APRIL IS

EMERGENCY COMMUNICATIONS MONTH

RESILIENT TOGETHER

CONTENTS

WELCOME TO EMERGENCY COMMUNICATIONS MONTH 2024

This April, the Cybersecurity and Infrastructure Security Agency (CISA) recognizes its third annual Emergency Communications Month to honor emergency communications professionals and highlight the critical role that emergency communications plays in keeping us safe. Ensuring interoperable and resilient communications for public safety, critical infrastructure and continuity of government operations in times of crisis is a national security issue. This year's theme, **Resilient Together**, highlights both the importance of building resilient emergency communications and the need to work together.

Emergency communications is a complex ecosystem with multiple stakeholders and moving pieces. It is more resilient and secure through strong partnerships and collaboration between emergency responders, government, information technology and communications providers, non-governmental organizations, and even private citizens. All through April, CISA invites the nation to celebrate the people who operate the systems we rely on and learn more about the vital role of emergency communications.

Through its emergency communications mission, CISA leads the nation's operable and interoperable public safety and national security and emergency preparedness communications efforts. This mission has only grown in importance as more of the critical services Americans rely on every hour of every day have moved online and new challenges are posed by technologies like Artificial Intelligence (AI). Fortunately, CISA provides tools, training, and resources to support our government and industry partners to help build and strengthen emergency communications capabilities.

THIS APRIL, TAKE ACTION WITH CISA TO REMAIN RESILENT TOGETHER IN SUPPORT OF OUR EMERGENCY COMMUNICATIONS COMMUNITY.

RESOLVE TO BE RESILIENT TOGETHER

At CISA we take pride in the invaluable partnerships we build every day across the nation. We understand through our strong relationships that we are more resilient together when faced with challenges. Being resilient together is how we as a nation, can recover quickly in the event of a cyberattack or national emergency.

Everyone plays a role in our nation’s security and resilience, and we can accomplish great things together through strong partnerships and collaboration between emergency responders, government, information technology and communications providers, non-governmental organizations, and even private citizens. In honor of Emergency Communications Month, this toolkit highlights strategic ways our partners at all levels within the federal, state, local, tribal and territorial (FSLTT) space can position themselves to remain resilient in the current threat environment.

THE CURRENT THREAT ENVIRONMENT

Cyber adversaries are actively targeting government entities and public safety organizations. For example, cyber disruptions to 911 call capabilities can impair a key conduit for the public to request assistance. Similarly, radio frequency jamming at an incident site may endanger first responders and hinder lifesaving operations.

Defending public safety and emergency communications systems from cyber threats is critical. Cybersecurity is a shared mission across all levels of government, the private sector, nongovernmental organizations, and the public. Public safety leaders recognize the need to modernize and customize cybersecurity solutions to meet emerging threats. It is critical that we work together to protect public safety personnel and the technology that supports them (learn more at CISA’s Public Safety Cybersecurity website).

WHAT CISA IS DOING TO SUPPORT EMERGENCY COMMUNICATIONS

OUR RESOLVE

CISA counters the evolving threats to emergency communications by focusing its initiatives in three priority areas:

- **Promote Emergency Communications Interoperability**: Promoting operability, resilience, and interoperability by providing the tools and resources, such as interoperability markers for stakeholders, developed in coordination with SAFECOM, to support the next generation environment and cyber ecosystem.
- **Expand Integrated, collaborative communications planning**: Bolstering and building teams and communities of practice with public safety stakeholders and communicators across all parts of the FSLTT and critical infrastructure sectors.
- **Increase Priority services adoption**: Partnering with industry to make priority voice, data, video, and information services available to and used day-to-day by qualified organizations that protect our nation and our communities.

EFFORTS TO SECURE EMERGENCY COMMUNICATIONS

- ***Integrating Land Mobile Radio (LMR) and Broadband Communications:*** LMR remains an essential part of emergency communications, but the benefits and opportunities broadband offers to public safety are undeniable. Citizens will be able to send a picture of a suspicious package or videos of an event as it is happening to emergency communications centers (ECCs)/public safety answering points (PSAPs) that can then share those files with first responders. This capability provides critical information in determining how to respond and what resources will be needed. LMR will continue to be the primary method of communication for first responders as broadband continues to pursue mission critical voice for public safety. Broadband is and will continue to greatly improve interoperable communications across the country.

- ***Transition to Next Generation-911 (NG911):*** Across the nation, ECCs and PSAPs are transitioning from analog 911 system to digital or Internet Protocol (IP)-based systems, known as NG911, to benefit from new capabilities and infrastructure, creating faster and more resilient communications systems. NG911 will strengthen and improve the ability to manage and share information and call load across jurisdictions. It will also allow the exchange of multimedia (e.g., photos, videos) between the public and ECCs/PSAPs. It will enable first responders, emergency management, and other public safety entities to provide optimal service not only to their own communities, but also to neighboring communities in need of additional resources or assistance.

- ***Cybersecurity in Emergency Communications for both Awareness and Prevention:*** The technologies that have made the nation's emergency communication more efficient have also exposed it to the risks and vulnerabilities inherent in information technology and operational technology. As emergency communications transition from voice-only to include DV&IS, emergency communicators must defend against attacks from adversaries seeking to interfere and/or profit. CISA works with emergency communications partners to improve preparedness capabilities to counter threats, mitigate critical vulnerabilities, and manage incidents as well as help organizations build resilience, design technology securely, and manage risk before incidents occur.

- *CISA works to:*
    - Adapt governance models to incorporate cybersecurity planning and intrusion prevention.
    - Customize cyber-focused Technical Assistance for Emergency Communications Centers (ECCs)/Public Safety Answering Points (PSAPs)/ 9-1-1 Systems / LMR functions to mitigate ransomware/telephony denial of service (TDoS) attacks on public safety networks, and systems that affect 9-1-1 and emergency communications.
    - Encourage dedicated research and development for emergency communications.
    - Shape Information Security initiatives (secure mobile, etc.) that include Advanced Encryption Standards (AES) for federal voice networks and larger CISA-hosted grant programs for cybersecurity of both digital voice and data capabilities.
    - Refine interoperability and cyber resilient NG911 risk profiles.
    - Collaborate with stakeholders and partners to enhance the National Incident Management System (NIMS) Incident Command System (ICS) Information and Communications Technology (ICT) position specific training to ensure effective, resilient, and secure incident communications.

WHAT YOU CAN DO TO BOLSTER YOUR EMERGENCY COMMUNICATIONS

No matter what line of work we are engaged in or where we live, nearly everything we do relies on the resiliency of our critical infrastructure and the reliability of our technology. This April, CISA is focusing on how our stakeholders can integrate the next generation of emergency communications systems and what measures they can take to prevent cyberattacks and bolster their resiliency.

As a call to action, we invite you to join us in becoming, remaining and encouraging others to be RESILENT TOGETHER. Below are some quick actions you can take to help make critical infrastructure and emergency communications more resilient in your agency or capacity. Visit CISA.gov to learn more.

Recommended Actions for 911 Professionals and Practitioners

- ✓ Identify a lead to coordinate Next Generation 911 (NG911) transition efforts and liaison with state, local, territorial and tribal (SLTT) partners, such as the Statewide Interoperability Coordinator (SWIC), on modernization efforts.
- ✓ Establish a comprehensive list of emergency communications centers (ECCs) within the agency and recommend ECC leadership use the SAFECOM and National Council of Statewide Interoperability Coordinators (NCSWIC) NG911 Self-Assessment Tool to determine current maturity state.
- ✓ Develop or update governance, standard operating procedures, Continuity of Operations (COOP), and incident response plans.
- ✓ Use change management best practices throughout NG911 transition.
- ✓ Discuss funding mechanisms to support the NG911 transition project, staffing, and training needs.
- ✓ Review the Considerations for Establishing Agreements for NG911 document for helpful tips for NG911 transition.
- ✓ Review public safety telecommunicator job descriptions to ensure they accurately reflect the evolving roles and responsibilities of a NG911 workforce.
- ✓ Prioritize cybersecurity of 911 and NG911 systems.

Recommended Actions for the Private Sector

- ✓ Improve security through a series of steps, including:
  - *Assess Your Risk.* Organizations must identify your most critical functions and assets, define dependencies that enable the continuity of these functions, and consider the full range of threats that could undermine functional continuity.
  - *Make a Plan and Exercise It.* Organizations should perform dedicated resilience planning, determine the maximum downtime acceptable for customers, develop recovery plans to regain functional capabilities within the maximum downtime, and test those plans under real-life conditions.
  - *Continuously Improve and Adapt.* Organizations must be prepared to regularly adapt to changing conditions and threats. This starts with fostering a culture of continuous improvement, based on lessons learned from exercises and real-world incidents and evolving

[1] The National 911 Program's *Public Safety Telecommunicator Reclassification Toolkit* includes resources to assist ECCs with developing public safety telecommunicator job descriptions, establishing or expanding public safety telecommunicator training programs, and developing a communications plan.

cross-sector risks.

- ✓ Add your voice to social media conversations by using the hashtag #ResilientTogether to emergency communications issues and how they relate to your mission and to the security environment of your office.
- ✓ Encourage clients, stakeholders, and state, local, tribal, and territorial government counterparts to learn about critical infrastructure, dependencies, and the importance of a whole-of-community effort throughout the month by visiting cisa.gov/ECM.
- ✓ Integrate cybersecurity into facility and operational protective measures.
- ✓ Build resilience into facility design and operations.

Recommended Actions for Sector Risk Management Agencies

- ✓ Educate members of your sector about critical infrastructure issues and how they relate to the sector's security environment and business operations during this time of transition.
- ✓ Discuss the evolution of focus on critical infrastructure—from protection to security and resilience— and dependencies requiring innovation and investment of infrastructure in newsletters, mailings and websites.
- ✓ Highlight your partnership with CISA, other federal agencies and the national critical infrastructure community to make these vital assets and systems secure and resilient.
- ✓ Host a virtual town hall to discuss local critical infrastructure issues.
- ✓ Promote training and exercise opportunities to owners, operators and internal staff.

Recommended Actions for State, Local, Tribal, and Territorial Government Officials

- ✓ Conduct or participate in a training or exercise to improve security and resilience.
- ✓ Develop or update your **Statewide Communications Interoperability Plans (SCIP)**. Aligned to the NECP, SCIPs define the strategic direction for interoperable and emergency communications within a state or territory.
- ✓ Develop a **Tactical Interoperability Communications Plan (TICP)** to document incident communications capabilities, and governance criteria for resource deployment and usage. TICPs can be developed for states, territories, tribes, regional bodies, or critical infrastructure.
- ✓ Develop an **Incident Communications Resource Plans (ICRP)** to identify needs and geographic location guidance for Information and Communications Technology (ICT) Branch tactical resources. The ICRPs include the resource qualification requirements, support and maintenance needs, and the long-term succession planning.
- ✓ Utilize CISA's **National Interoperability Field Operations Guide (NIFOG)**, which is a technical reference for emergency communications planning and for radio technicians responsible for radios that will be used in disaster response: Field Operations Guides (FOGs) | CISA.
- ✓ Leverage CISA's **Primary, Alternate, Contingency, Emergency (PACE)** communications plans to prepare backup communications capabilities in out-of-the-ordinary situations. PACE planning helps organizations establish options for redundant communications capabilities if primary capabilities are disrupted or degraded: NCSWIC PTE Committee Releases Leveraging the PACE Plan into the Emergency Communications Ecosystem | CISA.
- ✓ See if you qualify for the FY23 State and Local Cybersecurity Grant Program: State and Local Cybersecurity Grant Program | CISA.
- ✓ Connect public safety officials with private sector businesses.

- ✓ Meet with local business owners to discuss dependencies on critical infrastructure and distribute relevant materials.
- ✓ Include a message about the importance of infrastructure security and resilience in newsletters, mailings and websites.
- ✓ Meet with CISA representatives in your state or district to better understand your local infrastructure and the risks it faces: Emergency Communications Coordination Program | CISA.
- ✓ Host a town hall meeting to discuss local critical infrastructure issues.
- ✓ Write an opinion editorial in the local paper about the importance of critical infrastructure security and resilience.

Recommended Actions for Members of Congress

- ✓ Meet with CISA representatives in your state or district to better understand your local infrastructure and the risks it faces.
- ✓ Promote training and exercise opportunities to owners and operators.
- ✓ Engage state and local officials on current initiatives to improve security and resilience.
- ✓ Meet with local business owners to discuss dependencies and interdependencies of critical infrastructure.
- ✓ Include a message about the importance of infrastructure security and resilience in newsletters, mailings and websites.
- ✓ Write an opinion editorial in your local paper about the importance of critical infrastructure.

Communication Tips

In addition, partners can reference the tips below for engaging with various audiences:

- ✓ *Understand Your Audience*—Identify which groups of people you are trying to reach. Knowing who is receiving your message is important to what you say and do.
- ✓ *Know the Specific Risks in Your Area*—By tailoring messages to the specific risks in your area, you can make your outreach more effective and help your community prepare for the most likely events.
- ✓ *Make It Meaningful*—Tailor your message to each audience, whether this is owners or operators, individuals or families, employees, professionals in specific fields (such as education or medicine), young people, or those with special access and functional needs.
- ✓ *Make It Accessible*—Create messages and tools that are accessible to all audiences. Visit Digital.gov – Guidance on building better digital services in government for more information on accessibility.
- ✓ *Engage Your Audience*—Create activities that engage your community and promote interaction.

RESOURCES

CISA provides several resources that support security capacity building efforts, including those focused on priority telecommunications services, technical assistance, grant support and public safety cybersecurity. CISA also conducts exercises to help stakeholders assess their plans and can provide free site visits to assess current security posture and identify any vulnerabilities and areas for improvement. Below is a list of key CISA resources to support agencies with becoming and remaining resilient in their emergency communications:

Priority Telecommunications Services

- CISA's Emergency Communications Division provides Priority Telecommunications Services (PTS) to authorized users giving them access to the Government Emergency Telecommunications Service (GETS), Wireless Priority Services (WPS), and Telecommunications Service Priority (TSP).
- GETS, WPS, and TSP enable personnel working in organizations responsible for Critical Infrastructure to communicate when networks are degraded or congested:
  - **GETS** is an emergency telephone service that provides subscribers with priority access and prioritized processing in the local and long-distance segments of landline telephone networks. GETS is intended to be used in an emergency or crisis situation when the network is congested and the probability of completing a normal call is reduced.
  - **WPS** is a cellular communications service that provides authorized devices with priority calling on all nationwide regional networks.
  - **TSP** authorizes national security and emergency preparedness (NS/EP) organizations, as well as the 16 critical infrastructure sectors, to receive priority treatment for vital voice and data circuits provisioning and restoration requests by the service providers.
  - Learn more about these services at Priority Services | CISA.
- Personnel who span all organizational levels, from executive leadership positions to ground-level operations are encouraged to enroll in PTS. Examples include subject matter experts, functional managers, field operators, Chief Executive Officers, Public Information Officers, etc.
- Information for enrolling in the Priority Services can be found here: How to Enroll in Priority Telecommunications | CISA.
- **Regional PTS Area Representatives (PARS)** are field representatives based in the regions and are available to provide enrollment support. Contact information can be found here: Priority Telecommunications Services Area Representatives (PARS) Contact Information | CISA
- **Priority Telecommunications Service Center -** The Priority Telecommunications Service Center (Service Center) is comprised of a team of dedicated specialists who assist organizations with the enrollment process for Government Emergency Telecommunications Service (GETS), Wireless Priority Service (WPS), and Telecommunications Service Priority (TSP). In addition, the Service Center assists with all other aspects of managing an organization's Priority Services accounts. The Service Center is the first resource for assistance with Priority Services. The Service Center team is available Monday-Friday, from 8:00 AM ET until 6:00 PM ET, at 866-627-2255 or email support@gwids.cisa.gov.

CISA Technical Assistance

- **Technical Assistance** — CISA provides direct technical assistance and training to support 911. The service offerings, including NG911 strategic planning support and 911 cyber assessments, can be found in the CISA Technical Assistance Service Offerings Guide
- **Field Operations Guides (FOGs)** – CISA provides technical references for emergency communications planning and for radio technicians responsible for radios that will be used in emergency responses. Field Operations Guides (FOGs) | CISA

Grant Support

Interoperable communications programs encompass a wide range of activities—purchasing new equipment, hosting state meetings, and conducting training—that require significant funding. ECD supports the coordination of grant guidance across the federal government through development of the SAFECOM Grant Guidance on Emergency Communications Grants and support of the Emergency Communications Preparedness Center Grants Focus Group. ECD serves as the program office for the Border Interoperability Demonstration Project.

- SAFECOM Grant Guidance on Emergency Communications Grants
- Rural Emergency Medical Communications Demonstration Project (REMCDP)

Emergency Communications Planning

- **The National Emergency Communications Plan (NECP)** is the nation's strategic plan to strengthen and enhance emergency communications capabilities. The NECP navigates the complex mission of maintaining and improving emergency communications capabilities for emergency responders and serves as the nation's roadmap for ensuring emergency communications interoperability at all levels of government. The NECP establishes a shared vision for emergency communications and assists those who plan for, coordinate, invest in, and use operable and interoperable communications for response and recovery operations. This includes traditional emergency responder disciplines and other partners from the whole community that share information during incidents and planned events. National Emergency Communications Plan | CISA

Public Safety Resources

- Public Safety Cybersecurity | CISA - This page compiles resources, including the Public Safety Communications and Cyber Resiliency Toolkit, developed by CISA for public safety communications practitioners, as well as anyone looking to gain further knowledge about cybersecurity for public safety communications. This page provides resources to public safety practitioners regarding common questions related to public safety cybersecurity.
- 911 Cybersecurity Resource Hub | CISA – This one-stop shop compiles cybersecurity resources to make it easy for Emergency Communications Centers to report a cyber incident, find real-world case studies, access cybersecurity education and training opportunities, and learn about best practices to identify and protect networks from cyberattacks. CISA, SAFECOM, and NCSWIC worked collaboratively with state and local public safety and emergency communications stakeholders to develop this interactive website.
- **SAFECOM/NCSWIC** – Through collaboration with emergency responders and policy makers across all levels of government, SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC) work to improve multi-jurisdictional and intergovernmental communications interoperability. SAFECOM and NCSWIC work with existing Federal communications programs and key emergency response stakeholders to develop better technologies and processes for the multi-jurisdictional and cross-disciplinary coordination of existing communications systems and future networks. Resources | CISA
- Emergency Communications and Extreme Weather Factsheet – This resource aims to familiarize practitioners with the impacts of extreme weather on emergency communications. Emergency communications practitioners may not have previous response or mitigation expertise as a result. Some weather events may also produce multiple kinds of extreme conditions, resulting in compounding and concurrent communications concerns.
- Transition to Next Generation 911 (NG911) | CISA - CISA, in conjunction with the SAFECOM-NCSWIC Next Generation 911 (NG911) Working Group, uses stakeholder feedback from multiple levels of government to identify, document, and develop informational products and refine innovative concepts that will facilitate the transition to NG911. This page provides resources and tools to support 911 system operations, security, and NG911 transition.

- Encryption | CISA - Encryption ensures effective security where information cannot be intercepted and used to hinder emergency response or endanger responders and the public. The public safety community increasingly needs to protect critical information and sensitive data, particularly within land mobile radio (LMR) communications, and encryption is the best available tool to achieve that security. The resources below provide best practices and considerations for planning, implementing, and securely operating encryption with public safety communications.
- Field Operations Guides (FOGs) | CISA - FOGs are technical references for emergency communications planning and for radio technicians responsible for radios that will be used in emergency responses.
- Stop Ransomware: Public Safety Emergency Communications Resources | CISA – Emergency communications operations are crucial to public health and safety; interruptions in service could result in loss of life. Because of the urgent nature of their operations, emergency communications centers (ECC) are high-value targets for cyber threat actors. This page provides resources designed to help reduce the risk of ransomware.
- CISA Tabletop Exercise Packages | CISA – **CTEPs** are a comprehensive set of resources designed to assist stakeholders in conducting their own exercises. Partners can use CTEPs to initiate discussions within their organizations about their ability to address a variety of threat scenarios.
- SAFECOM Writing Guide for Standard Operating Guidelines - developed to support communities writing SOGs or instructions for incident response. This resource highlights significant components of a standard SOG.

Resilience Planning and Supply Chain Security

- The Security Assessment at First Entry | CISA tool is a high-level resource for facilities that have limited or no security measures or planning in place. It is designed to assess current security posture and produce a report in under two hours.
- State and local governments as well as critical infrastructure operators can use CISA's *Infrastructure Resilience Planning Framework (IRPF)* to better identify critical infrastructure, assess related risks, and develop and implement resilience solutions.
- Using the Mitigating ICT Supply Chain Risks with Qualified Bidder and Manufacturer Lists and Vendor Supply Chain Risk Management (SCRM) Template can help ensure the Internet Communication Technology (ICT) products you buy from vendors meet industry standards. Both tools are great resources for IT or cyber security personnel, acquisitions and procurement professionals, those who manage vendor and supplier lists, among others.
- The Regional Resiliency Assessment Program | CISA is a voluntary, cooperative assessment of specific critical infrastructure that identifies a range of security and resilience issues that could have regionally or nationally significant consequences. The goal of the program is to generate greater understanding and action among public and private sector partners to improve the resilience of a region's critical infrastructure.

Self-Assessment and Exercises

- 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.
- CISA provides ready-to-use *exercise packages* for our security partners working with public gatherings and crowded places to use in initiating training within their organizations. Each package can be customized and includes templates with exercise objectives, scenarios, and discussion questions.
- Learn about resources available for vulnerability assessments and continuity plans, including Critical Infrastructure Assessments | CISA.

Resources for All

- Report suspicious activity to local law enforcement to public safety officials to discuss security and resilience enhancements.

- Within each CISA region are local and regional Protective Security Advisors (PSAs), Cyber Security Advisors (CSAs), Emergency Communications Coordinators (ECCs), and Chemical Security Inspectors (CSIs). Contact your regional representative today for a complimentary assessment: Security Advisors | CISA.
- The Cross-Sector Cybersecurity Performance Goals | CISA were developed in close partnership with organizations across government and the private sector. They provide voluntary guidance to critical infrastructure and other organizations to help them prioritize security investments toward areas that will have the greatest impact on their cybersecurity.
- CISA offers three priority telecommunications services that enable essential personnel to communicate when networks are degraded or congested. Enroll in all three services here: Priority Telecommunications Services | CISA.
- Visit Telework Guidance and Resources | CISA for guidance on teleworking securely.
- Learn about the legal protections for information shared with CISA under the Protected Critical Infrastructure Information (PCII) Program at Protected Critical Infrastructure Information (PCII) Program | CISA.

TEMPLATES

Please find below templates crafted for your agency's use in amplifying awareness about Emergency Communications Month.

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 press release was authored by CISA.”

(Month, Day)
(Contact Name)
(Phone/Email)

CITY, STATE - (ORGANIZATION) Joins National Effort to Promote Security and Resilience as part of Emergency Communications Month.

(ORGANIZATION) has committed to participate in Emergency Communications Month to focus on the importance of our nation’s emergency communications systems. We all share the responsibility to keep our emergency communications secure and resilient. Public-private partnerships leverage our shared commitment by identifying vulnerabilities and mitigating risks through protective programs and training.

(INSERT QUOTE FROM YOUR ORGANIZATION SPOKESPERSON HERE)

This year’s theme is Resilient Together. Weather is becoming more extreme, physical and cyberattacks are a persistent threat, and technology is advancing in ways that will change our future very quickly. We must prepare by accepting that it’s our responsibility to strengthen emergency communications and protect the vital services it provides. We can do this by embracing resiliency and building it into our preparedness planning—and then exercising those plans. The safety and security of the nation depends on the ability of emergency communications to be able to prepare for and adapt to changing conditions and to withstand and recover rapidly from disruptions. This starts with building resilience into emergency communications investment.

America’s national security and economic prosperity are increasingly dependent upon emergency communications systems that are at risk from a variety of hazards, including both physical and cyber. Emergency communications 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 emergency communications, 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 EMERGENCY COMMUNICATIONS AND MAKE IT MORE RESILIENT).

For more information about Emergency Communications Month, visit [INSERT ORGANIZATION WEBPAGE IF APPLICABLE] or cisa.gov/emergency-communications-month.

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

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 Emergency Communications 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.

Resolve to be Resilient Together

April is Emergency Communications Month, a nationwide effort to raise awareness and reaffirm the commitment to keep our nation's emergency communications systems secure and resilient. (ORGANIZATION) has committed to building awareness of the importance of emergency communications.

[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 ***Resilient Together***. Weather is becoming more extreme, physical and cyberattacks are a persistent threat, and technology is advancing in ways that will change our future very quickly. We must prepare by accepting that it's our responsibility to strengthen emergency communications and protect the vital services it provides. We can do this by embracing resiliency and building it into our preparedness planning—and then exercising those plans. The safety and security of the nation depends on the ability of emergency communications to be able to prepare for and adapt to changing conditions and to withstand and recover rapidly from disruptions. This starts with building resilience into emergency communications investment.

The safety and security of the nation depends on the ability of emergency communications to be able to prepare for and adapt to changing conditions and to withstand and recover rapidly from disruptions. Attacks cannot be completely prevented from happening, but we can minimize their impact by building resilience into our emergency communications and into our society.

For more information, visit CISA's Emergency Communications Month web page for more information and resources: cisa.gov/emergency-communications-month.

The message contained in this newsletter/blog was authored by the Cybersecurity and Infrastructure Security Agency (CISA).

SLTT Proclamation Template

If you choose to use this template, you must include the following language attributing the authorship to CISA: "This Message contained in this proclamation was authored by CISA."

PROCLAMATION

Emergency Communications Month April 2024

WHEREAS, "Emergency Communications Month" creates an important opportunity for every resident of [REGION, TOWN, or STATE] to recognize that emergency communications play an indispensable role in protecting our nation's critical infrastructure and enhancing our national security and resilience is a national imperative; and

WHEREAS, the nation's emergency communications systems facilitate coordination among diverse public safety responders, keeping emergency communications secure, functioning, and resilient requires a unified whole-of-nation, whole-of-community effort; and

WHEREAS, managing and mitigating risks to emergency communications systems 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 emergency communications systems secure and resilient is a shared national responsibility that all citizens of [REGION, TOWN or STATE] can get involved in and do their part, along with the many businesses and industries that make up the emergency communications community, and in their local communities by learning about risks to emergency communications in their areas and taking steps to build resilience. THEREFORE, BE IT RESOLVED that the [GOVERNING BODY] hereby proclaims April 2024 as Emergency Communications Month and encourages communities to support the national effort to strengthen emergency communications security by engaging in partnerships together toward creating a more resilient society.

DATED this _____ Day of _____________ 2024 by the [GOVERNING BODY]

____

NAME, TITLE

The message contained in this proclamation was authored by the Cybersecurity and Infrastructure Security Agency (CISA).

SOCIAL MEDIA AND ONLINE RESOURCES

Social Media

CISA will use social media to share news and updates about Emergency Communications Month. *Visit CISA.gov for more information and follow us on X, Facebook, LinkedIn, Instagram* and use the hashtag #ResilientTogether to join the conversation. Also, be sure to check our page for updates at cisa.gov/emergency-communications-month.

Useful Videos

Emergency communications-related videos are available through the DHS YouTube page. These links can be used in messaging materials or through Twitter and Facebook postings.

- ✓ 911 is just the Beginning of Emergency Communications Month – Oklahoma Statewide Interoperability Coordinator Nikki Dallas talks about how calling 911 is just the beginning of emergency communications.: 911 is just the Beginning of Emergency Communications (youtube.com)
- ✓ Why CISA chose April as the Official Emergency Communications Month – Deputy Director Nitin Natarajan and Executive Assistant Director for Emergency Communications Billy Bob Brown Jr. answer why CISA chose April as the official month to recognize the important field of Emergency Communications: Why CISA chose April as the Official Emergency Communications Month (youtube.com)
- ✓ National Emergency Communications Plan - The National Emergency Communications Plan (NECP) is the Nation's strategic plan to strengthen and enhance emergency communications capabilities: National Emergency Communications Plan | CISA

Downloadable Graphic

This graphic can be used in messaging materials or through social media (X, Twitter, and Facebook: 1200x627 and Instagram: 1080x1080 and 1920x1080) postings.

FREQUENTLY ASKED QUESTIONS (FAQS)

What are Emergency Communications?

Emergency Communications are the means and methods for exchanging the information necessary for successful incident management - all day, every day. This includes the use of various technologies, protocols, and systems to facilitate communication and coordination among emergency personnel, government agencies, private sector entities, and the public. Effective emergency communications are essential for situational awareness, resource allocation, and decision-making during emergencies and disasters. CISA works with federal, state, local, tribal, territorial, and private sector partners to enhance the reliability, interoperability, and security of emergency communication systems across the United States.

Emergency Communications enable critical infrastructure to remain secure and resilient and keep the American people and its allies safe.

Who is Part of the Emergency Communications Community?

Emergency communications constitute a complex and essential ecosystem, facilitating coordination among diverse responders at the federal, state, local, tribal, and territorial levels, enabling the real-time exchange of vital information during crises. This vast field encompasses 911 telecommunicators, first responders from fire, police, EMS, alerts, warnings and notifications officials, critical infrastructure and public works partners, public health personnel, and cybersecurity professionals, all working collaboratively to respond to and recover from disasters and emergencies.

How is CISA carrying out its Emergency Communications Mission?

CISA’s Emergency Communications Division in coordination with CISA's Emergency Communications Coordinators leads the nation’s public safety, national security, and emergency preparedness communications efforts to keep America safe, secure, and resilient through the following:

Nationwide Interoperability – CISA promotes interoperability and resilience by providing the tools and resources for stakeholders to operate in the next generation environment and cyber ecosystem, including direct assistance to jurisdictions across the U.S. and improving awareness of Next Generation 911 (NG911) capabilities.

Effective Communications Planning – CISA bolsters existing partnerships and building bridges to emergency communications stakeholder across critical infrastructure sectors to reduce risk to National Critical Functions. In partnership with stakeholder groups like SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC), CISA provides resources to the districts, states, territories and tribal nationals to develop Statewide Communication Interoperability Plans. These plans help advocate for sustainment and investment funding from state and local governments. Additionally, at every level of the emergency communications ecosystem, planning should incorporate options for Primary, Alternate, Contingency and Emergency (PACE) communications for resiliency against all threats and hazards and for appropriate interoperability.

Moving Information with Interoperable Priority – CISA partners with industry and research organizations to make priority data, video, and information services available to all national security and emergency preparedness stakeholders through a constellation of carrier partners. CISA ensures that interoperable priority service requirements are satisfied by cooperating with network service providers as they evolve to next generation networks.

CISA plays a role in support response efforts by ensuring that its stakeholders have the tools needed to communicate during steady state and emergency operations. We encourage our stakeholders to connect with their Statewide Interoperability Coordinator (SWIC) who can help with securing training, planning for the use of new technologies, and building partnerships across all levels of government, individual states or territories.

Why is it Important to Focus on the Emergency Communications Needs of the Country?

Focusing on the emergency communications needs is crucial for several reasons. Firstly, effective communication is essential for coordinating emergency response efforts during crises such as natural disasters, terrorist attacks, or public health emergencies. Timely and accurate communication can save lives by facilitating the deployment of emergency services, disseminating critical information to the public, and coordinating rescue and relief operations. Secondly, robust emergency communication systems enhance community resilience by empowering individuals to prepare for and respond to emergencies effectively. Clear and reliable communication channels foster public trust and confidence in emergency response agencies, encouraging active participation in preparedness activities and adherence to evacuation or shelter-in-place directives. Additionally, prioritizing emergency communications infrastructure strengthens national security by safeguarding critical assets and ensuring continuity of operations in the face of cyber threats, physical attacks, or infrastructure failures.

Overall, focusing on the emergency communications needs of the country is essential for enhancing public safety, preserving infrastructure resilience, and safeguarding national security in an increasingly complex and interconnected world.

And the underpinning to all of that is the need to be able to communicate interoperably, securely, and resiliently. Officials at every level of government and the public must be able to connect in both regular every day and steady-state situations AND emergency situations or crises response.

How do Cyber Interdependencies Affect Emergency Communications?

Cyber interdependencies profoundly affect emergency communications by disrupting communication channels, compromising data integrity, overloading systems with denial-of-service attacks, targeting digital technologies, exploiting interconnectedness with critical infrastructure, and raising concerns about data privacy and confidentiality. These threats can result in delayed response times, misinformation dissemination, inaccessibility to emergency services, and cascading disruptions across critical infrastructure sectors. Mitigation strategies involve implementing robust cybersecurity measures, conducting regular risk assessments, fostering collaboration between cybersecurity experts and emergency response agencies, and prioritizing employee training to enhance preparedness and resilience against cyber threats in emergency communication systems.

CISA makes available several resources that further inform actions organizations can take to integrate security, including:

- **911 Cybersecurity Resources Hub** – This one-stop shop compiles cybersecurity resources to make it easy for Emergency Communications Centers to report a cyber incident, find real-world case studies, access cybersecurity education and training opportunities, and learn about best practices to identify and protect networks from cyberattacks. CISA, SAFECOM, and NCSWIC worked collaboratively with state and local public safety and emergency communications stakeholders to develop this interactive website. To learn more visit: 911 Cybersecurity Resource Hub | CISA

- **Communications and Cyber Resiliency Toolkit:** The ability to maintain voice and data communications at all times is critical for public safety agencies to perform their life-saving missions. By establishing resiliency measures, public safety communications can better withstand potential disruptions to service. CISA developed the Public Safety Communications and Cyber Resiliency Toolkit to assist public safety agencies and others responsible for communications networks in evaluating current resiliency capabilities, identifying ways to improve resiliency, and developing plans for mitigating the effects of potential resiliency threats.

- **Transition to Advanced Encryption Standard White Paper:** The Federal Partnership for Interoperable Communications (FPIC) has released The Transition to Advanced Encryption Standard White Paper. The White Paper highlights the vulnerabilities of the continued use of the Data Encryption Standard (DES) and non-standard algorithms and provides an overview of actions and next steps being taken to support state, local, tribal, territorial (SLTT) agencies transition to Advanced Encryption Standard

(AES) capabilities. It also provides background information on the Criminal Justice Information Service (CJIS) Policy, and the Protected Critical Infrastructure Information (PCII) Program. The document can be used by public safety agencies to better understand the vulnerabilities to sensitive information from using DES and other non-standard encryption algorithms. Agencies can also find background information about CJIS policies and resources, like the PCII Program, to better protect critical infrastructure and information.

- **Cybersecurity and Physical Security Convergence Guide**: An informational guide about convergence and the benefits of a holistic security strategy that aligns cybersecurity and physical security functions with organizational priorities and business objectives. The guide describes the risks associated with siloed security functions, a description of convergence in the context of organizational security functions, benefits of convergence, a flexible framework for aligning security functions, and several case studies. To learn more, visit Cybersecurity and Physical Security Convergence Action Guide | CISA.

It is also important to understand not only how critical infrastructure relies on secure cyber systems, but also how to protect our critical infrastructure against cyberattacks. Through Emergency Communications Month, CISA promotes shared awareness and understanding of the diverse hazards affecting critical infrastructure resilience. For tools and tips on cybersecurity visit Cybersecurity Best Practices | CISA.