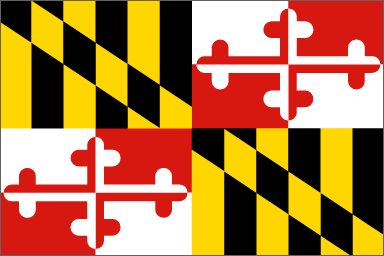
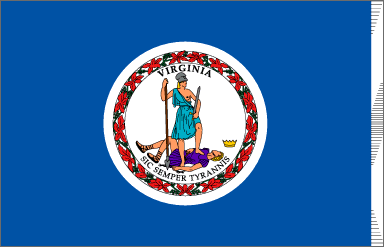
**** **Operation Rankl3 th3 R$ch**



**2013 National Capital Region**

**EPC Senior Leader Seminar**

**General Overview**

****



**November 1, 2013**

# Seminar Overview

|  |  |  |
| --- | --- | --- |
| **Seminar Name** | 2013 National Capital Region (NCR) Emergency Preparedness Council (EPC) Senior Leader Seminar (SLS) | |
| **Seminar Date** | November 1, 2013 | |
| **Scope** | This seminar is a facilitated, tabletop discussion, planned for four hours at the Convention Center, Washington, D.C. The seminar will raise awareness of cyber risk management, cyber-related information and intelligence-sharing and other issues related to cyber incident prevention, protection, mitigation and response. | |
| **Mission Area(s)** | Cyber Incident Prevention, Protection, Mitigation and Response | |
| **Objectives** | OBJECTIVES:   1. Provide cybersecurity awareness by informing NCR leadership on existing strategic cybersecurity doctrine during a 4-hour seminar geared towards prevention, protection, mitigation and response 2. During this seminar, determine the cyber-related information and intelligence sharing mechanisms in the NCR 3. During this seminar, identify cybersecurity escalation criteria and potential courses of action by NCR jurisdiction members 4. By means of this seminar, develop an annotated outline for use in the development of a Strategic National Capital Region Cyber Coordination Framework designed to assist with coordination of a regional, broad-based approach to cyber incidents | |
| **Threat or Hazard** | Cyber Attack | |
| **Scenario** | In conjunction with physical protests occurring throughout the NCR, a hacktivist group plans to conduct cyber operations against NCR governments in support of the physical protests. | |
| **Sponsor** | Metropolitan Washington Council of Governments (MWCOG) | |
| **Participating Organizations** | Departments and Agencies from the MWCOG Member Jurisdictions | |
| **Points of Contact** | **Steve Bieber**  Metropolitan Washington Council of Governments  777 North Capitol Street, N.E.  Suite 300  Washington, DC 20002-4239  (202) 962-3219  [sbieber@mwcog.org](mailto:sbieber@mwcog.org)  **Dave McMillion**  Metropolitan Washington Council of Governments  777 North Capitol Street, N.E.  Suite 300  Washington, DC 20002-4239  (202) 962-3708  [dmcmillion@mwcog.org](mailto:dmcmillion@mwcog.org) | **Jennine Gilbeau**  DHS National Cybersecurity and Communications Integration Center (NCCIC)  Operational Planning, Exercise, and Training Integration Unit  (703) 235-5271  [jennine.gilbeau@hq.dhs.gov](mailto:jennine.gilbeau@hq.dhs.gov)  **DHS Cyber Exercise Program**  (703) 235-3025  [CEP@hq.dhs.gov](mailto:CEP@hq.dhs.gov) |

# General Information

## Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the seminar. Groups of participants involved in the seminar, and their respective roles and responsibilities, are as follows:

* **Players.** Players are personnel who have an active role in discussing or performing their regular roles and responsibilities during the seminar. Players discuss or initiate actions in response to the simulated emergency.
* **Observers.** Observers do not directly participate in the seminar. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.
* **Facilitators.** Facilitators provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Seminar Planning Team members may also assist with facilitation as subject matter experts (SMEs) during the seminar.
* **Evaluators.** Evaluators are assigned to observe and document certain objectives during the seminar. Their primary role is to document player discussions, including how and if those discussions conform to plans, polices, and procedures.

## Seminar Structure

The regional Senior Leader Seminar is intended to provide the impetus and focus for a Strategic NCR Cyber Coordination Framework. It is envisioned that the Framework will be focused on the following core elements:

1. Assessment
2. Prevention and Preparedness
3. Protection and Information Sharing
4. Regional Response

This seminar will be a multimedia, facilitated, tabletop discussion. Players will participate in the following two modules:

* Module 1: Disruption
* Facilitated jurisdiction-specific discussion
* Facilitated plenary discussion
* Module 2: Cyber Attacks Begin and Escalate
* Facilitated jurisdiction-specific discussion
* Facilitated plenary discussion

Each module begins with a multimedia update that summarizes key events occurring within that time period. After the updates, participants will break out into jurisdiction-specific groups to discuss issues specific to their jurisdictions and how those issues may impact the region. Following this, a facilitated plenary discussion will focus all jurisdictions on developing key points of a Strategic National Capital Region Cyber Coordination Framework.

## Seminar Guidelines

* This Seminar will be held in an open, low-stress, no-fault environment. Varying viewpoints, even disagreements, are expected.
* Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.
* Decisions are not precedent setting and may not reflect your organization’s final position on a given issue. This seminar is an opportunity to discuss and present multiple options and possible solutions.
* Assume cooperation and support from other responders, agencies, and jurisdictions.
* Issue identification is not as valuable as suggestions and recommended actions that could improve prevention, protection, mitigation, response, and other efforts. Problem-solving efforts should be the focus.
* Situation updates, written materials, and resources provided are the basis for discussion; there are no situational or surprise injects.

## Seminar Assumptions and Artificialities

In any seminar, assumptions and artificialities may be necessary to complete play in the time allotted and/or account for logistical limitations. Participants should accept that assumptions and artificialities are inherent in any seminar, and should not allow these considerations to negatively impact their participation. During this seminar, the following apply:

* The seminar is conducted in a no-fault learning environment wherein capabilities, plans, systems, and processes will be evaluated.
* There is no “hidden agenda” nor are there any trick questions.
* The seminar scenario is plausible, and events occur as they are presented.
* All players receive information at the same time.
* The scenario is not derived from current intelligence.

## Seminar Evaluation

Evaluation of the seminar is based on the seminar objectives and aligned capabilities. Players will be asked to complete participant feedback forms. These documents, coupled with facilitator observations and notes, will be used to evaluate the seminar and compile the After-Action Report.