National Level Exercise (NLE) 2012

Overview for Northeast Disaster Recovery Information X-Change (NEDRIX)

March 14, 2012

FEMA

The Cyber Threat

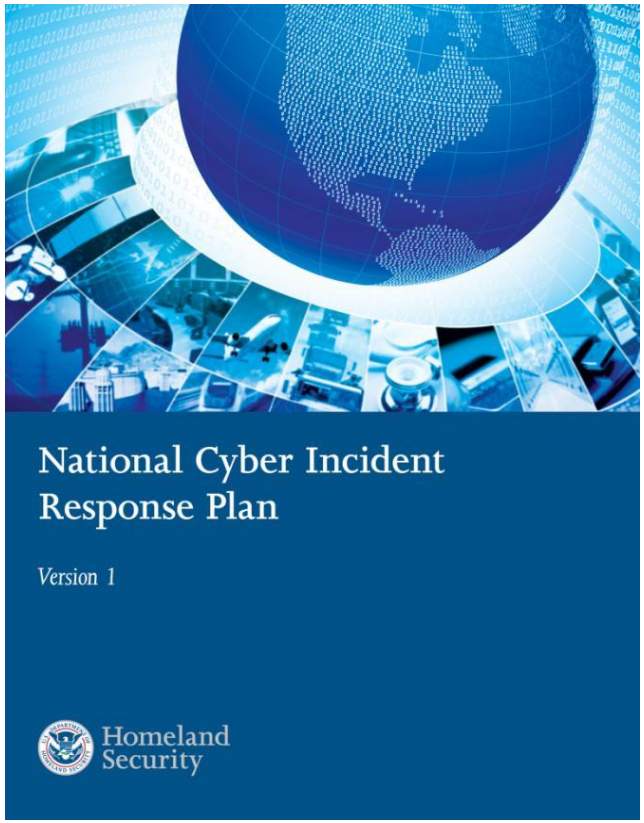
- Cyber threats to critical infrastructure and Federal systems are evolving and growing
  - Sources include criminals, foreign nations, hackers, and disgruntled employees
- Security incidents from Federal agencies increased over 650% over the past 5 years
  - Impact national and economic security
  - Loss of classified information and intellectual property worth millions of dollars
- In 2011, DHS responded to more than 106,000 incidents reported across the country

The "cyber threat is one of the most serious economic and national security challenges we face as a nation…America's economic prosperity in the 21st century will depend on cybersecurity." **President Barack Obama**

FEMA

Cybersecurity Initiatives

- White House Cyberspace Policy Review (May 2009)
  - Top-to-bottom review of U.S. government's efforts to defend information and communications infrastructure
  - Recommended development of a "cybersecurity incident response plan"
- National Cyber Incident Response Plan (NCIRP)
  - Provides a strategy for coordinating the operational response activities among:
    - Federal, state, local, tribal, and territorial governments
    - Private sector
    - International partners



Key Themes of the NCIRP

- Incident response in the cyber domain:
  - Often requires rapid response
  - Is dependent on private sector participation
  - Is highly dependent on the development of trusted relationships
- Incident response capabilities must be built on “steady state”
  - Cyber incidents happen every day
  - Need to build from “steady state” activities to maintain trust and coordination during a significant cyber incident
- The Federal Government and its partners must maintain the flexibility to adapt to rapidly evolving threats
  - No single agency has authority over all of cyberspace
  - The authorities and capabilities of multiple agencies may be needed for rapid, effective response
  - Synchronization of preparedness, planning, and operational response activities will be key to successful response efforts

NLE 2012 Overview

- **Cyber-centric:** the NLE 2012 process will examine the Nation's ability to coordinate and implement prevention, preparedness, response, and recovery plans and capabilities pertaining to a significant cybersecurity event or a series of related cybersecurity events.
- **Examining national plans:** NLE 2012 will also examine national response plans and procedures including the interim NCIRP and the National Response Framework (NRF).
- **NLE format:** NLE 2012 will include four national component exercises with common scenario elements, conducted from March-June 2012.
- **Exercise sensitivities:** uniqueness of topic presents challenges to exercise planners and opportunities for exploitation.

NLE 2012 Principal Objectives

- Examine the NCIRP in guiding the Nation to prepare for, respond to, and recover from a significant cyber event.
- Evaluate government (Federal; state, local, tribal, territorial [SLTT]; and international) roles and responsibilities in coordinating national cyber response efforts and their nexus with physical response efforts, including allocation of resources.
- Examine the ability to share information across all levels of government and with the private sector as well as the general public, to create and maintain cyber incident situational awareness, and coordinate response and recovery efforts.
- Assess key decision points and decision making in a significant cyber event.

FEMA

Source: *White House Memorandum from John O. Brennan, 1 October 2011*

NLE 2012 Scope

- Federal interagency
- Regional and state engagement
  - FEMA Regions: I, II, III, and V
  - States: Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, Vermont, New York, New Jersey, D.C., West Virginia, Michigan, Wisconsin, and Nevada (tribal representation)
- International: Australia, Canada, New Zealand, United Kingdom
- Private Sector
  - Critical Infrastructure (including the Sector Coordinating Councils and the Information Sharing and Analysis Centers)
  - Non-governmental organizations
  - Higher education
  - Others (drawing from Whole Community)

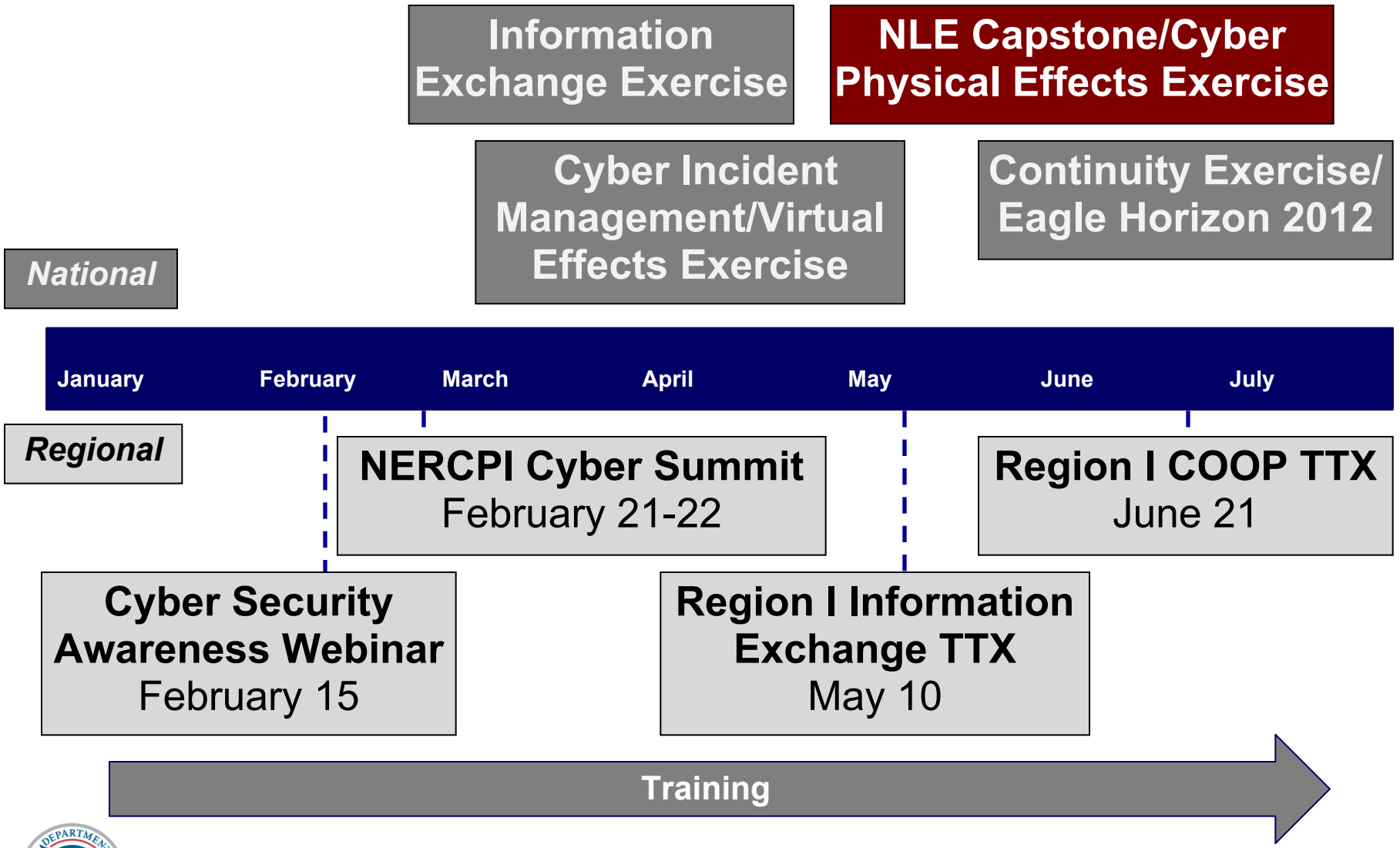
Scenario High-level Design Goals

- Project ambiguous threat landscape with multiple adversary types
- Include national security implications within scenario arc
- Produce physical impacts resulting from cyber attack and cascading effects
- Introduce conditions to stimulate Stafford Act discussions
- Affect critical commercial logistics and data, industrial control systems, and associated operations
- Utilize *"threat of…"* attacks to drive wide-ranging analysis, planning, and implementation of protective measures among public and private stakeholders
- Present conditions that demonstrate the need for timely decision making with respect to protective measures and cyber responses

National Exercise Components

	Exercise #1 **Information Exchange**	Exercise #2 **Cyber Incident Management/ Virtual Effects**	Exercise #3 **NLE Capstone/ Cyber Physical Effects**	Exercise #4 **Continuity Exercise/Eagle Horizon**
Target Dates	March	April	June	June
Locations	Arlington, VA	Greater DC area	Regions I, II, III, V, and the DC area	Distributed
Scope	■ Discussion-based ■ Cyber Unified Coordination Group ■ Cyber Operations Centers ■ TS/SCI	■ Discussion-based ■ Part I: National Tabletop Exercise (TTX) to examine NCIRP (**broad participation**) ■ Part II: Senior-Level Exercise	■ Operations-based ■ Whole Community ■ Simultaneous testing of NRF and NCIRP	■ Operations-based ■ Emergency Relocation Groups (Federal) ■ Selected regions and states
Focus Areas	■ Information exchange	■ The NCIRP at the operational level	■ Strategic decisions ■ Activation of operations centers ■ Operational decisions	■ Relocation ■ Devolution ■ Communications

Region I Timeline of Key Events



FEMA

NLE Capstone/Cyber Physical Effects

- **June 2012**
- **Purpose:** The NLE Capstone event will address cyber and physical response coordination, including resource allocation. Depending on dynamic exercise play and player action, the exercise may also allow policy makers the opportunity to review functions involving emergency assistance and disaster relief resources, relative to cyber event(s) with physical effects.
- **Scope:** The NLE Capstone event will ensure consequence management and larger Whole Community emergency management issues are examined during the exercise.
- **Objectives:**
  - Examine Whole Community cyber and physical response coordination, including resource allocation.
  - Examine strategies and operational capabilities and identify interdependencies between Federal Government and partners that are required to respond to and recover from the physical effects related to a cyber attack.

NLE Capstone: Region I Overview

- Connecticut
  - Communications focus
  - Mobile Emergency Response Support (MERS) deployment
- Maine
  - 3 days State Emergency Operations Center (EOC) play with three different areas of focus
    - Transportation
    - Water
    - Continuity of government
- Massachusetts
  - 3 full days State EOC play
  - Water and transportation sectors

NLE Capstone: Region I Overview (cont.)

- New Hampshire
  - 1 business day State EOC play
  - Water sector scenario focus
- Rhode Island
  - 3 full days State EOC play
  - Water and transportation sectors
- FEMA Region I
  - 3 full days Regional Response Coordination Center (RRCC) activation
  - Objectives focus on:
    - Examining cyber incident response plans
    - Support to affected states
    - Unified messaging
    - Communications

Region I Information Exchange TTX

- **May 10, 2012**
- **Purpose:** The TTX will examine how cyber threat and attack information is shared, with particular emphasis being placed on the involvement and roles of the private sector, given that a majority of cyber critical infrastructure falls under their purview. Participants will also analyze required cyber response actions.
- **Scope:** Participants will include organizations listed in regional and state cybersecurity and cyber incident response plans as well as entities that may be targeted.
- **Objectives:**
  - Examine the mechanisms for sharing actionable cyber intelligence information among regional, state, and local partners in the public and private sectors.
  - Discuss whether and how these mechanisms interact with, depend upon, and/or support national-level cyber intelligence sharing mechanisms.

Private Sector Participation Options

- Private Sector Participant Guide outlines opportunities to:
  - Engage virtually
  - Employ a downloadable TTX
  - Participate in training opportunities
- Appendix A of the guide contains participant registration form
- Information on NLE participation options and other information regarding NLE 2012 is found at www.fema.gov/plan/nle

Virtual Engagement

- Remote participation in NLE Capstone event
- Reduced resource commitment
- Follow the exercise via regular scenario and player action updates
- Opportunity to monitor exercise activities, resulting in the ability to better understand information sharing and exchange activities, as well as response and incident management activities
- Allows organization to consider impact on their own environment and take corresponding action at organizational level

Registration Required
Registration form in Appendix A of Private Sector Participant Guide
For more information contact: Private.SectorNLE@dhs.gov

FEMA

Downloadable TTX

- Part of the NLE exercise cycle is a downloadable TTX that will be available in late May
- Scaled down version of NLE 2012 for participation at organization's own schedule and pace
- Adaptable for use by all sizes of and all levels within a business or organization
- PowerPoint-based presentation with:
  - Embedded multimedia updates
  - Facilitator guidance and discussion questions
  - Training information
  - Exercise ground rules and proposed objectives
  - Scenario introductions and updates
  - Participant debriefing instructions
- For internal use only and will not be monitored; no registration required

Summary

- Cyber threat and plans
- NLE 2012 purpose and outcomes
- Region I events
- Participation options

NLE 2012 Contacts

FEMA/National Exercise Division

Nathan Rodgers
NLE 2012 Program Manager
Nathan.Rodgers@fema.dhs.gov

Shayleen Schutz
Region I Coordinator, NLE 2012 Support Team
Shayleen.Schutz@L-3com.com

FEMA Region I

Lauren DeMarco
Regional Exercise Manager/NLE Lead
Lauren.DeMarco@fema.dhs.gov

Chris Lynch
Regional Exercise Officer/Capstone Lead
Christopher.Lynch4@fema.dhs.gov

General Inquiries: NEP@dhs.gov

FEMA