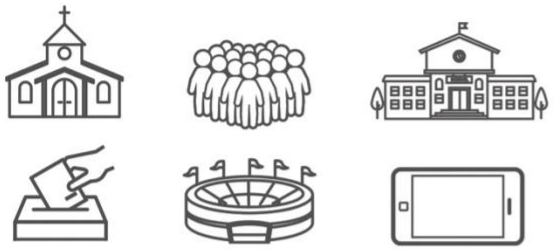

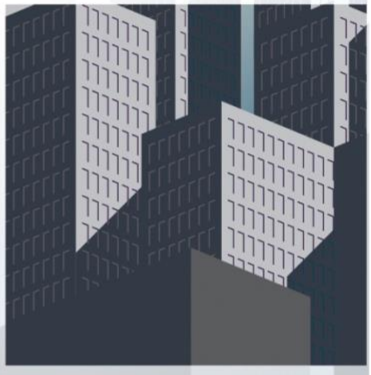

Infrastructure Security Month 2019

CISA.gov

CISA
CYBER+INFRASTRUCTURE

TABLE OF CONTENTS

INFRASTRUCTURE SECURITY MONTH TOOLKIT

Welcome to Infrastructure Security Month 2019

How often do you think about the things that sustain the American way of life? Safe transportation networks that get us where we need to go. Reliable and secure communications and internet infrastructure that connect us to the online tools and systems we rely on. Clean, available water for drinking and sanitation. Chemicals that are integral to everything from plastics to food preservation to medicines, and the electricity that keeps everything running. What about the malls, sports arenas, office buildings and other commercial facilities that house the places we gather for work and recreation? Even the systems that support our democratic processes—voting machines and the systems that support voting—are critical. Critical infrastructure security and resilience also includes the people who gather for activities that are part of our lives: attending a house of worship, going to a concert or other event, even gathering in a crowded open venue like a holiday market or festival.

These are just a few examples of the 16 critical infrastructure sectors and additional subsectors that are absolutely essential to the standard of living that Americans have come to expect and rely on every day. Yet most people take these things for granted. It's not until one of these systems breaks down that we truly appreciate all we have.

Infrastructure Security Month is a time to shine a light on the vital role that these systems and places play in keeping the nation and our communities safe, secure and prosperous. It is also 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—things like instant access to energy; safe, clean drinking water; reliable transportation; agriculture that supplies plentiful food year around; and even chemicals that are the building blocks of everything from plastics to electronics to fuel. Our infrastructure also includes the places that draw communities together to worship, learn or even enjoy a game or concert.

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) is leading the efforts on Infrastructure Security Month. In November 2018, Congress approved the Cybersecurity and Infrastructure Security Agency Act, creating CISA as a federal agency with the responsibility of leading the national effort to protect and enhance the security and resiliency of US cybersecurity, emergency communications, and critical infrastructure.

This mission requires effective coordination and collaboration among a broad spectrum of government and private sector organizations.

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

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

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

National Risk Management – CISA provides planning, analysis, and collaboration to identify and address the most significant risks to our nation's critical infrastructure. CISA works in close coordination with the private sector and other key stakeholders in the critical infrastructure community to: Identify; Analyze; Prioritize; and Manage the most strategic risks to our National Critical Functions.

This year, Infrastructure Security Month offers a chance to shine the spotlight on the systems and places that are so very important to maintaining the American way of life—and we want you to be part of the action. Read on to learn more about the issues and what you can do to contribute to a strong, resilient nation and economy.

HOW TO PROMOTE INFRASTRUCTURE SECURITY AND RESILIENCE AWARENESS

Managing risks to critical infrastructure requires an integrated approach across the whole-of community to identify, deter, detect, and prepare for threats and hazards to the Nation's critical infrastructure; reduce vulnerabilities of critical assets, systems, and networks; and mitigate the potential consequences to critical infrastructure of incidents or adverse events that do occur.

Much of this work is done through CISA's cross-cutting risk management efforts with the private sector and government to improve the defense of our nation's critical infrastructure.

We encourage you to involve your community and business leaders in the planning process. The information in this toolkit provides ideas for the events, messages, and communication techniques you can use to reach and engage your community.

Themes for Infrastructure Security Month 2019

Throughout the month of November, we will be encouraging our partners to enhance resilience through preparedness and exercises and promote smart, secure investment in resilient national infrastructure.

Each week, we will highlight a different theme. This year's themes reflect some of the nation's most pressing risks, as well as more perennial issues that are urgent nevertheless. These include:

- Managing risk to a converging cyber and physical world
- Protecting our hometowns: Soft target security
- Securing the American Democracy: Election security 2020
- Secure from the inside out: Combatting insider threats

Today's Threats and Issues

The threats to our critical infrastructure continue to evolve. As our world grows more interconnected, and our infrastructure grows more interdependent with other systems and functions, we must look at our risks from both a cyber and a physical perspective. Today, economic prosperity, health and safety rely on a complex network of physical and cyber systems, all working together in harmony. A major storm or wildfire can interrupt or destroy a region's power grid, and with a simple email, a determined adversary can then wreak havoc on that same infrastructure from the other side of the world. Either way, the impacts from the loss of power can quickly ripple through the regions, impacting emergency response, transportation, and financial transactions.

Below are just a few example of the priorities CISA is working on. No matter what line of work you are in or where you live, nearly everything you do relies on cyber and physical infrastructure. Fortunately, you can take steps to help keep these systems running smoothly. Get familiar with important critical infrastructure issues facing the Nation.

Cybersecurity

Internet-enabled systems and functions have revolutionized the way we work and play. Thanks to the wonders of technology, bank transactions, travel and communication are faster, more efficient and more economical. Yet these improvements also open up new vulnerabilities.

What you can do:

- Update your operating system and security software as soon as updates are available.
- Use complex passwords and don't share them.
- Implement cyber training for employees.
- Get educated on what you can do to prevent phishing/ransomware attacks.

Additional Resources

- https://www.cisa.gov
- https://www.cisa.gov/blog-list
- https://www.dhs.gov/stopthinkconnect

Soft Targets and Crowded Places

The places where people gather form the heart of American communities. Ordinary places like houses of worship, concerts, shopping centers, museums, movie theaters, sports arenas, and even office buildings are also places where we expect to feel safe and secure, but often their open, public nature means fewer security measures are in place.

Adversaries realize this as well, and in recent years terrorists and extremists have shifted tactics to focus on what we call soft targets and crowded places. Attackers can often carry out simple, low cost attacks using whatever is at hand—a vehicle, small arms, knives or improvised explosive devices. Such an attack might require few resources and very little planning, making it hard—but not impossible—to identify and thwart a would-be attacker.

What you can do:

- Connect with local responders, and learn about each other's responsibilities during an incident
- Plan and put in place the policies and procedures your organization needs to follow in an emergency.
- Train staff and volunteers on emergency plans and procedures;
- Report suspicious activity to local authorities.

Additional Resources

- https://www.cisa.gov/cisa/hometown-security
- https://www.cisa.gov/securing-soft-targets-and-crowded-places
- https://tripwire.dhs.gov

Insider Threats

According to the National Insider Threat Task Force, “The insider threat is the risk that an insider will use their authorized access, wittingly or unwittingly, to do harm to their organization. This can include theft of proprietary information and technology; damage to company facilities, systems or equipment; actual or threatened harm to employees; or other actions that would prevent the company from carrying out its normal business practice.”

This threat exists across public and private sector organizations. Insiders may be a trusted current or former employee, or a contractor or associate who causes harm, either wittingly or unwittingly, to a company or public sector.

Insider threats can manifest in a broad range of physical and cyber actions, from theft to subtle forms of sabotage to more aggressive and overt forms of vengeance, and even workplace violence.

What You Can Do

Whether you are a large corporation, a small business, or a government agency, it is important to consider all potential threats posed by trusted insiders as part of your overall security plans.

- **Form a Threat Management Team**: Given the significant risks associated with insider threats, organizations are encouraged to form Threat Management Teams that incorporate different disciplines within an organization such as human resources, security, and IT to address behaviors or incidents reported by employees or others.
- **Establish and Insider Threat Program:** Establishing an insider threat program is an important first step toward synchronizing organizational efforts to protect against insider threats.

Additional resources

- https://www.dhs.gov/cisa/insider-threat-mitigation
- https://www.dhs.gov/sites/default/files/publications/fact-sheet-insider-threat-mitigation-program-092018-508.pdf
- https://www.dhs.gov/insider-threat-trailer-and-video
- https://www.dhs.gov/pathway-violence-video
- https://training.fema.gov/is/courseoverview.aspx?code=IS-915

Election Security

Election security is national security. Similar to security of any other system, it is a continuously evolving process that requires constant vigilance, innovation, and adaptation. The systems that comprise our Nation’s election infrastructure are diverse and complex, as are the measures taken to defend them.

The Cybersecurity and Infrastructure Security Agency (CISA) leads the effort with state and local officials to increase the resilience of the election infrastructure.

CISA is currently working with all 50 states, nearly 2000 local jurisdictions, both major political parties and more than a dozen presidential campaigns to broaden the reach and depth of information sharing and assistance.

What you can do

- Preach – get out to your communities to raise awareness on security practices, and advocate for broader participation in election security and national security efforts at all levels.
- Plan – know what you are going to do in the run up to an election; where you are voting, what the registration laws are in your state, how provisional ballots work, and what you need to do and have in place before, on, and after election day.
- Participate – whatever you do, participate in the process whether that is by voting, volunteering, or contributing additional resources. If you are part of the security community, let's push back against the bad guys.

Resources

- https://www.dhs.gov/publication/foreign-interference
- https://www.cisa.gov/cisa/election-security
- https://www.usa.gov/election-day

How to Engage: Private Sector

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 https://www.dhs.gov/cisa/hometown-security for free tools and resources for small and medium-sized businesses related to security and resilience
- ✓ Meet with your local Protective Security Advisor (PSA), 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 CIOCC.Physical@cisa.dhs.gov)
- ✓ Learn about resources available for vulnerability assessments and continuity plans, including https://www.cisa.gov/infrastructure-security and www.ready.gov/business
- ✓ Learn about the legal protections for information shared with CISA under the Protected Critical Infrastructure Information (PCII) Program https://www.dhs.gov/cisa/pcii-program
- ✓ Integrate cybersecurity into facility and operational protective measures
- ✓ Report suspicious activity to local law enforcement
- ✓ Write an op-ed in the local paper about the importance of critical infrastructure
- ✓ Reach out to public safety officials to discuss security and resilience enhancements
- ✓ Add your voice to social media conversations by using the hashtag **#infrastructure** and **#InfrastructureResilience**

How to Engage: Public Sector

Federal Departments and Agencies

- ✓ Include messaging about the importance of infrastructure in newsletters, mailings, and websites
- ✓ Promote interagency and multi-level collaboration on critical infrastructure issues
- ✓ Educate your employees about critical infrastructure issues and how they relate to your mission and to the security environment of your office
- ✓ Encourage clients, stakeholders, and SLTT counterparts to learn about critical infrastructure, dependencies, and the importance of a whole-of-community effort for security and resilience
- ✓ Use shared, consistent messaging throughout the month by visiting www.cisa.gov.

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
- ✓ Discuss the evolution of focus on critical infrastructure—from protection, to security and resilience—and dependencies requiring innovation and investment to strengthen the Nation
- ✓ Include a message about the importance 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 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
- ✓ 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 particular audience, whether it 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 www.digitalgov.gov for more information on accessibility.
- ✓ *Engage Your Audience* – Create activities that engage your community and promote interaction.

FREQUENTLY ASKED QUESTIONS

About Infrastructure Security Month…

What is Infrastructure Security Month?

Infrastructure Security Month is an annual effort to educate and engage the private sector, all levels of government, and the American public about the vital role critical infrastructure plays to our Nation's well-being and why it is important to strengthen critical infrastructure security and resilience.

As part of the Infrastructure Security Month, CISA is encouraging partners to increase resilience through preparedness and exercises, and promote smart, secure investment in national infrastructure. Each week, a different theme will be highlighted through a month-long social media campaign.

CISA also has a webpage dedicated to Infrastructure Security Month.

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, whether physical or 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; 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 are increasingly dependent upon critical infrastructure that is at risk from a variety of hazards and threats, both natural and man-made, including aging or failing infrastructure, extreme weather, cyberattacks, or evolving terrorism threats that impact our economy and communities. Critical infrastructure security and resilience requires a clear understanding of the risks we face and a whole-of-community effort that involves partnership between public, private, and nonprofit sectors.

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 that benefit from the critical infrastructure around us. Efforts also include the venues where people gather, such as houses of worship, schools, public festivals. 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, 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 vast 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?

The nation's critical infrastructure faces an increasing range of threats, such as extreme weather, aging infrastructure, cyber threats, or acts of terrorism. The evolving nature of the threat to critical infrastructure—as well as the maturation of our work and partnership with the private sector—has necessitated a shift from a focus on asset protection to an overarching system that builds resilience from all threats and hazards.

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. In particular, 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. The Department of Homeland Security is committed to leading the national effort to make infrastructure secure and resilient in the face of all hazards, including cyber vulnerabilities. Through Critical Infrastructure Security and Resilience Month, CISA is promoting a shared awareness and understanding across the critical infrastructure community of the diverse hazards affecting resilience and ensuring CISA partners have access to the resources and tools needed to inform decision making to address cyber-related challenges.

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

TEMPLATES

Press Release Template

If you choose to use this template, you much 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), 2019
Contact: (Contact Name), (Phone/Email)

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

CITY, STATE – November is Critical Infrastructure Security and Resilience 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 different themes related to critical infrastructure security and resilience, including:

- ✓ Securing the American Democracy: Election security 2020
- ✓ Our interconnected world: Cyber-physical convergence
- ✓ Protecting our hometowns: Soft target security
- ✓ Secure from the inside out: Combatting insider threats

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 requires 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 www.cisa.gov.

(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 much 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.

Keeping Infrastructure Strong and Secure

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.]

During November, we focus on engaging and educating public and private sector partners to raise awareness about the systems and resources that support our daily lives, underpin our society, and sustain our way of life. Safeguarding both the physical and cyber aspects of critical infrastructure is a national priority that requires public-private partnerships at all levels of government and industry.

We know critical infrastructure as the power we use in our homes and businesses, the water we drink, the transportation systems that get us from place to place, the first responders and hospitals in our communities, the farms that grow and raise our food, the stores we shop in, and the Internet and communication systems we rely on to stay in touch with friends and family. It also includes places where people gather, like houses of worship, entertainment venues, schools, and festivals. The security and resilience of this critical infrastructure is vital not only to public confidence, but also to the Nation's safety, prosperity, and well-being.

Managing risks to critical infrastructure involves preparing for all hazards, reinforcing the resilience of our assets and networks, and staying ever-vigilant and informed.

This November, help promote infrastructure security and resilience by training and exercising your employees on various threats, taking part in the Hometown Security effort, engaging with your community partners or supporting long term investments in critical infrastructure. We all need to play a role in keeping infrastructure strong, secure, and resilient. We can do our part at home, at work, and in our community by being vigilant, incorporating basic 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 www.cisa.gov.

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: "The message contained in this newsletter/blog was authored by CISA."

PROCLAMATION

Critical Infrastructure Security and Resilience Month, November 2018

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

WHEREAS, the Nation's critical infrastructure spurs our economy and supports our well-being, 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 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 www.cisa.gov. THEREFORE, BE IT RESOLVED that the [**GOVERNING BODY]** hereby proclaims November 2019 as Critical Infrastructure Security and Resilience Month and encourages communities to support the national effort to strengthen critical infrastructure security by engaging in partnerships together toward creating a more resilient society.

DATED this _____ Day of _____ 2019 by the [**GOVERNING BODY]**

_____

NAME, TITLE

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

SOCIAL MEDIA AND ONLINE RESOURCES

Social Media

DHS will use social media to share news and updates about Critical Infrastructure Security and Resilience month. Feel free to follow us on @CISAHarrell and @CISAgov and retweet our messages about Critical Infrastructure Security Resilience month, and be sure to check our page for updates at www.cisa.gov.

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 Video: http://www.youtube.com/watch?v=FqzJOBgSJs4
- ✓ "**Protected Critical Infrastructure Information (PCII) Program**" 3:22 Video: http://www.youtube.com/watch?v=-ucPhM2ecQ0
- ✓ "**Options for Consideration**" demonstrates possible actions to take if confronted with an active shooter scenario" 7:52 Video: https://www.youtube.com/watch?v=pY-CSX4NPtg
- ✓ "**Vehicle Ramming Attack Mitigation**" provides insightful analysis and recommendations aimed at protecting organizations and individuals against a potential vehicle ramming incident https://www.youtube.com/watch?v=Yw-fY86WhRg&list=PLyTgR4PDHXBnnl7dd-MyGV3oqq6GalOIb&index=3&t=0s
- ✓ "**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 https://www.youtube.com/watch?v=5GLNKHJCSkg&index=4&list=PLyTgR4PDHXBnnl7dd-MyGV3oqq6GalOIb&t=0s
- ✓ "**UAS and Critical Infrastructure"** contains information on critical infrastructure security challenges associated with the UAS threat, Counter UAS security practices, actions to consider for risk mitigation, and provides messages of facility and organizational preparedness related to UAS incidents https://www.youtube.com/watch?v=o6x-cj1wXZk&index=5&list=PLyTgR4PDHXBnnl7dd-MyGV3oqq6GalOIb&t=0s
- ✓ **"Pathway to Violence"** discusses behavioral indicators that assailants often demonstrate before a violent act. https://www.youtube.com/watch?v=GjK1U6VpfJE&list=PLyTgR4PDHXBnnl7dd-MyGV3oqq6GalOIb&index=6&t=0s
- ✓ **"Active Shooter Emergency Action Plan"** video guides viewers through important considerations of EAP development utilizing the first-hand perspectives of active shooter survivors, first responder personnel, and other subject matter experts who share their unique insight

https://www.youtube.com/watch?v=8Pjlr2rrEZc&list=PLyTgR4PDHXBnnl7dd-MyGV3oqq6GalOIb&index=7&t=0s

For more information about Infrastructure Security Month, please visit www.cisa.gov.