Addressing the Threat: Cyberterrorism Defense Initiative (CDI)

Cyberterrorism threats to our nation’s technical infrastructure are real and immediate. Computers and servers in the United States are the most aggressively targeted information systems in the world. Each year, the attacks increase in severity, frequency, and sophistication. As our nation’s critical infrastructure grows more reliant on information technologies, it also becomes more exposed to cyber-attacks, both foreign and domestic. These attacks can threaten our nation’s economy, public works, communication systems, computer networks, and all other critical infrastructure.

To counter this threat, the Criminal Justice Institute’s Cyberterrorism Defense Initiative (CDI) has developed and delivers two courses provided at no cost to technical personnel working within our nation’s critical infrastructure. The two courses, Comprehensive Cyberterrorism Defense (CCD) and Cyberterrorism First Responder (CFR), are delivered utilizing a blended learning approach that incorporates instructor-led classroom lecture with hands-on lab applications by use of a mobile computer training lab.

Comprehensive Cyberterrorism Defense provides participants with the hands-on expertise necessary to defend data and communication networks from cyberterrorism events. Course participants are introduced to cyber-defense tools that will assist them in monitoring their computer networks and implementing cyber-security measures to prevent or greatly reduce the risk of a cyber-based attack against our nation’s critical cyber infrastructure.

Cyberterrorism First Responder focuses on emergency response to a cyber-based attack that has crippled or disabled critical cyber infrastructure. CFR prepares cyber first responders to effectively counter any type of cyber-based attack and restore critical infrastructure as quickly and efficiently as possible. Course participants are trained to use cyberterrorism response tools against real world simulated cyber-attacks, and learn the proper steps of incident response to include incident assessment, detection and analysis, and the containing, eradicating, and recovering process from a system or network-based attack.

Since initial funding was received in 2004, 271 courses have been delivered to 5,003 technical personnel trained in 32 states and 1 U.S. territory.

Attendees have included representatives from the following sectors:
- State, Local and Federal Government
- Public and Private Utilities
- Public Safety and Emergency Response
- Banking and Finance
- Colleges, Universities and Schools
- Hospital and Healthcare Providers
- Communications and Transportation
- Food and Agriculture

CDI and its courses were developed under a cooperative agreement from the U.S. Department of Homeland Security/FEMA, National Training and Exercises Division.

For a schedule of upcoming classes, visit: www.cyberterrorismcenter.org

CJI is a member of the National Cybersecurity Preparedness Consortium.

To learn more: www.cyberpreparednessconsortium.org