Critical Infrastructure Security and Resilience Month 2016 Toolkit

November 2016

Homeland Security

Table of Contents

CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE MONTH

The Nation's critical infrastructure provides essential services that underpin American society and sustain the American way of life. 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. 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.

November is Critical Infrastructure Security and Resilience Month, an opportunity to highlight the efforts between Federal, State, local, territorial, and tribal (SLTT) governments and private sector partners to protect and secure our Nation's critical infrastructure and enhance infrastructure resilience.

Critical Infrastructure Security and Resilience Month reinforces the importance of critical infrastructure to America's homeland security and economic prosperity and reiterates the Department of Homeland Security's (DHS) commitment to keep our critical infrastructure, and the communities that depend on them, safe and secure. This requires a nationwide effort, with public and private partners working together toward a common goal.

In 2015 and 2016, the public and private sectors collaborated on updating specific plans to address the unique capabilities, characteristics, and risk profiles of the critical infrastructure sectors. The Sector-Specific Plans, which supplement the National Infrastructure Protection Plan, set the strategic direction for voluntary, collaborative efforts to reduce risk and build resilience.

Critical Infrastructure Security and Resilience Month activities will focus on several key themes each week throughout the month to enhance security and resilience:

- Highlighting interdependencies between cyber and physical infrastructure;
- Pointing small and medium-sized businesses to the free tools and resources available to them to increase their security and resilience through Hometown Security and the four steps of Connect, Plan, Train, and Report (www.dhs.gov/hometown-security);
- Promoting public-private partnerships; and
- Fostering innovation and investments in infrastructure resilience.

This toolkit includes suggested activities that SLTT governments, businesses, nongovernmental organizations, and community organizations can take to participate in Critical Infrastructure Security and Resilience Month. It also includes templates and drafts of newsletter articles, blogs, and other collateral material for use in outreach efforts. As you familiarize yourself with the toolkit and prepare for outreach efforts, keep in mind the audiences and stakeholders that you plan to engage, and select the tools and messages that will help your organization communicate with them most effectively.

HOW TO PROMOTE CRITICAL 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.

We need your help to raise awareness of the importance of critical infrastructure and make Critical Infrastructure Security and Resilience Month a success. The month relies on everyone to reach out to many different audiences and inspire them to learn about the importance of 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.

How to engage: Private Sector

Owners and Operators

- ✓ Participate in a training or exercise to improve security and resilience
- ✓ 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 www.dhs.gov/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) to better understand infrastructure in your area (For more information on who the PSA is in your area, contact NICC@hq.dhs.gov)
- ✓ Learn about resources available for vulnerability assessments and continuity plans, including www.dhs.gov/critical-infrastructure and www.ready.gov/business
- ✓ 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**

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.dhs.gov/cisr-month and using **#infrastructure** on social media

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 DHS, 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 your local Protective Security Advisor to better understand infrastructure in your district or State

✓ 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

✓ 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 your local Protective Security Advisor to better understand infrastructure in your area

✓ 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.disability.gov and www.digitalgov.gov for more information on accessibility.
- ✓ *Engage Your Audience* – Create activities that engage your community and promote interaction.

FREQUENTLY ASKED QUESTIONS

About Critical Infrastructure Security and Resilience Month…

What is Critical Infrastructure Security and Resilience Month?

Critical Infrastructure Security and Resilience 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 2016 Critical Infrastructure Security and Resilience Month, DHS highlights interdependencies between cyber and physical infrastructure; points small and medium-sized businesses to the free tools and resources available to them to increase their security and resilience through Hometown Security and the four steps of Connect, Plan, Train, and Report (www.dhs.gov/hometown-security); promotes public-private partnerships; and fosters innovation and investments in infrastructure resilience.

DHS also has a webpage dedicated to Critical Infrastructure Security and Resilience 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, such as 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. 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 everyday. 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?

Threats to the Nation's critical infrastructure include extreme weather, aging infrastructure, cyber threats, and 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.

Are there challenges facing critical infrastructure today as a result of cyber interdependencies?

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, DHS is promoting a shared awareness and understanding across the critical infrastructure community of the diverse hazards affecting resilience and ensuring DHS partners have access to the resources and tools needed to inform decision making to address cyber-related challenges.

Visit www.dhs.gov/cybersecurity for tools and tips on cybersecurity.

TEMPLATES

Press Release Template

PRESS RELEASE

(Date – Month, Day), 2016
Contact: (Contact Name), (Phone/Email)

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

CITY, STATE – November is Critical Infrastructure Security and Resilience Month. (ORGANIZATION) has committed to participate in Critical Infrastructure Security and Resilience Month to focus on the importance of our Nation's critical infrastructure 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)

This November, Critical Infrastructure Security and Resilience Month will highlight four different themes related to critical infrastructure security and resilience.

> Week 1: Our connected infrastructure: Cyber and physical interdependence
> Week 2: Hometown Security – "Connect, Plan, Train, Report."
> Week 3: Partnering with the public and private sectors to build resilience
> Week 4: Fostering innovation and investment in resilient infrastructure

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 Critical Infrastructure Security and Resilience Month, visit
[INSERT ORGANIZATION WEBPAGE IF APPLICABLE] or www.dhs.gov/cisr-month

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

Newsletter/Blog Post Template

Please consider highlighting Critical Infrastructure Security and Resilience Month in your organization by including a brief article in your newsletter or a post on your blog if you have one. To help get you started, here is an example of what you might want to include.

Keeping Infrastructure Strong and Secure

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

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

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. 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 and reinforces the resilience of our assets and networks, and staying ever-vigilant and informed.

This November, help promote Critical Infrastructure Security and Resilience Month by training your employees on cyber awareness, 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.dhs.gov/cisr-month

SLTT Proclamation Template

PROCLAMATION

Critical Infrastructure Security and Resilience Month, November 2016

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.dhs.gov/critical-infrastructure

THEREFORE, BE IT RESOLVED that the **[GOVERNING BODY]** hereby proclaims November 2016 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 _____ 2015 by the **[GOVERNING BODY]**

_____

NAME, TITLE

SOCIAL MEDIA AND ONLINE RESOURCES

The following content highlights how DHS and its partner organizations can use established social media channels to share news and updates about Critical Infrastructure Security and Resilience month. This messaging also helps direct and encourage others to take action by providing short, concise social media messaging content.

Sample Twitter Posts

Use the Critical Infrastructure Security and Resilience Month hashtag: **#infrastructure**

- ✓ Welcome to Critical Infrastructure Security and Resilience Month! www.dhs.gov/cisr-month
- ✓ Help your community or workplace be more resilient. Visit www.dhs.gov/cisr-month to learn how! #infrastructure
- ✓ Does your business plan for infrastructure related disruptions? Find out more at www.dhs.gov/cisr-month #infrastructure
- ✓ Talk to coworkers and clients to encourage them to learn more about the importance of critical #infrastructure
- ✓ Calling all infrastructure owners and operators! Have you updated business continuity plans? #infrastructure
- ✓ What is #infrastructure? www.dhs.gov/what-critical-infrastructure#DHS #CISRMonth
- ✓ America's critical infrastructure relies on YOU to help out. Find out how you can make a difference www.dhs.gov/cisr-month #infrastructure
- ✓ America is only as strong as her #infrastructure [insert image showing critical infrastructure that you use daily] #CISRMonth
- ✓ Keeping America secure. Keeping America resilient. Learn more about #CISRMonth www.dhs.gov/cisr-month #infrastructure

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

For more information about Critical Infrastructure Security and Resilience Month, please visit www.dhs.gov/cisr-month or email infrastructure@hq.dhs.gov.