Federal Reserve Bank of Dallas

The Federal Reserve Bank of Dallas is hosting MGT456 Integration of Cybersecurity Personnel into the Emergency Operations Center **March 26-28, 2024**. Below, I have included additional information regarding the class:

LOCATION:
Federal Reserve Bank of Dallas
2200 N Pearl St
Dallas, TX 75201

Please use our Parking Lot address if you plan on parking onsite in our free parking lot:
2320 Thomas Ave
Dallas, TX 75201

DATE & TIME:
March 26-28, 2024
- 8:00 AM – 5:00 PM

Registration:
https://my.teex.org/TeexPortal/Default.aspx?MO=mCourseCatalog&D=FP&C=MGT456&S=18

Course Description:
This scenario-based course will guide emergency response organizations and critical infrastructure IT personnel through multiple simulated events to learn how to coordinate efforts during a cyber incident. These real-time exercises are designed to assist jurisdictions with managing cyber response efforts between traditional emergency responders and IT professionals. The use of expert instructors from IT and emergency response fields will offer participants real-world knowledge to successfully integrate cybersecurity personnel into the Emergency Operations Center (EOC).

Topics:
- Define cyber-related terminology.
- Identify characteristics of cyber incidents.
- Explain the impacts of various cyber incidents.
- Discuss integrating cybersecurity into community preparedness.
- Explain the purpose of the Emergency Operations Center (EOC).
- Compare the organizational models of the EOC.

- Identify the functions within the EOC.
- Determine the integration of a cyber component within the EOC management structure.
- Discuss preparation methods that help protect organizations from cyber incidents.
- Explain activities that help the occurrence of a cyber incident.
- Describe response activities to cyber incidents.
- Describe actions that help an organization recover from cyber incidents.
- Interpret the Emergency Operations Center (EOC) management processes.
- Manage information to maintain internal EOC and external situational awareness.
- Mange the process for acquiring recourses.
- Mange the continual execution, evaluation and revision of the plan.

Target Participants:
- Emergency Management
- Information security and cybersecurity personnel
- Chief Information Officer
- Chief Information Security Officer
- Elected and/or appointed Officials
- Law Enforcement
- Fire Service
- Emergency Medical Services
- Public Health
- Public Works
- Hospital/Medical Centers
- Non-Governmental Organizations
- Transportation Authority
- Critical infrastructure representatives

POINT OF CONTACT:
For any further questions regarding the course, please contact Matt Miller.
Matt Miller:
Mobile: (972)322-7383
Email: matthew.miller@dal.frb.org