FEMA and CISA Release First-Ever Cyber Incidents Planning Guidance For Emergency Managers

Release Date: November 7, 2023

WASHINGTON – Today, Department of Homeland Security (DHS) Secretary Alejandro N. Mayorkas, FEMA Administrator Deanne Criswell and Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly announced the release of an important new resource guide for emergency managers. The new "Planning Considerations for Cyber Incidents: Guidance for Emergency Managers" is a foundational product that provides a roadmap for emergency managers across the nation to plan for swift and effective solutions to address the consequences of a cyber incident.

"Protecting our communities against cyberattacks is a team effort and the Department of Homeland Security is continually working with our state, local, tribal and territorial partners to support their resilience," said Secretary Mayorkas. "This new resource guide combines the cybersecurity expertise of CISA with the emergency management experience of FEMA to provide communities with the latest information and resources to prepare for, protect against, and respond to cyber incidents. Releasing this guide is part of our continued commitment to helping emergency managers strengthen critical infrastructure and enhance the resilience of the communities they serve."

"We all rely heavily on technology in our day-to-day lives, yet even with the best cybersecurity program in place, cyber incidents are always a risk," said Administrator Criswell. "An interruption to one organization or system can have widespread impacts across a network, whether from natural hazards, human error, equipment failure, or malicious attacks. This new guide, created in partnership with CISA, will provide a roadmap for emergency managers to navigate the worst-case scenario, especially when lives are at risk and significant economic challenges arise."

“Emergency managers are used to dealing with whatever is thrown at them, from natural disasters to intentional acts to everything in between,” said Director Easterly. “In today’s world, where we are increasingly connected and our critical infrastructure relies on technology, an emergency manager’s role includes planning for a significant cyber incident. This guide will help organizations develop cyber incident response plans and ensure their resilience, preventing a bad day from becoming worse. I encourage every emergency manager to review this new guide and take steps to ensure they’re ready to respond to and mitigate a cyberattack.”

This new guidance document is the result of robust community engagement with the stakeholders, designed to help, state, local, tribal and territorial (SLTT) emergency management personnel. The straightforward best practices and comprehensive resources within the guide may also benefit emergency managers in academia, nonprofits, or the private sector, especially if they serve on a jurisdiction’s planning team.

Organizations and jurisdictions must have both a cybersecurity program to protect against disruptions and a cyber incident response plan to enable organizations to act quickly when interruptions occur. An effective and efficient response plan to cyber threats helps to reduce negative impacts and return functional services as soon as possible.

As FEMA and CISA continue to work together on the shared Department of Homeland Security National Preparedness Goal of maintaining a secure and resilient nation, this new tool guidance, combined with the department's national preparedness and cybersecurity grant programs, will support SLTTs with extensive cybersecurity planning and project development.

FEMA, in cooperation with CISA, will host several 60-minute webinars to provide an overview of the guide and supporting materials. To learn more about the webinar sessions and to download the guide and supporting materials, visit Planning Guides | FEMA.gov.