of these control systems are now automated and connected to the internet to allow for offsite control, making them increasingly vulnerable to cyber intrusions. These systems operate many physical processes that produce the goods and services that we rely upon, such as energy, drinking water, emergency services,

transportation, and public health.

However, it is 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.

Visit cisa.gov/cybersecurity for tools and tips on cybersecurity.

How to Get Involved

Private Sector, Including Owners and Operators

- ✓ 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
- ✓ Meet with your local Protective Security Advisor, Cybersecurity Advisor, Chemical Inspector or Emergency Communications Representative to better understand infrastructure in your area. (For more information on how to contact CISA in your area, contact central@cisa.gov.)
- ✓ Learn about resources available for vulnerability assessments and continuity plans, including Critical Infrastructure Vulnerability Assessments | CISA and Business | Ready.gov.
- ✓ 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.
- ✓ Report suspicious activity to local law enforcement to public safety officials to discuss security and resilience enhancements.
- ✓ 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.
- ✓ 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/ismonth.
- ✓ Visit Identifying Critical Infrastructure During COVID-19 | CISA for guidance on the critical infrastructure during COVID-19.
- ✓ Register for the 2021 Chemical Security Seminars to come together to discuss threats to the chemical industry, hear case studies from industry experts with real-world experience, and share best practices to enhance chemical security.
- ✓ 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 | CISA.

Sector-Specific 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.

Members of Congress and Staff

- ✓ Meet with CISA representatives in your state or district to better understand your local infrastructure.
- ✓ 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 on critical infrastructure.
- ✓ Include a message about the importance of infrastructure in newsletters, mailings, and websites.
- ✓ Write an op-ed in your local paper about the importance of critical infrastructure.

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.
- ✓ Visit COVID-19 Disinformation Toolkit | CISA for guidance on misinformation/disinformation during the pandemic.
- ✓ Visit Identifying Critical Infrastructure During COVID-19 | CISA for guidance on the critical infrastructure during COVID-19.
- ✓ 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 in newsletters, mailings, and websites.
- ✓ Meet with CISA representatives in your state or district to better understand your local infrastructure.
- ✓ 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.

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), 2021
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 and 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)

During November, Infrastructure Security Month, we will promote our theme *"Build It In,"* which includes the following sub-themes:

- ✓ Week 1 (November 1-7): Interconnected and Interdependent Critical Infrastructure: Shared risk means building in shared responsibility.
- ✓ Week 2 (November 8-14): Secure Public Gatherings: Build in security for mass gatherings starting with your planning.
- ✓ Week 3 (November 15-21): Build Security and Resilience into Critical Infrastructure
- ✓ Week 4 (November 22-30): Secure Elections: Building resilience into our democratic processes.

Our nation relies on critical infrastructure for how we travel; communicate with our friends, family, coworkers, and customers; conduct business; handle money; obtain clean, safe food and water; and conduct additional important daily functions. Managing risks to critical infrastructure involves preparing for all hazards, reinforcing the resilience of our assets and networks, and staying ever vigilant and informed.

America's national security and economic prosperity are increasingly dependent upon critical infrastructure that is at risk from a variety of hazards, including cyberattacks. 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/ismonth.

(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.

Critical Infrastructure: Build in Security and 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 and Resilience: Build it In,"* as a reminder of how important it is to consider infrastructure security and resilience from design concept all the way through development and implementation. We will highlight how critical infrastructure is interconnected and interdependent which means multiple stakeholders may share risk, thus they must share the responsibility to reduce that risk.

Events in 2021 have highlighted the interconnectedness of the nation's critical infrastructure and the need to build in security and resilience from the earliest point possible. Despite the threats, there is ample opportunity to mitigate or even avoid much of the risk. The monthly theme and supporting weekly messages will highlight ways that we can "build in" security and resilience.

This November join us in recognizing our nation's infrastructure and celebrating those who work to keep it running. We all need to play a role in keeping infrastructure and our country strong, secure, and resilient. We can do our part at home, at work, and in our community by being vigilant, incorporating state-enforced safety practices and cybersecurity behaviors into our daily routines, and making sure that if we see something, we say something by reporting suspicious activities to local law enforcement.

To learn more, visit cisa.gov/ismonth.

The message contained in this press release was authored by 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 2021

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 at home, at work in the many businesses and industries that make up the critical infrastructure community, and in their local communities by being prepared for all hazards, reporting suspicious activities, and learning more about critical infrastructure security and resilience by visiting cisa.gov/ismonth. THEREFORE, BE IT RESOLVED that the [**GOVERNING BODY**] hereby proclaims November 2021 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 _____ 2021 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. Follow us on Twitter here @CISAgov and here @CISAInfraSec and retweet, like us at facebook.com/CISA and share, and follow us on Instagram @cisagov and share our messages about Infrastructure Security Month. Also, be sure to check our page for updates at cisa.gov/ismonth.

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