

CYBERSECURITY INCIDENT RESPONSE AND MANAGEMENT

PER-371

DHS/FEMA-funded course



CYBERSECURITY INCIDENT RESPONSE AND MANAGEMENT

PER-371

The Cybersecurity Incident Response and Management course utilizes NIST 800-61r2 to introduce participants to the cyber incident lifecycle. By engaging with a virtual cyber range, participants will gain practical, hands-on experience in responding to simulated real-world cyber attacks, enhancing their understanding of the critical role of information exchange during live cyber incidents. This course integrates the Incident Command System (ICS) that ultimately equips the public and private sectors with the framework, knowledge and practical skills needed to effectively navigate and manage the full spectrum of the cyber incident lifecycle.

Topics

- Cybersecurity incident response
- NIST Incident Command System integration into cybersecurity operations
- Initial and cascading impacts of cyber incidents
- Cybersecurity incident data analysis
- Strategic methods for containing and eradicating malicious software
- Recovery strategies implementation
- Managing a multi-faceted cybersecurity incident
- Situational awareness

Prerequisites

None

Recommendations

Participants are recommended to have successfully completed any one of the following courses: **AWR136**, **AWR169w**, **AWR376**, **AWR383**, **AWR395**, **AWR399w**, **AWR421**. These courses can be found online at: teex.org/program/dhs-cybersecurity/

In addition, participants are recommended to have successfully completed all of the following courses: **ICS 100**, **ICS 200**, and **ICS700**. These courses can be found online at: training.fema.gov/is

FEMA / SID Number

Students must have a FEMA Student Identification Number (SID) to attend classes. To obtain a SID, register online at: cdp.dhs.gov/femasid

Course Length

24 hours

Class Size

30 Participants

Venue

Emergency Operation Training Facility -
 College Station, TX

Participants

It is essential to have representation from cross-sector public and private entities who should coordinate with emergency management to address local jurisdiction cybersecurity emergencies or disasters. This includes representatives from:

- Information Technology
- Risk Management/Emergency Planning/Continuity Planning/Disaster Recovery
- Public Works/Wastewater and Water
- Schools/Universities
- Communication Sector
- Transportation Sector
- Energy Sector
- Defense/Industrial Base Sector
- Elected and Appointed Officials
- Financial Sector
- Health Care Sector
- Emergency Services Sector

For more information, contact:

TEXAS A&M ENGINEERING EXTENSION SERVICE

200 Technology Way

College Station, Texas 77845-3424

979.431.4837

bcs@teex.tamu.edu

TEEX.org/cyber

