



**FEMA**

# **National Level Exercise 2012**

## **Quick Look Report**

March 2013

This page is intentionally blank.

---

## DOCUMENT CONTROL

This document was produced by the U.S. Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA). For questions or more information regarding the enclosed content, please contact [NEP@fema.dhs.gov](mailto:NEP@fema.dhs.gov).

This page is intentionally blank.

## CONTENTS

<b>EXECUTIVE SUMMARY</b> .....	<b>1</b>
<b>EXERCISE DETAILS</b> .....	<b>3</b>
<b>EXERCISE OVERVIEW</b> .....	<b>5</b>
Exercise Objectives.....	5
Core Capabilities.....	6
Scenario.....	7
Participation.....	9
<b>PRELIMINARY OBSERVATIONS</b> .....	<b>11</b>
<b>WAY FORWARD</b> .....	<b>13</b>
<b>APPENDIX A: ACRONYM LIST</b> .....	<b>A-1</b>

This page is intentionally blank.

## EXECUTIVE SUMMARY

National Level Exercise (NLE) 2012 was a series of exercise events that examined the ability of the United States (U.S.) to execute a coordinated response to a series of significant cyber incidents. As a part of the National Exercise Program, NLE 2012 emphasized the shared responsibility among all levels of government, the private sector, and the international community to secure cyber networks and coordinate response and recovery actions. The NLE 2012 series was focused on examining four major themes: planning and implementation of the draft National Cyber Incident Response Plan (NCIRP), coordination among governmental entities, information sharing, and decision making.

NLE 2012 successfully highlighted the challenges in detecting, assessing, and responding to a significant cyber event and emphasized the critical importance of coordinating national and international response efforts. NLE 2012 also demonstrated the critical importance of integrating the private sector into decision making.

The exercise, however, drew attention to multiple areas requiring further improvement—which was expected. The cyber threat had not been previously exercised in such a comprehensive manner with such a broad range of stakeholders. The exercise scenario presented an advanced, multi-dimensional, sustained cyber attack against a wide range of critical Federal Government, state government, and private sector assets in multiple critical infrastructure sectors. By design, prevention of the attack was not an option. Participants had to figure out how to contain and stop the attack, as well as repair or restore damaged systems and data. They were confronted with these enormous response challenges while testing a relatively new plan (the draft NCIRP). Thus, the degree of difficulty confronting the exercise participants was significant—as it was designed to be. NLE 2012 pushed the system to the breaking point. Yet the areas identified for improvement that emerged from this challenging framework will, when successfully pursued, markedly enhance our national preparedness for a significant cyber incident.

### AREAS FOR IMPROVEMENT

- **Development of a Cyber Common Operational Picture (COP).** Exercise participants had a difficult time ascertaining accurate situational awareness of the developing cyber situation and the resultant cyber and physical impacts throughout the Whole Community. Major contributing factors included the lack of consistent information sharing among Federal cyber centers and confusion regarding cyber incident reporting requirements (i.e., what to report to whom regarding the status of organizational network degradations and cyber challenges, respectively, across Federal departments and agencies [D/As], other levels of government, and other partners).

- **NCIRP Revision.** The exercise exposed a number of areas within the draft NCIRP that require examining, to include the following:
  - **National Cyber Risk Alert Level (NCRAL).** The NCRAL was not well understood by most of the exercise participants and therefore, implications of changing the NCRAL were largely unknown.
  - **Roles and Responsibilities.** Exercise participants expressed uncertainty regarding membership, membership roles, responsibilities, and other expectations of the National Cybersecurity and Communications Integration Center (NCCIC), the staff and senior levels of the Unified Coordination Group (UCG), the Domestic Resilience Group (DRG), the Cyber Response Group (CRG), law enforcement, and private sector owners and operators of critical infrastructure.
  - **National Mitigation and Resources.** Exercise participants, particularly at the Federal level, were unable to generate a viable, prioritized Incident Action Plan (IAP) in response to the exercise scenario. Participants were also unfamiliar with available cyber response resources and were unable to provide or procure the necessary technical resources being requested by Federal D/As and states. Additionally, questions remain about how private sector resources will be integrated into Federal efforts.
- **Authorities and Associated Courses of Action.** NLE participants require further clarification of relevant authorities and their application, especially those that may support or otherwise impact states and the private sector. Such authorities include the Robert T. Stafford Disaster Relief and Emergency Assistance Act (determining what elements of a cyber incident might meet standards for obtaining such Federal assistance) and the Defense Production Act (implementation processes and requirements for applying the Act while also recognizing private sector reservations).
- **Decision-Making Processes.** The highly deliberative and time-consuming decision-making processes used by the Federal Government during the exercise series ran counter to the need to make decisions quickly as the event escalated. The various leadership forums became too focused on tactical and operational details without arriving at timely decisions.

Ultimately, NLE 2012 confirmed what many exercise stakeholders had long suspected: that an advanced cyber threat is menacing and, when realized, presents debilitating and cascading effects across a range of critical functions and assets. Our collective proficiency with our existing cyber response plans—as well as the plans themselves—require additional work and diligence.

## EXERCISE DETAILS

**Exercise Name:** National Level Exercise 2012

### Component Exercises:

Exercise	Name	Type	Dates
Exercise #1	Information Exchange	Tabletop	March 28-29, 2012
Exercise #2	Cyber Incident Management/Virtual Effects	Tabletop	April 25-27, 2012
Exercise #3	NLE Capstone/Cyber Physical Effects	Functional	June 4-7, 2012
Exercise #4	Continuity Exercise/Eagle Horizon	Full-scale	June 19-21, 2012

**Sponsor:** U.S. Department of Homeland Security

**Program:** National Exercise Program and National Continuity Program

### Core Capabilities and Mission Areas:

Core Capability	Mission Areas
Cybersecurity	Protection
Intelligence and Information Sharing	Prevention, Protection
Operational Communications	Response
Operational Coordination	Prevention, Protection, Mitigation, Response, Recovery
Public Information and Warning	Prevention, Protection, Mitigation, Response, Recovery
Situational Assessment	Response

**Scenario Type:** Multi-vector cyber intrusion, exfiltration, and disruption campaign that exposed vulnerabilities and produced both electronic and physical damage to government networks, critical infrastructure, and transportation assets and systems.

This page is intentionally blank.

## EXERCISE OVERVIEW

The purpose of NLE 2012 was to examine the Nation's ability to coordinate and implement prevention, preparedness, response, and recovery plans and capabilities pertaining to a series of significant cyber events. NLE 2012 examined national response plans and procedures including the draft NCIRP, the National Response Framework (NRF), and the NRF Cyber Incident Annex through the conduct of four distinct exercises. NLE 2012 included participation from all levels of government, the private sector, academia, international partners, and non-governmental organizations. The National Security Staff (NSS) and DHS/FEMA/National Exercise Division planned NLE 2012 with input from participating Federal, state, international, and private sector planners.

### EXERCISE OBJECTIVES

The NLE 2012 process was guided by a set of overarching objectives (known as Principal Objectives) as established by the White House/NSS. The NLE 2012 Principal Objectives applied to all NLE 2012 supporting events, exercises, and training activities and continue to serve as the focus of exercise evaluation efforts. The NLE 2012 Principal Objectives include the following:

- Examine the [draft] NCIRP in guiding the Nation to prepare for, respond to, and recover from a significant cyber event.
- Evaluate government (Federal, state, local, tribal, territorial, 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 (classified and unclassified) 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.

In addition to the Principal Objectives, the NLE 2012 process was also guided by general objectives for each of the four NLE 2012 exercises. These objectives are listed below:

#### **Exercise #1: Information Exchange**

- Demonstrate the ability to share actionable and relevant classified and unclassified information among the relevant stakeholders.
- Examine the mechanisms for sharing actionable cyber intelligence information.

**Exercise #2: Cyber Incident Management/Virtual Effects**

- Examine the Nation's response to a significant cyber event, including evaluation of the [draft] NCIRP.
- Demonstrate the Nation's ability to respond to a significant cyber event, to include exercising the coordination, authorities, responsibilities, and operational capabilities among governmental entities and the private sector.

**Exercise #3: NLE Capstone/Cyber Physical Effects**

- Examine Whole Community cyber and physical response coordination, including resource allocation.
- Assess strategies and operational capabilities and identify interdependencies between government and the private sector that are required to protect critical infrastructure.

**Exercise #4: Continuity Exercise/Eagle Horizon**

- Evaluate the continuity capability of D/As, including the performance of essential functions, during a significant national cyber event in accordance with continuity directives.
- Examine and test public communications capability redundancies and the continuity of social media during a significant cyber event.

**CORE CAPABILITIES**

The NLE 2012 evaluation effort has linked the Principal Objectives and general objectives to six core capabilities (please refer to the National Preparedness Goal for definitions of each core capability):

- Cybersecurity;
- Intelligence and Information Sharing;
- Operational Communications;
- Operational Coordination;
- Public Information and Warning; and
- Situational Assessment.

## SCENARIO

The NLE 2012 scenario backstory centered on Nation State X (NS-X). NS-X sought to erode the public's trust in their security and safety and cause impacts to the U.S. economy by disrupting critical infrastructure networks and information technology infrastructures, logistics systems, and the communications capabilities of U.S. Federal and state agencies. Towards this goal, NS-X launched a campaign that included a series of carefully orchestrated and coordinated activities and components. The campaign resulted in vulnerabilities in network interface cards, embedded network communications devices, and supervisory control and data acquisition networks. Not only did the campaign exploit these vulnerabilities in attacks against critical infrastructure networks, but it also released a combination of botnets and remote access tool programs that caused a disruption of communications, loss of data, and the unavailability of certain key services.

In Exercise #1, the participants confronted the indications and warning phase of the cyber campaign, focusing primarily on the adversaries' theft of identification and other credentials, and the compromise of an information technology sector manufacturing process—tactics that were used to gain access to the targeted networks and systems. In Exercise #2, the looming threat of the adversaries' planned attacks was discovered by the participants. Exercise #3 opened with multiple, targeted attacks on U.S. government network infrastructures, as well as water and transportation systems, thus establishing that the full cyber campaign was underway. In response to this scenario, participants implemented various response actions over the course of the exercise to include the following:

- Federal D/As, states, and the private sector took actions to respond to the impacts on their respective affected systems.
- The NCCIC developed and disseminated Situation Reports (SITREPs), conducted Cyber UCG meetings, and established Incident Management Teams (IMT) to address legal authorities, mitigation strategies, resources, and public messaging.
- The CRG and DRG conducted joint meetings, and both the Homeland Security Council Deputies Committee and the President's Cabinet met to discuss policy issues and make decisions on options raised by the Cyber UCG.
- Cyber entities raised alert levels. For example, the Multi-State and Financial Services Information Sharing and Analysis Centers (ISACs) raised their cyber alert levels and DHS raised the NCRAL from "Guarded" to "Severe."
- FEMA deployed a senior liaison officer to the NCCIC on June 4, 2012. After an initial Level 3 activation for communication checks, the Agency activated the National Response Coordination Center to Level 1 on June 7, 2012 in response to the physical

effects from the cyber incident. FEMA also deployed state liaison officers to affected states.

- Massachusetts, New Jersey, Wisconsin, and Rhode Island declared a State of Emergency and some requested assistance through the Stafford Act. Of those, Massachusetts was granted an Emergency Declaration. The assistance was provided for physical consequences of the cyber attacks (e.g., Massachusetts was granted assistance to address requirements for potable water and firefighting water supply after cyber attacks on water systems) but not for efforts to assess or repair networks and control systems, or defend them from continued or future cyber attacks.
- The National Joint Information Center (NJIC) developed coordinated internal and external messages on the incident and communicated throughout the exercise with state, regional, and private sector partners with periodic National Incident Communications Conference Line, State Incident Communications Coordination Line, and Public Information Communication Coordination Line calls. NJIC participants actively participated in Cyber UCG deliberations.
- The Federal Government communicated and coordinated with the private sector through the ISACs, Cyber UCG meetings, and the National Infrastructure Coordination Center.

## PARTICIPATION

Participation in NLE 2012 events spanned across many Federal D/As, FEMA Regions, state and territorial governments, private sector organizations, and international partners.

- **Exercise #1:** Phase 1 included players from various Federal cyber centers including the NCCIC and the U.S. Computer Emergency Readiness Team (US-CERT). Phase 2 included those participants in Phase 1 with additional representatives from international partners (Australia, Canada, New Zealand, and the United Kingdom), the private sector, state governments (New Hampshire, Rhode Island, and Wisconsin), and four other Federal D/As.
- **Exercise #2:** The National Tabletop Exercise participants included representatives from the various Federal cyber centers, 21 Federal D/As, three international partner nations, eight states, and FEMA Region I. The private sector included representatives from eight ISACs, the American Red Cross, the Business Emergency Operations Center Alliance, eleven Sector Coordinating Councils, and the Southeastern Emergency Response Network. The Deputies Committee portion of Exercise #2 included the deputy secretaries from Cabinet D/As.
- **Exercise #3:** The NLE Capstone included participation from approximately 36 Federal D/As in addition to participants from FEMA Regions I, II, III, and V; ten states; the private sector; higher education institutions; and international partners. There were approximately 130 exercise play sites between the National Capital Region and various locations across the United States. Exercise #3 also included a Cabinet meeting.
- **Exercise #4:** All D/As were mandated to participate in the Eagle Horizon Continuity of Operations exercise. However, only Category I and Category II D/As, as listed in the National Security Presidential Directive 51/Homeland Security Presidential Directive 20, National Continuity Policy, were mandated to participate in the devolution portion. A total of 64 D/As participated on the first day of the exercise. In addition, several states participated in Exercise #4.

This page is intentionally blank.

## PRELIMINARY OBSERVATIONS

In order to document play and collect data, exercise evaluators observed the exercises and collected player feedback through post-exercise meetings, feedback forms, and other documentation. An initial review of issues highlighted by players and evaluators is shown below in Table 1.

**Table 1: Preliminary Observations**

<b>Cybersecurity</b>
<b>Areas for Improvement</b>
Under the circumstances presented in the NLE, the Federal Government was able to identify the legal authority to seek a court order to block the malware attacks, but this legal authority may not apply to all future malware attacks.
Under the specific conditions presented during the NLE, the Federal Government identified potential theories upon which certain private sector entities could be protected from civil liability pursuant to statute for certain remedial actions undertaken pursuant to a court order, though the private sector expressed reservations about this effort.
There was a lack of clarity on when and how Stafford Act authorities could be used in response to a significant cyber incident.
Exercise participants lacked familiarity with implementation processes and plans for specific application of the Defense Production Act to a cyber incident.
Exercise participants, particularly at the Federal level, were unable to generate a viable, prioritized IAP in response to the exercise scenario. Additionally, exercise participants were generally unable to provide or procure the necessary technical resources being requested by Federal D/As and states.
<b>Intelligence and Information Sharing</b>
<b>Areas for Improvement</b>
There was generally a lack of consensus regarding cyber threat and vulnerability information that should be shared between the public and private sectors.
Existing processes for downgrading or “tear-lining” classified information, removing handling restrictions, and resolving competing equities of the involved D/As may impede timely information sharing.
Not all incidents experienced by Federal D/As were reflected in NCCIC SITREPs, and the current manual reporting system for developing the cyber COP is not fast enough to provide real-time situational awareness for cyber events.
<b>Operational Communications</b>
<b>Areas for Improvement</b>
Exercise #4 revealed bottlenecks in the operation of DHS Public Affairs’ coordination calls in a degraded communications environment.

<b>Operational Coordination</b>
<b>Areas for Improvement</b>
The draft NCIRP lacks depth and detail regarding formation of Cyber UCG IMTs and also lacks depth and detail regarding descriptions of responding organizations, their functions, and actions relevant to a national response to a cyber event.
The NCRAL does not provide sufficient information on needed actions by Federal D/As, state and local governments, critical infrastructure entities, the private sector, and the public.
Exercise participants, particularly at the Federal level, did not demonstrate shared awareness of cyber-specific technical resources or the ability to provide them to those requesting assistance. The exercise validated the need for a catalog of cyber resource types and quantities as well as processes to support resource requests, prioritization, allocation, and deployment.
The multiple layers of coordination for cyber incidents confused participants and contributed to slow decision-making relative to the speed of the evolving cyber campaign.
The draft NCIRP does not resolve overlapping Federal responsibilities for private sector coordination during a cyber incident.
The respective roles of NCCIC and US-CERT remained unclear to many participants.
<b>Public Information and Warning</b>
<b>Areas for Improvement</b>
Coordination of mitigation actions with public information officers was not sufficient to ensure timely public messaging.
Exercise participants struggled with the utility and implications of the NCRAL for public messaging.
Operational coordination and public communications planning did not fully address international coordination requirements.
<b>Situational Assessment</b>
<b>Areas for Improvement</b>
The frequency and distribution of NCCIC products did not meet some recipients' expectations for a cyber COP.
The NCCIC and its partners in the Cyber UCG struggled to analyze and connect multiple "steady state" incidents as indicators. Many NLE 2012 participants had difficulty ascertaining accurate situational awareness of the developing cyber situation and the resultant cyber and physical impacts. Major contributing factors included the lack of consistent information sharing among the seven cyber centers and the lack of (and confusion regarding) cyber incident reporting requirements (i.e., what to report to whom regarding the status of organizational network degradations and cyber challenges, respectively, across Federal D/As, other levels of government, and other partners).

## WAY FORWARD

The NLE 2012 process includes an extensive evaluation and improvement planning phase. This phase involves all stakeholders involved in the NLE and additional organizations as needed to ensure corrective actions are identified and completed. FEMA and its partners will continue to champion the NLE after-action process in the unified effort to enhance national cyber response capabilities.

This page is intentionally blank.

## APPENDIX A: ACRONYM LIST

COP	Common Operational Picture
CRG	Cyber Response Group
D/As	Departments and Agencies
DHS	Department of Homeland Security
DRG	Domestic Resilience Group
FEMA	Federal Emergency Management Agency
IAP	Incident Action Plan
IMT	Incident Management Team
ISAC	Information Sharing and Analysis Center
NCCIC	National Cybersecurity and Communication Integration Center
NCIRP	National Cyber Incident Response Plan
NCRAL	National Cyber Response Alert Level
NJIC	National Joint Information Center
NLE	National Level Exercise
NRF	National Response Framework
NSS	National Security Staff
NS-X	Nation State X
SITREP	Situation Report
UCG	Unified Coordination Group
U.S.	United States
US-CERT	U.S. Computer Emergency Readiness Team

This page is intentionally blank.