# INFRASTRUCTURE SECURITY MONTH 2020

cisa.gov

# CONTENTS

# INTRODUCTION

## Welcome to Infrastructure Security Month 2020

Each November we recognize Infrastructure Security Month. This year's theme is *Critical Infrastructure in a Time of Transformation*, in recognition of the rapid shifts in technology as we adapt to the COVID-19 environment. We will highlight information technology and healthcare systems, which have changed rapidly over the past seven months due to the COVID-19 response. We will also focus on the seismic shift to remote work and school, as well as critical infrastructure resilience in the face of natural disasters and insider threats.

### Security and Response During a Time of Transformation

In 2020, the global pandemic has focused our attention on key infrastructure such as communications and healthcare and has highlighted the importance of essential critical infrastructure workers. As the Nation has undergone a transformative mass move to remote work, distance learning, and telemedicine, the importance of cybersecurity has never been more apparent.

### The Future of Securing Critical Infrastructure

The Nation's critical infrastructure faces an increasing range of threats, from extreme weather to 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 caused us to shift our focus from asset protection to that of building resilience from all threats and hazards. As the Nation grapples with critical infrastructure impacts today, we must continue to plan for the resilient infrastructure of tomorrow.

### Key Messages

The year 2020 has presented our Nation with unprecedented challenges, including a global pandemic and historic natural disasters, compounded by the Presidential election cycle. These factors have driven rapid, dramatic changes in how we work, learn, vote, and socialize. As a result, we are seeing shifts in how we use and rely on critical infrastructure. Information technology and healthcare systems are strained under the impacts of mass telework, distance learning, and COVID-19.

This year's crises have also highlighted the crucial role of our historically under-recognized essential critical infrastructure workers. The global pandemic has shone a spotlight on the importance of essential critical infrastructure workers, who have proved their determination in 2020. We must prioritize the safety of essential workers while supporting ongoing infrastructure operations across the Nation.

# HOW TO PROMOTE INFRASTRUCTURE SECURITY AND RESILIENCE AWARENESS

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 two sub-themes for Infrastructure Security Month 2020: Critical Infrastructure in a Time of Transformation. These sub-themes are Security and Response During a Global Pandemic and The Future of Securing Critical Infrastructure.

- 2020 has been a historic year for the Nation and its critical infrastructure as we grapple with a global pandemic, a U.S. Presidential election, and unprecedented natural disasters. These factors have driven a rapid and dramatic change in how the Nation works, learns, votes, and socializes.
- 2020 has been a year of transition in how we use and rely on critical infrastructure. Information technology and healthcare systems bear the brunt of the impacts from mass telework and distance learning, as well as the detection, prevention, and treatment of COVID-19.
- This year's crises have highlighted the crucial role of our historically under-appreciated essential critical infrastructure workers.
- Infrastructure Security Month 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 during this time of transition. These include:
    - 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 during this critical time, and we must coordinate and collaborate across every level of government, private sector, and community organization.
- During this year's Infrastructure Security Month, we ask every organization to:
    - Identify and prioritize the ability of essential workers to work safely while supporting ongoing infrastructure operations across the Nation
    - Bring awareness to misinformation, disinformation, and conspiracies appearing online related to COVID-19, 5G, election security, or other critical infrastructure, functions, or threats
    - Recognize the societal transformation of securing infrastructure and responding to disasters during a global pandemic
    - Understand the modernization of securing critical infrastructure as we defend today, secure tomorrow

## THE THREAT ENVIRONMENT

America's national security and economic prosperity are dependent upon critical infrastructure at risk from a wide range of hazards during this time of transition. Our way of life relies on a complex network of physical and cyber systems, all working together in harmony, to defend against critical infrastructure threats, both natural and man-made. Our infrastructure grows more interdependent with other systems and functions and is under special strain during the time of pandemic. We must look at our risks from both a cyber and a physical perspective.

- The Nation relies on information technology infrastructure for remote work and schooling on a scale not seen before 2020.
- The Nation also relies on its critical infrastructure workforce and must prioritize the ability of essential workers to work safely while supporting ongoing infrastructure operations across the Nation.
- Essential infrastructure (including healthcare, public safety, public transportation and other critical workforce) has been intensely impacted by the necessity of detecting, treating, and preventing COVID-19.
- The security of our election infrastructure has been under scrutiny during this Presidential election year occurring during an unprecedented pandemic.
    - The American people play a critical role in protecting our democracy by being prepared, participating, and patient voters.
    - As Election Day approaches and millions of Americans cast their ballots, a lot of information is out there about the security of your vote. CISA is ensuring voters have safeguards in place to help ensure a safe and secure election.
    - The #Protect2020 Rumor vs. Reality webpage, cisa.gov/rumorcontrol, is designed to help the American public answer questions about the security of their vote and address common misconceptions about election security.
    - CISA encourages everyone to use care when consuming information they receive or come across. Practicing media literacy—including verifying sources, seeking alternative viewpoints, and finding trusted sources of information—is the most effective strategy for limiting the effect of disinformation.
- Natural disasters, while always a threat to critical infrastructure, pose unique threats to physical and technological infrastructure, as we have seen in this year's fires, hurricanes, and other storms, such as the Iowa derecho.
- Internal threats remain a special concern to physical and cyber infrastructure.
- Foreign disinformation and misinformation related to COVID-19 and our elections is especially concerning during this pandemic and Presidential election year.
- The impacts from a disruption of these systems have wide ripple effects across the country, influencing emergency response, transportation, and the economy.
- Critical infrastructure security and resilience requires a clear understanding of the risks we face, as well as a whole-of-community effort that involves partnership between public, private, and non-profit sectors.
- Managing risks to critical infrastructure involves preparing for all hazards, reinforcing the resilience of our assets and networks, and remaining vigilant and informed.

### 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.

## COVID-19 AND CRITICAL INFRASTRUCTURE

- COVID-19 is different than any emergency the Nation has faced, especially considering the modern, tightly interconnected economy and American way of life. In traditional emergencies, government coordinates with the private sector to get businesses back to business.
- In this case, as the government works with partners to slow the spread of COVID-19 and reopen communities, the economic goal is maintaining resilience of the Nation's foundation—its critical infrastructure.
- In the modern economy, there are many types of employees required to sustain normal day-to-day services that enable our economy and our way of life. This goes far beyond utilities and public works.
- Government and industry have identified workers who are key to continuation of vital services and may require accommodations to work safely.
- To ensure resilient infrastructure operations and worker safety, CISA has provided guidance for critical infrastructure owners and jurisdictions. A key resource is CISA's Identifying Critical Infrastructure During COVID-19 webpage: cisa.gov/identifying-critical-infrastructure-during-covid-19.

### What You Can Do

- Identify tailored risk-mitigation strategies for specific workplace settings.
- Assess risks faced by workers and implement measures to increase worker wellbeing; increased protective measures should be implemented for high-risk workers.
- Engage with the essential worker community and develop a plan for allocation of potentially scarce resources should COVID-19 cases continue to rise or enter another wave. A plan will ensure that workers can continue to perform essential tasks supporting critical infrastructure.
- Ensure that workers who perform essential tasks and/or have consistent interactions with at-risk populations (e.g., the elderly or those with pre-existing conditions) can obtain the necessary resources to reduce the transmission of the virus.

## CYBER-PHYSICAL CONVERGENCE

- During the pandemic, Americans have relied more heavily on internet-enabled systems and functions to carry out everyday tasks like shopping, banking and finance, employment, education, socialization, and even voting. This has revealed vulnerabilities affecting multiple critical infrastructure sectors.

### 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.

## INSIDER THREATS

- Insider threats exist across public and private sector organizations. An insider may be a trusted current or former employee, a contractor or associate who causes harm, either wittingly or unwittingly, to a company or public sector.
- Insider threats include 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.
- 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.

### What You Can Do

- 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 information technology to address behaviors or incidents reported by employees or others.
- The ability to recognize and respond to physical and cyber-based threats increases an organization's capacity to protect its people, facility, and information. It can also enhance traditional security mechanisms that guard against threats from outside the organization.
- While some insider threats stem from malicious intent, others result from unintentional or careless behavior. Threats can manifest in a variety of ways, ranging from breaches of sensitive information to workplace violence to terrorism.
- Establishing an insider threat program is an important first step toward synchronizing organizational efforts to protect against insider threats. A key resource is CISA's Insider Threat Mitigation webpage: cisa.gov/insider-threat-mitigation.

## 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.
- CISA leads the effort with state and local officials to increase the resilience of the election infrastructure with tabletop exercises and technical assistance.
- CISA is currently working with all 56 states and territories, nearly 2,000 local jurisdictions, both major political parties and presidential campaigns to broaden the reach and depth of information sharing and assistance.
- CISA has prepared resources, infographics, and fact sheets to support state and local election officials and to encourage voters to be prepared, participating, and patient during this election year that will have more mail-in and absentee votes. Please visit CISA's election security webpage: cisa.gov/election-security-library.

### 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 leading 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—Get involved in the election process, whether this is by volunteering or contributing additional resources. If you are part of the security community, or a state or local election official, help in the effort to push back against threats to this critical infrastructure. For more information on how to get involved, please visit CISA's election security webpage: cisa.gov/election-security-library.
- Patience—Understand that results may be slower this election year than in past elections. Increased usage of mail-in and absentee ballots resulting from the public health emergency may lead to slower than usual results reporting in some states. Election officials perform due diligence and follow defined processes to verify election results.

### MISINFORMATION AND DISINFORMATION

- Misinformation and disinformation related to COVID-19, 5G, or election security are spread online and pose a threat to the security of critical infrastructure.
  - Misinformation is information that is false, but not created or shared with the intention of causing harm.
  - Disinformation is false information that is deliberately created to mislead, harm, or manipulate a person, social group, organization, or country.
- Disinformation creates division among the American people and is spread by both foreign and domestic bad actors.
- CISA works with multiple agencies and entities to combat misinformation and disinformation with toolkits, messaging, and emphasis on trusted sources.

#### What You Can Do

- Learn to recognize disinformation and misinformation when it is spread online and educate your community. Think before you share or link to a source.
- Rely on trusted sources of information. Turn to the Centers for Disease Control and Prevention and state/local health officials about COVID-19; rely on trusted elections sources such as state or local election boards. For more information, please visit cisa.gov/rumorcontrol.

### 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?

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 in our Nation's wellbeing and why it is important to strengthen critical infrastructure security and resilience.

As part of Infrastructure Security Month, CISA encourages partners to increase resilience through preparedness and exercises. Together, we can promote smart, secure investment in our national infrastructure.

During the month-long social media campaign, a different theme will be highlighted each week. More information can be found on CISA's Infrastructure Security Month webpage.

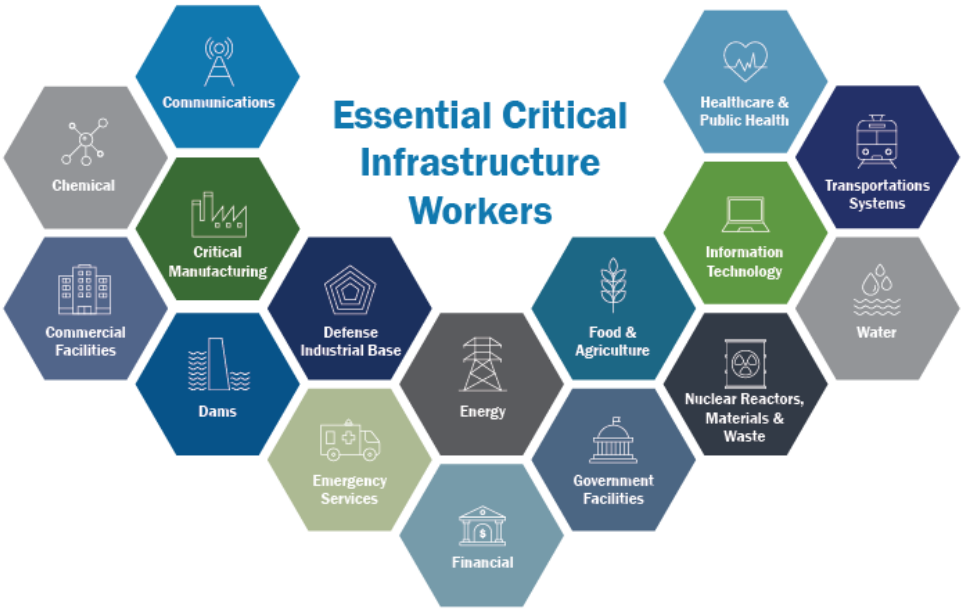
## About the Significance of Critical Infrastructure

### 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; 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. These hazards and threats include aging or failing infrastructure, extreme weather, cyberattacks, or evolving terrorism threats that 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.

## 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. This year, COVID-19, natural disasters, and the Presidential elections have converged, driving a rapid and dramatic change in how

we work, learn, vote, and socialize. Consequently, we are seeing shifts in how we use and rely on critical infrastructure. Information technology and healthcare systems bear the brunt of the impacts from mass telework and distance learning, as well as the detection, prevention, and treatment of COVID-19.

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?

The COVID-19 pandemic is distinct from any other national emergency, one made more critical by today's interconnected economy and way of life. In traditional emergencies, government coordinates with the private sector to get businesses back to business. During the COVID-19 emergency, government works with partners to slow the spread of the virus and reopen communities to safeguard our economy, thus maintaining resilience of our critical infrastructure.

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. 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 Infrastructure Security Month, CISA promotes shared awareness and understanding of the diverse hazards affecting critical infrastructure resilience. CISA invites partners to access resources and tools needed to address cyber-related challenges and inform decision-making.

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

# 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 cisa.gov/identifying-critical-infrastructure-during-covid-19 for guidance on the critical infrastructure during COVID-19.

- ✓ Visit cisa.gov/telework for guidance on telework.
- ✓ Visit cisa.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, 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 cisa.gov/infrastructure-security and ready.gov/business.
- ✓ Learn about the legal protections for information shared with CISA under the Protected Critical Infrastructure Information (PCII) Program at cisa.gov/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 Department 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 cisa.gov/ismonth.
- ✓ Visit cisa.gov/identifying-critical-infrastructure-during-covid-19 for guidance on the critical infrastructure during COVID-19.

### 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 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 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 cisa.gov/protect2020 for election security and disinformation/misinformation resources.
- ✓ Visit cisa.gov/covid-19-disinformation-toolkit for guidance on misinformation/disinformation during the pandemic.
- ✓ Visit cisa.gov/identifying-critical-infrastructure-during-covid-19 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 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), 2020
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 *"In a Time of Transformation,"* which includes the following sub-themes:

- ✓ Security and Response During a Global Pandemic
- ✓ The Future of Securing Critical 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 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.

*Security and Response During a Time of Transformation*

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 *Critical Infrastructure in a Time of Transformation*, in recognition of rapid shifts in how we are using technology as well as changes as we adapt to a COVID environment. We will highlight information technology and healthcare systems, which have changed rapidly over the past seven months due to the COVID-19 response. We will also focus on the seismic shift to remote work and school, as well as critical infrastructure resilience in the face of natural disasters and insider threats.

This global pandemic has focused attention on key infrastructure such as communications and healthcare and highlighted the important role of essential critical infrastructure workers. As the Nation has undergone a transformative mass move to remote work, distance learning, and telemedicine, the importance of strong cybersecurity has never been more apparent.

This year 2020 has made us all more aware of and vigilant for potential outsider threats. As a Nation, we now know how important it is to protect our critical infrastructure. It is the center of all aspects in our daily lives—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. Critical infrastructure 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 Country's safety, prosperity, and wellbeing.

This November join us in recognizing our Nation's infrastructure and celebrating those who work to keep it running. The global pandemic has focused attention on key infrastructure such as communications and healthcare and highlighted the important role of essential critical infrastructure workers.

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 2020

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 2020 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 _____ 2020 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 Infrastructure Security Month. Feel free to follow us on Twitter @CISAgov, like us at facebook.com/CISA, 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): www.youtube.com/watch?v=FqzJOBgSJs4
- ✓ **"Protected Critical Infrastructure Information (PCII) Program**" (3:22 duration): www.youtube.com/watch?v=-ucPhM2ecQ0
- ✓ **"Options for Consideration Active Shooter Training Video"** demonstrates possible actions to take if confronted with an active shooter scenario (7:52 duration): 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 (12:39 duration): www.youtube.com/watch?v=Yw-fY86WhRg&list=PLyTgR4PDHXBnnI7dd-MyGV3oqq6GaIOIb&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 (30:36 duration): www.youtube.com/watch?v=5GLNKHJCSkg&index=4&list=PLyTgR4PDHX BnnI7dd-MyGV3oqq6GaIOIb&t=0s
- ✓ **"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): www.youtube.com/watch?v=o6x-cj1wXZk
- ✓ **"Pathway to Violence"** discusses behavioral indicators that assailants often demonstrate before a violent act (11:07 duration): www.youtube.com/watch?v=GjK1U6VpfJE&list=PLyTgR4PDHXBnnI7dd-MyGV3oqq6GaIOIb&index=6&t=0s
- ✓ **"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) www.youtube.com/watch?v=8Pjlr2rrEZc