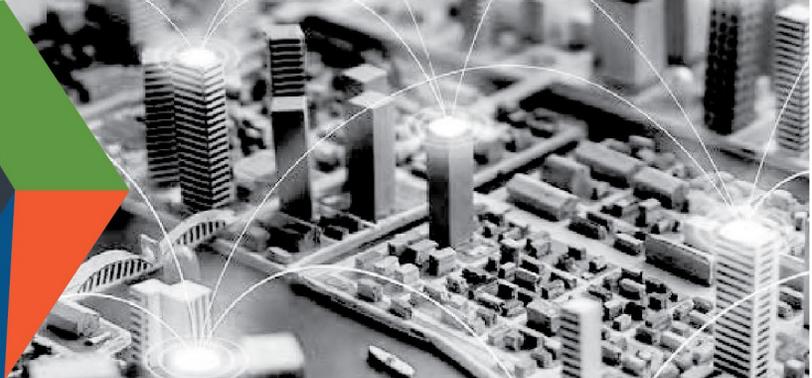




**CISA**  
CYBER+INFRASTRUCTURE

DEFEND TODAY, SECURE TOMORROW



# GUIDELINES FOR 911 CENTERS: PANDEMIC PLANNING

These recommendations are advisory and are not to be considered Federal directives or standards. Individual centers should review and apply the guidance based on their own requirements and discretion. All actions should appropriately balance public safety, the health and safety of the workforce, and the continued delivery of essential services and functions.

Maintaining operational and resilient emergency communications is imperative during pandemic response for both public health and safety, as well as community well-being. A critical component of emergency communications are 911 centers—to include emergency communication centers (ECC), public safety answering points (PSAP), public safety communication centers (PSCC), emergency operations centers (EOC), and other public service command centers. A pandemic presents an immediate threat to the ability of these centers to operate effectively. The following guidance is intended to support public safety partners across all levels of government when engaging in the development of pandemic plans that promulgate policies, procedures, governance, resource planning, and contingency considerations.

For the most current guidance on disease control and prevention, visit the [Centers for Disease Control and Prevention](#) (CDC). Be sure to look for specific guidance for current circumstances and role. For example, for the coronavirus pandemic (COVID-19), consult [Interim Guidance for Emergency Medical Services \(EMS\) Systems and 911 Public Safety Answering Points \(PSAPs\) for COVID-19 in the United States](#).

## GOVERNANCE

Strong and transparent governance should be the basis of center operations, especially when planning for and responding to a pandemic. It is recommended that centers coordinate with all stakeholders and partners (e.g., agencies served by the center; local health departments; public utilities; public works; communications network service providers; third-party service providers [e.g., language translation services]; poison control lines; neighboring jurisdictions; Federal, State, local, Tribal, and territorial partners) to ensure that pandemic response plans remain accurate, effective, and adaptable. Centers should develop a pandemic plan as part of their continuity of operations (COOP) plan.<sup>1</sup> The pandemic plan should be regularly reviewed and updated consistent with revisions in guidance. Training and exercises are vital parts of the planning process to ensure all personnel are aware of their roles and responsibilities and can execute them during a pandemic. The plan should be periodically tested and exercised, while lessons learned should be incorporated into plan updates.

## DEFINITIONS



**Continuity:** “the ability to provide uninterrupted services and support, while maintaining organizational viability, before, during, and after an incident that disrupts typical operations.”<sup>2</sup>



**Contingency Planning:** planning and implementation of measures to mitigate risks based on identification and regular monitoring of risks, vulnerabilities, and capacities.<sup>3</sup>

<sup>1</sup> For example, see the [Pandemic Continuity of Operations Response Plan Outline](#), which is consistent with best practices recommended from the CDC, Federal Emergency Management Agency (FEMA), National Emergency Numbering Association (NENA), National Fire Protection Association (NFPA), Equal Employment Opportunity Commission (EEOC), and Occupational Safety and Health Administration (OSHA).

<sup>2</sup> FEMA, “[Continuity Resource Toolkit](#),” last modified May 1, 2020.

<sup>3</sup> World Health Organization (WHO), “[WHO Guidance for Contingency Planning](#),” 2018.

CONNECT WITH US  
[www.cisa.gov](http://www.cisa.gov)

For more information,  
email [ECD@cisa.dhs.gov](mailto:ECD@cisa.dhs.gov)



[Linkedin.com/company/cybersecurity-and-infrastructure-security-agency](https://www.linkedin.com/company/cybersecurity-and-infrastructure-security-agency)



@CISAgov | @cyber | @uscert\_gov



[Facebook.com/CISA](https://www.facebook.com/CISA)

911 centers serve a common mission across the Nation, but their individual operating procedures and protocols differ. Prior to drafting any governing documents, it is important that 911 centers translate continuity and contingency planning to their unique organizational and operational environments. Each plan should address the four phases of emergency management—mitigation, prevention, response, and recovery. Consider these steps:

- Identify and prioritize the center’s essential functions through evaluations, such as risk assessments and business process and impact analysis.
- Determine appropriate mitigation options including alternate/additional operating locations, telework, devolution, and mutual aid agreements.
- Identify the center’s key elements that correlate with the essential functions, including both human resources and technology.
- Establish an order of succession that presents a predefined transition of leadership. List positions, delegations of authority, and consider alternatives for positions that cannot be readily replaced. Review and update regularly.
- Develop a continuity plan and implement selected options and elements based on identified present needs, previous research, and prioritization.
- To ensure that the governing plans and procedures remain accurate and up-to-date, follow the Federal Emergency Management Agency’s (FEMA) recommended continuity program management cycle<sup>4</sup>:
  - Step 1: Develop Plans & Procedures
  - Step 2: Conduct Test, Training & Exercises
  - Step 3: Develop Evaluations, After Action Reports (AARs), & Lessons Learned
  - Step 4: Develop Improvement Plans

## RESOURCE PLANNING

Planning resources for a pandemic is different from preparing for a natural disaster. Pandemics are typically longer in duration and may occur in waves.<sup>5</sup> Pandemics also occur over a wide geographic area, thus affecting people and supply chains, potentially including worldwide impacts. Leadership at 911 centers should carefully consider the depth and breadth of resources required to maintain daily operations and the resources that those who rely on emergency services may need at this time.

<sup>4</sup> FEMA, “[Continuity Resource Toolkit](#),” last modified May 1, 2020.

<sup>5</sup> OSHA, “[Pandemic Influenza Preparedness and Response Guidance for Healthcare Workers and Healthcare Employers](#),” 2009.

### *Potential Pandemic Planning Partners*

Internal and external stakeholders should be included throughout the planning process. Pandemic planning teams could include:

- ✓ Center or agency personnel (e.g., oversight personnel, administrators, telecommunicators, Communication Unit Leader [COML], Public information officer (PIO)/Public Affairs representatives, Computer-Aided Dispatch [CAD] System Manager, Geographic Information System [GIS] Coordinator, Training Coordinator)
- ✓ Public safety entities (e.g., law enforcement, fire services, emergency medical services [EMS], public works)
- ✓ State and local emergency management agency representatives
- ✓ State and local health departments
- ✓ Government elected or appointed officials
- ✓ City or county finance office
- ✓ City or county attorney
- ✓ State or local government risk managers or insurance providers
- ✓ Statewide Interoperability Coordinator (SWIC)
- ✓ State and local public health services (e.g., hospital emergency room administrators and urgent care providers)
- ✓ Providers of key services (e.g., local exchange carriers, commercial communications service providers, utility providers, food service providers, transportation, lodging)
- ✓ Critical infrastructure owners and operators
- ✓ Representatives from local Tribes and other Tribal partners
- ✓ Representatives of voluntary agencies (e.g., fire departments, rescue squads, EMS organizations, organizations that serve the deaf and hard-of-hearing communities)
- ✓ Representatives of unions or collective bargaining units of response employees and other agencies, as required

While not all these parties will contribute to writing the plan, engaging them in the review process and considering their role and responsibilities (e.g., approval authority, individual contributor, supply chain) during a pandemic will strengthen the plan.

When planning, expect:

- Significant loss of staff hours and availability (e.g., illness, need to care for others)
- Need to modify call answering and medical dispatch protocols
- Moderate fluctuations in call volume and dispatched calls for services to all serviced disciplines
- Need to include new or additional operating locations (e.g., backup communication center, field hospitals) or closure procedures
- Shortage of critical supplies and resources (e.g., cleaning/disinfecting supplies and equipment, personal protective equipment [PPE], telecommunications and technology resources, facility equipment and space)
- Need for continuous community outreach and support
- Need to adapt to evolving circumstances, including easing of restrictions and return to normalcy

The subsequent sections provide best practices to mitigate the impacts of these challenges.

## *Maintain Staffing Levels*

- Coordinate with State or local governments and other pandemic task forces to ensure that essential center personnel are identified as members of the essential critical infrastructure workforce and afforded the same protections and priorities as other first responders (e.g., pandemic testing, transportation, alternative sheltering options).
- Institute pandemic policies and procedures to maintain staffing levels. Examples include:
  - Cancel all prearranged and upcoming meetings and conferences
  - Consider cancelling pre-approved leave, if necessary
  - Limit training to essential personnel on an as-needed basis (e.g., how to properly use and dispose of PPE)
- Take steps to prevent, mitigate, and respond to the spread of the virus among center staff, including authorizing priority supply of sanitizing supplies and PPE to centers with accompanying training to ensure effective use. Advise personnel to use PPE mindfully and follow the CDC's [Strategies to Optimize the Supply of PPE and Equipment](#). Develop recovery plans now to assure triggers that signal the change from response to recovery are well understood and achievable.
- Create tools such as job aids for vital roles and functions (e.g., checklist of activities, contact information) to assist personnel in learning and understanding roles different from their normal functions.
- Coordinate with human resources, risk management, and legal counsel to ensure easily accessible medical screening capabilities throughout the pandemic; be aware of Americans with Disabilities Act (ADA) and Health Insurance Portability and Accountability Act of 1996 (HIPAA) compliance requirements.
- Cross-train positions to ensure personnel are qualified, with minimal refamiliarization training, to assume roles to cover for employees who might be absent.
- Establish a telephone response unit (TRU) to respond to non-emergency calls or calls for services that do not require the physical presence of a public safety responder (e.g., criminal reports for property crimes of non-violent nature, with no suspect or witness information, occurred more than 30 minutes ago).
- Develop processes and procedures for directing callers to the locality's information phone line (e.g., 311 or other government directory numbers) if applicable.
- Reference [Guidelines for 911 Centers: Pandemic Operating Procedures](#) and [Guidelines for 911 Centers: Cleaning and Disinfecting During a Pandemic](#) for additional best practices on limiting staff exposure to illness and maintaining a clean facility.

## *Modify Call Answering and Medical Dispatch Protocols*

- Develop a call screening process specific to the pandemic. Train floor personnel on its usage and make sure that all relevant information is captured in call notes and the information is communicated over the radio or mobile data systems to responders. This screening process may change as the pandemic evolves and new information emerges.

**CONNECT WITH US**  
[www.cisa.gov](http://www.cisa.gov)

**For more information,**  
email [ECD@cisa.dhs.gov](mailto:ECD@cisa.dhs.gov)



[Linkedin.com/company/cybersecurity-and-infrastructure-security-agency](https://www.linkedin.com/company/cybersecurity-and-infrastructure-security-agency)



@CISAgov | @cyber | @uscert\_gov



[Facebook.com/CISA](https://www.facebook.com/CISA)

- Ensure availability of CAD administrator and vendor support, as call answering modifications may require CAD tailoring or additions to the CAD or call taking software depending upon the center's technology.

## *Anticipate Fluctuations in Call Volume and Dispatched Calls for Services Across All Disciplines*

- While centers will experience fluctuations in telephone and dispatched call volumes due to outbreak circumstances, the length of time to manage each call may also increase due to the requirements associated with pandemic screening protocols. Centers should explore innovative ways to manage EMS calls for service to keep the number of calls in queue as low as possible.
- Coordinate emergency orders and guidance across pandemic response partners. This will ensure consistency in messaging and allow the center to anticipate increased call volume upon release of the guidance. Reference [Guidelines for Executives: 911 Center Pandemic Recommendations](#) for additional best practices on partner coordination.

## *Develop Additional Operating Locations and/or Closure Procedures*

- Communications centers may need to transfer operations or combine operations with a back-up center. Transferring of 911 calls to another center is generally either part of a standard COOP strategy or can be accomplished by the local exchange carrier (911 telephone service provider). When developing a plan to transfer operations:
  - Review guidance on telework and consult with the information technology (IT) section or department to assess telework risk. Reexamine telework policies and allow remote work whenever possible.
  - Document available backup facilities and systems (e.g., broadband, cloud-based CAD, access to radio system control or remote consoles, mobile data systems access).
  - Identify whether critical capabilities (e.g., location, CAD, other critical center IT tools) will be available.
  - Consider that radio resources (the ability to dispatch public safety agencies from remote communications centers) are dependent upon either the presence of a mutual aid radio network (e.g., a Statewide/countywide radio network), or pre-existing planning, engineering, and deployment of radio access consoles or other equipment.
  - Define temporary work-arounds, such as establishing dispatch functions at police stations, fire stations, or other suitable facilities and alerting the public to call a seven- or 10-digit number for public safety response.
  - Examine potential efficiency losses, such as time delays in coordinating call-taker-to-dispatch seven- or 10-digit dialing or a loss of CAD system access and loss of management and control of calls for services and field responder status. These could create longer translations via pencil and paper, increased susceptibility to misrouting, increased probability of call and field resources tracking, and closure errors.
  - Clean backup site(s) and test all equipment to prepare for potential move of operation. If possible, staff backup location to monitor operations and to ensure a smooth transition of operations if needed.
- There is no single authoritative source of information regarding when communications centers are to shut down. The decision to close a center is made by the agency having jurisdiction. Close coordination is recommended with other communications centers, the first responder agencies that the communications center serves, the center's/agencies' COMLs and the jurisdiction's emergency management agency.
- When the decision to close is made, notifications should be made to the jurisdiction's elected and appointed leaders, SWICs, State and local emergency management agencies, critical infrastructure partners, alerting authorities, PIO/Public Affairs representatives, departments and agencies within the communications center's jurisdiction, Tribal partners, and departments and agencies in neighboring jurisdictions.
- The PIO or Public Affairs representatives should prepare and disseminate an alert to the general public, using broadcast AM, FM, and TV stations, and any cable or satellite TV and radio providers serving the jurisdiction. The

jurisdiction's websites and social media should also publicize the closing of a communications center and provide directions to the public on how to reach emergency services while the center remains closed in the event of a complete shutdown.

## *Plan and Sustain Critical Supplies and Resources*

Ensure that any identified gaps in needed resources or services to maintain the center's operations are consistently monitored, and if solutions are not forthcoming, be prepared to work with emergency management officials to elevate official requests to the next level of government. Executives and elected officials should be prepared to make additional outreach for help and resources. The tables in this section specifically address best practices regarding management of cleaning and disinfecting supplies and PPE, telecommunications and technology resources, and facility space and equipment.

### Cleaning/Disinfecting Supplies and PPE

Obtain and inventory enough critical supplies to last through the first wave of a pandemic and stage supplies at each worksite; keep the supplies in a secure location or plan for security to protect the supplies; follow the CDC's [Strategies to Optimize the Supply of PPE and Equipment](#), CDC's [Reopening Guidance for Cleaning and Disinfecting Public Spaces, Workplaces, Businesses, Schools, and Homes](#), U.S. Environmental Protection Agency's (EPA) list of [Disinfectants for Use Against SARS-CoV-2](#) (the virus that causes COVID-19)

Maintain an inventory supply list and review at the end of each shift to assess the need to reorder supplies. Consider capture and analysis of user generated data (e.g., [PPE burn rate](#)) to develop awareness to predict and alert critical needs; design flow charts and infographics based on the analysis to assist in timely decision-making

### Telecommunications and Technology Resources

Identify minimum communications requirements to perform essential functions and alternate equipment and systems, staff and their responsibilities, and facilities or base locations

Consider route diversity<sup>6</sup>, redundancy, and protective and restorative measures (e.g., [Telecommunications Service Priority Restoration](#)) to decrease the likelihood of disruption during a pandemic, including measures for teleworking staff (e.g., alternate phone numbers, email, instant messaging)

Document alternative communications systems available but not used during day-to-day operations (e.g., satellite)

Ensure enrollment in and dissemination of procedures for accessing priority service programs (i.e. [Government Emergency Telecommunications Service](#), [Wireless Priority Service](#)) in the event that commercial communication systems become congested

Be aware that [Telecommunications Service Priority](#) provisioning may be helpful in terms of getting critical private lines to service providers (e.g., firehouses, police substations) or to target hazard sites (e.g., prisons, hospitals, bulk petroleum storage sites) and getting other telephone lines established and activated on short notice

At the onset of an incident, implement a stress test to evaluate the center's communications capabilities (e.g., enterprise network, virtual private network [VPN]), and configure accordingly to accommodate the surge of personnel who may be teleworking

Test, review, and update essential records, databases, and systems. These resources will need to be available electronically to employees who are teleworking or located at alternate sites. This may include secure access to network and other databases to allow for functions such as payroll processing, ordering of supplies, and the ability for vendors to remotely provide services, such as needed software upgrades

Implement a daily radio system, CAD system, and other critical IT systems (e.g., alert, warnings, and notification [AWN] systems) health check and continue preventative maintenance

Actively monitor critical systems health and performance and initiate maintenance or corrective services to any anomalies

Maintain technology and telecommunications (e.g., lighting, network connections, Wi-Fi [both guest and restricted access]) on the operations floor and beyond (e.g., meeting rooms, training rooms) in the event they may be pressed into service or used for additional entities (e.g., task force, media)

<sup>6</sup> Cybersecurity and Infrastructure Security Agency (CISA), [Communications Resiliency](#), last accessed May 6, 2020.

## Telecommunications and Technology Resources

Establish agreements with contracted service vendors that address operational continuity in the event of a pandemic. Source critical parts and pieces and train personnel on basic repair procedures. Confirm service level agreements (SLA) will continue to be performed, making sure “force majeure” does not excuse non-performance or lead to contract termination, so that services will be available from all critical systems vendors

Determine requirements and procure backup systems in addition to maintaining existing ones and train personnel on usage and switch-over processes

Establish inventory of primary and backup center hardware, including each piece’s respective manufacturer’s cleaning instruction

Establish an inventory of all software authorized for use, provide appropriate cybersecurity controls, and ensure all software is patched with the latest updates. These updates should be done regularly, regardless of pandemic response needs

Prepare to issue alternate credentialing tools if centers cannot issue or use standard credentials (e.g., tokens, Personal Identity Verification [PIV] cards) for physical and logical access. Ensure that essential vendors and service providers have been vetted and provided viable credentials for access to facilities

Verify passwords for access to services and programs essential to daily operations (e.g., logging on to desktop, Awn systems, services such as center’s network resources, CAD, [National Law Enforcement Telecommunications System](#) [Nlets], [National Crime Information Center](#), State and local Criminal Justice Information Services [CJIS])

Consider the potential for using the center as a source of real-time, reliable data that could inform response efforts throughout the public safety ecosystem; research and apply Geographic Information System (GIS)-based services or programs to visually represent call volume, response level, outages, and other pertinent categories

## Facility Space and Equipment

Examine local options for tent rentals, space rentals, or storage facilities if additional square footage will be needed for essential supplies or to enable physical distancing

Maintain primary and backup facilities and functions (e.g., lighting; heating, ventilation, and air conditioning [HVAC] system; plumbing). As the pandemic continues, it may become increasingly difficult to fix these functions

## Maintain Community Outreach and Support

- Inform the public of changes in call handling and response through a coordinated messaging with other public safety partners; distribute the information as widely as possible via available communications channels. For additional best practices on Awn, use the [Public Safety Communications Ten Keys to Improving Emergency Alerts, Warnings & Notifications](#).
- Include updated response procedures that reflect the area and population served. Gender, age, ethnicity, socioeconomic status, transitory or recently arrived status, familial relationships, an individual’s or community’s past experiences, environmental and social factors, access and functional needs, language, literacy, ability, remoteness or isolation, access to technology, and other factors can all affect how people interpret and subsequently respond to Awn. Centers should actively engage these diverse populations to be as inclusive and accessible as possible in continuity and protective measures planning. Additionally, pre-messaging and alternative guidance can help those who need more time to prepare or cannot take the recommended protective actions.

## Adapt to Evolving Circumstances, Including Easing of Restrictions

While continuity of operations should be planned for in advance, there will be unforeseen circumstances that do not allow for advanced planning or training and exercises. Center managers should be flexible when unforeseen circumstances occur and draw upon resources that are available to them through reliable sources (e.g., CISA, CDC, FEMA, OSHA, Office of Personnel Management [OPM], The National 911 Program, NENA, The National Association of State 911 Administrators [NASNA], Association of Public-Safety Communications Officials-International [APCO]). Throughout the pandemic, and on a continuous basis, documenting and sharing lessons learned with partners, including SWICs, provides immediate situational awareness and enables improvements in future pandemic planning. As isolation or quarantine restrictions are eased, centers should be

**CONNECT WITH US**  
[www.cisa.gov](http://www.cisa.gov)

For more information,  
email [ECD@cisa.dhs.gov](mailto:ECD@cisa.dhs.gov)



[Linkedin.com/company/cybersecurity-and-infrastructure-security-agency](https://www.linkedin.com/company/cybersecurity-and-infrastructure-security-agency)



@CISAgov | @cyber | @uscert\_gov



[Facebook.com/CISA](https://www.facebook.com/CISA)

prepared to gradually transition staff and facilities back into normal service. This transition may include:

- Return to normal shift patterns and staffing allocations, adjusted to the newly identified incoming telephone and field calls for services patterns and loads
- Adjust resource allocations for calls for services from serviced public safety organizations
- Maintain or modify caller interrogation criteria as pandemic surveillance or triage requirements change
- Maintain constant communication and awareness of emergency management posture and public health pandemic surveillance that indicate changes in the devolution of the pandemic
- Ensure that cleaning continues and all capabilities to ramp up to a new wave of pandemic response are in place should the conditions warrant returning to modified responses, quarantine, or isolation<sup>7</sup>
- Anticipate changes to center operations and staffing needs based upon the devolution of the pandemic and more people resuming normal activities
- Consider ongoing staff obligations outside of work, including that dependent and pet care services may not yet be available
- Continue to ensure personnel access to mental and behavioral health assistance; recognize and reward personnel's accommodation to pandemic measures; and document unmet training or professional development requirements
- Review and prioritize facility and technology maintenance and repair needs

## OTHER PANDEMIC RESOURCES

Recognizing the critical importance of the health and performance of 911 centers during a pandemic, CISA has developed a suite of documents providing specific guidance, in addition to maintaining a clean and safe workspace:

- [Guidelines for Executives: 911 Center Pandemic Recommendations](#)—Emphasizes the importance of communications centers, highlights the unique risk of a pandemic to resiliency of 911 operations, communicates the need for executive level action, and provides a brief description of available guidance for 911 administrators.
- [Guidelines for 911 Centers: Pandemic Operating Procedures](#)—Provides recommendations on how to organize, train, and care for personnel while operating through a pandemic.
- [Guidelines for 911 Centers: Cleaning and Disinfecting for a Pandemic](#)—Provides unique cleaning and disinfecting guidance and resources for 911 centers during a pandemic.

In addition, the following resources provide guidance regarding pandemic planning:

- [FEMA Independent Study \(IS\)-1300: Introduction to Continuity of Operations](#)—Training course for government and private sector partners who are responsible or interested in continuity and continuity planning.
- [FEMA IS-520: Introduction to Continuity of Operations Planning for Pandemic Influenzas](#)—Training course specific to pandemic planning that introduces characteristics of a pandemic influenza, its effects on all facets of society, and the steps an organization can take to mitigate and minimize the effects.
- [FEMA Continuity Resource Toolkit](#)—Web-based toolkit that contains tools, templates, and additional resources to help implement concepts described in FEMA's [Continuity Guidance Circular](#).
- [U.S. Department of Transportation Preparing for Pandemic Influenza: Recommendations for Protocol Development for 9-1-1 Personnel and Public Safety Answering Points](#)—Education on pandemic influenza, including guidance on PSAP roles and responsibilities, provision of information to the public, and call screening and dispatch.
- [Pandemic Continuity of Operations Response Plan Outline](#)—Template with best practices from the CDC, FEMA, NENA, NFPA, EEOC, and OSHA.

---

<sup>7</sup> See CDC's [Reopening Guidance for Cleaning and Disinfecting Public Spaces, Workplaces, Businesses, Schools, and Homes](#) for detailed recommendations and best practices.

**CONNECT WITH US**  
[www.cisa.gov](http://www.cisa.gov)

**For more information,**  
email [ECD@cisa.dhs.gov](mailto:ECD@cisa.dhs.gov)



[Linkedin.com/company/cybersecurity-and-infrastructure-security-agency](https://www.linkedin.com/company/cybersecurity-and-infrastructure-security-agency)



@CISAgov | @cyber | @uscert\_gov



[Facebook.com/CISA](https://www.facebook.com/CISA)