



EMERGENCY SERVICES SECTOR INFORMATION SHARING BULLETIN

October 2024



The Emergency Services Sector Information Sharing Bulletin (ESS ISB) is a monthly resource, produced by the Cybersecurity and Infrastructure Security Agency (CISA) Emergency Services Sector Management Team (ES SMT), which provides current, relevant information for sector stakeholders. The goal of the ESS ISB is to help improve the security and resilience of the entire Emergency Services Sector, including the law enforcement, fire and rescue services, emergency medical services, emergency management, and public works disciplines.

[CISA Active Shooter Guidance 2024](#)

On Wednesday, October 16, 2024, 10:30am – 12 noon (ET), please join the Region 2 National Preparedness Division, in partnership with the Cybersecurity and Infrastructure Security Agency (CISA) for a condensed webinar on steps you and your employees can take during an active shooter event.

Preparing employees for a potential active shooter incident is an integral component of an organization's incident response planning. Because active shooter incidents are unpredictable and evolve quickly, preparing for and knowing what to do in an active shooter situation can be the difference between life and death.

Who should attend? The whole community, workplace management, federal, state, local, tribal, and territorial agencies, community and faith-based organizations.

[Heightened Global Conflict Webinar: Implications for U.S. Preparedness & Homeland Security](#)

On Thursday, October 17, 2024, 2pm – 3pm (ET), please join the Center for Homeland Defense and Security for this webinar with national security experts discussing how conflicts abroad can impact U.S. capabilities and readiness here at home and the Nation's ability to respond to domestic threats and emergencies.

Foreign conflicts can significantly influence U.S. homeland security by heightening the threat of violent extremism, cyberattacks, and state-sponsored terrorism, as adversaries may target the U.S. in retaliation or to exploit perceived vulnerabilities. Such conflicts can also shift national priorities, focusing policy attention and finite resources on external threats.

Participants are encouraged to submit questions in advance on the webinar registration page or by emailing them to chds-eeep@nps.edu.



EMERGENCY SERVICES SECTOR INFORMATION SHARING BULLETIN

October 2024



Crisis Governing and Decision Making in Response to COVID-19: Lessons and Reflections Across Washington State

On October 23, 2024, 10:30am – 11:30am (PDT), Partners In Emergency Preparedness will facilitate this webinar. The prolonged nature of COVID-19, its lack of geo-spatial boundaries, and its magnitude and multi-sectoral impact created new challenges for structuring decision-making and who to involve at all levels of the responses. To get a better understanding of lessons learned around crisis decision-making during responses to Covid, the Washington State Legislature provided funding for the Washington Emergency Management Division to contract with the William D. Ruckelshaus Center to explore lessons learned around decision-making at multiple levels of government, public health entities, universities, businesses, and other key responders.

The presenters of this session will share findings and recommendations that can be considered by emergency management professionals, elected officials, public health professionals, and others.

FLETC Virtual Targeted Violence Prevention Presentations

On Thursday, October 24, 2024, 10am – 11:30am (ET), the Federal Law Enforcement Training Center will host a webinar that will discuss how mass violence attackers almost always follow a discernable pathway to violence. One step on that pathway to violence is probing and breaching. This presentation will examine where on the pathway to violence behavioral probing and breaching may take place. It will also identify examples of behavioral probing and breaching engaged in by previous attackers. The goal of this presentation is to familiarize participants with the concept of behavioral probing and breaching and identify those behaviors in people of concern.

Time to Act: CISA & FBI Call for Vigilance Against Iranian Cyberattacks

In a joint effort to fortify the security of U.S. democratic institutions, the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have published a crucial fact sheet aimed at safeguarding individuals and organizations associated with national political entities.

The document, titled *How to Protect Against Iranian Targeting of Accounts Associated with National Political Organizations*, outlines the ongoing threats posed by cyber actors affiliated with the Iranian government's Islamic Revolutionary Guard Corps (IRGC) and provides actionable steps to mitigate their impact.

For more information, visit [CISA.gov/Emergency-Services-Sector](https://www.cisa.gov/Emergency-Services-Sector) or contact us at EmergencyServicesSector@mail.cisa.dhs.gov.