# Cybersecurity Incident Management and Response

MGTXXX

Course Design Document – ILT

*June, 2015*

FEMA

# Course Description

Cybersecurity has become one of the nation's most serious challenges today. However, the role of emergency managers in preventing, mitigating, and responding to a major cyber incident with physical consequences remains unclear. According to the U.S. Department of Homeland Security's 2013 *National Preparedness Report*, cybersecurity is still one of the lowest rated capabilities in the *State Preparedness Report*—and many states have reported that they do not expect to focus on building additional capacity in this field. This is despite the fact that findings from the Federal Emergency Management Agency's *National Level Exercise (NLE) 2012 Quick Look Report* pinpointed many areas for improvement specific to a cybersecurity that could adversely impact all levels of government.

This course is intended to be delivered across the country to jurisdictions at all response levels: local, state, tribal, territorial, as well as private industry.

## *Overview*

The threat of cyber incidents to our Nation's critical infrastructure is real and immediate. Computers and servers in the United States are the most aggressively targeted information systems in the world, with attacks increasing in severity, frequency, and sophistication each year. As information technologies continue to evolve and our nation's critical infrastructure grows more reliant on computer networks and information systems, it also becomes more susceptible to cyber incidents perpetrated by a wide array of actors, including criminal and terrorist organizations, both foreign and domestic. Through contact with professionals in the fields of emergency management and cyber security, the National Cybersecurity Preparedness Consortium has determined a need for this type of training course.

The *National Preparedness Report* (2013) identified that 73 percent of states and territories rated Infrastructure Systems as a high-priority capability, but it was among the 5 weakest capabilities that states and territories identified through the report. The after-action document prepared from the *National Level Exercise* (2012) identified that state, local, tribal, and territorial partners bear responsibility for securing their networks, but are unprepared to do so.

Traditionally, cybersecurity is the responsibility of each organization individually utilizing their own information security and technology personnel to manage threats. However, the physical consequences of a cyber incident are a shared responsibility that involves all levels of government, law enforcement, the private sector, and other "stakeholders." With this shared responsibility, there is a clear need to bring IT professionals and traditional emergency management personnel together to prepare for, respond to, and recover from the impacts of a cyber incident.

## *Scope*

This course is designed to assist jurisdictions with coordinating and managing response efforts between emergency response organizations and critical infrastructure information technology (IT) personnel necessary as a result of a cyber incident. The course will help to ensure that traditional emergency management personnel and IT personnel recognize the importance of working together to mitigate the effects of a cyber incident.

This course utilizes the Emergency Management Exercise System (EM*ES) incident simulation software which provides many features that resemble or imitate actual incident management systems.

## *Course Goal*

Upon successful completion of this course, participants will be able to initiate the coordination of IT personnel and emergency response personnel while managing response efforts to a cyber incident.

## *Target Audience*

This course was developed for personnel assigned to work in the jurisdiction's emergency operations center, policymakers, elected and/or appointed officials, emergency responders, IT and cybersecurity personnel and managers responsible for identifying and responding to cyber events for local government and private industry, and critical infrastructure representatives from both private and public entities.

## *Recommended Training*

Participants are expected to have successfully completed IS-100, IS-200, and IS-700.

Completion of IS-800 is also recommended. These courses can be found online at: http://training.fema.gov/IS/NIMS.asp.

*Cyber Incident Awareness Training* and *Emergency Management for IT Professionals* are also recommended, and can be found online at: http://www.nuarilearn.com/Pages/Home.aspx.

## *Course Length*

This course is 24 hours.