Lesson 11 Outline

Course Number: XXXX

Course: Foundations of Critical Infrastructure Security and Resilience

University of XXXXXX

Fall/Spring Semester 20XX

LESSON 11 TOPIC: MANAGING IMPACTS TO CRITICAL INFRASTRUCTURE IN AN ALL-HAZARDS ENVIRONMENT

****Special Activity**: **Incident Management Exercise Preparation**. Today's class involves a conceptual "walk-through" of the next lesson's interactive, discussion-based table top exercise (TTX) driven by a terrorism- or major hurricane-based scenario. This lesson will focus on gaining an understanding of the National Incident Management System (NIMS) and the National Response Framework (NRF) as they apply to CISR in the context of incident management. This lesson will also explore the relationship between the NIPP and the NRF in detail, including an examination of how the public and private sectors share information, maintain situational awareness, and provide assistance to one another during all-hazards emergencies. The discussion will focus on the roles, responsibilities, and interaction between FSLTT governments; the private sector; and the general public in the context of an emergent threat as well as an incident in progress. Participant discussion will focus on communication and information sharing, coordination, integration of capabilities, and problem identification and resolution.

1. Lesson Goals/Objectives:

- Identify and evaluate the processes and mechanisms used to build situational awareness and facilitate government-private critical infrastructure-related emergent threat and incident response coordination and information sharing among the various NIPP partners.
- Identify and understand critical infrastructure security laws, policies, and programs with application to the management of emergent threats and incidents.

2. Discussion Topics:

- What are the key government and private sector incident management nodes according to the NIPP, the NRF, and the National Prevention Framework (NPF)?
- What are the roles and responsibilities of the various NIPP partners vis-à-vis national incident management? What are their major needs?
- How is the CISR mission area addressed in the NRF and NPF?
- What are the principal elements of the Critical Infrastructure Support Annex to the NRF? How do they work?
- How are information and intelligence shared between the various public and private sector nodes of the NIPP Partnership Framework in an emergent threat scenario? During an incident in progress? Does the process work? How could it be

improved?

- What actions do the sectors take in response to an emergent threat or National Terrorist Advisory System (NTAS) elevation? What are the near and long term ramifications across the sectors?
- How is situational awareness maintained among the various NIPP partners during incident response?
- How are private sector requests for assistance assessed and addressed during incident response operations?

3. Required Reading:

Review the NIPP 2013 Partnership and Risk Management Framework, http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508.pdf.

U.S.Department of Homeland Security, "National Terrorism Advisory System," http://www.dhs.gov/files/programs/ntas.shtm.

U.S. Department of Homeland Security, National Response Framework, CIKR Support Annex, May2013, http://www.fema.gov/media-library-data/20130726-1914-25045-5422/nrf_support_annex_cikr_20130505.pdf

U.S. Department of Homeland Security, *National Prevention Framework*, May 2013, http://www.fema.gov/media-library-data/20130726-1913-25045-6071/final_national_prevention_framework_20130501.pdf

U.S. Department of Homeland Security, *National Response Framework*, 2013, http://www.fema.gov/media-library/assets/documents/32230?id=7371http://www.fema.gov/media-library-data/20130726-1914-25045-1246/final_national_response_framework_20130501.pdf.

4. Additional Recommended Reading:

U.S. Department of Homeland Security, *Overview of the National Planning Frameworks*, (May 2013). http://www.fema.gov/media-library-data/20130726-1914-25045-2057/final_overview_of_national_planning_frameworks_20130501.pdf.

https://www.fema.gov/national-incident-management-system

Framework for Dealing with Disasters and Related Interdependencies, July 2009, http://www.dhs.gov/xlibrary/assets/niac/niac_framework_dealing_with_disasters.pdf.

Foundations of Critical Infrastructure Security and Resilience

Lesson 11: Managing Impacts to Critical Infrastructure in an All-Hazards Environment

Lesson 11 Objectives

- Identify and evaluate the processes and mechanisms used to build situational awareness and facilitate government-private critical infrastructure-related emergent threat and incident response coordination and information sharing among the various NIPP partners.

- Identify and understand critical infrastructure security laws, policies, and programs with application to the management of emergent threats and incidents.

Special Activity

- This lesson will:
  - promote an understanding of the NIMS, the NPF, and the NRF as they apply to CISR in the context of incident management.
  - focus on the roles, responsibilities, and interaction between FSLTT governments and the private sector in the context of an emergent threat as well as an incident in progress.
  - include an examination of how the public and private sectors share information, maintain situational awareness, and provide assistance to one another during all-hazards emergencies.

PPD-8 Review: The CISR Nexus

- National Preparedness Goal
- National Preparedness System
- National Mission Area Frameworks
  - Prevention
  - Protection
  - Mitigation
  - Response
  - Recovery
- Federal Interagency Operational Plans
- How does CISR fit into the PPD-8 schemata?

PPD-8 Core Capability: Infrastructure Systems

Objective: Stabilize critical infrastructure functions, minimize health and safety threats, and efficiently restore and revitalize systems and services to support a viable, resilient community.

- **Critical Tasks:**
  - Decrease and stabilize immediate infrastructure threats to the affected population, to include survivors in the heavily-damaged zone, nearby communities that may be affected by cascading effects, and mass care support facilities and evacuation processing centers with a focus on life-sustainment and congregate care services.
  - Re-establish critical infrastructure within the affected areas to support ongoing emergency response operations, life sustainment, community functionality, and a transition to recovery.

National Prevention Framework Overview

- The National Prevention Framework describes what the whole community—from community members to senior leaders in government—should do upon the discovery of intelligence or information regarding an imminent threat to the homeland in order to thwart an initial or follow-on terrorist attack.

- NPF Nation-level coordinating structures: DHS National Operations Center (NOC), FBI Strategic Information and Operations Center (SIOC), Office of the Director of National Intelligence (ODNI) National Counterterrorism Center (NCTC), DoD National Military Command Center (NMCC), FBI National Joint Terrorism Task Force (NJTTF), and others.

- NPF field coordinating structures: FBI JTTFs and Field Intelligence Groups (FIGs); state and major urban area fusion centers; state and local counterterrorism and intelligence units; and others.

National Response Framework Overview

- The NRF is a guide to how the Nation responds to all types of disasters and emergencies.
- Describes specific authorities and best practices for managing incidents that range from the serious but purely local to large-scale terrorist attacks or catastrophic natural disasters.
- Defines scalable, flexible, and adaptable coordinating structures based on the NIMS, as well as key roles and responsibilities for integrating capabilities across the whole community, to support the efforts of local, state, tribal, territorial, insular area, and Federal governments in responding to actual and potential incidents.
- Composed of a base document, Emergency Support Function (ESF) Annexes, Support Annexes, and Incident Annexes.

NRF: Incident Roles & Responsibilities

- Federal Authorities
  - Stafford Act & non-Stafford Act; Federal-to-Federal Support; Inherent Federal Authorities
- SLTT Authorities
- Private Sector
  - CI owners/operators; responsible parties; commercial businesses
  - Nongovernmental Organizations
- Communities

NRF: Coordination Structures & Operational Nodes

- Private Sector
- Local
- State
- Federal
- ESFs + EOCs + MACCs at all levels

NRF Critical Infrastructure Support Annex

- Purpose: describes policies, roles and responsibilities, and the concept of operations for assessing, prioritizing, protecting, and restoring critical infrastructure (CI) during actual or potential domestic incidents.

NRF Critical Infrastructure Support Annex

- Describes roles and responsibilities for CI protection, response, recovery, restoration, and continuity of operations relative to NRF coordinating structures and NIMS guiding principles.
- Establishes a concept of operations for incident-related CI protection, response, recovery, and restoration.
- Outlines incident-related actions (including pre-response and post-response) to expedite information sharing and analysis of actual or potential impacts to CI and facilitate requests for assistance and information from public- and private sector partners.

NRF CI Support Annex CONOPS

- Describes specific organizational approaches, processes, coordinating structures, and incident-related actions required for the protection and restoration of CIKR assets, systems, networks, or functions within the impacted area and outside the impacted area at the local, regional, and national levels.

- The CONOPS uses the organizational structures and info-sharing mechanisms established in the NIPP and describes protocols to integrate these steady-state organizational elements with NRF incident management organizational structures and activities.

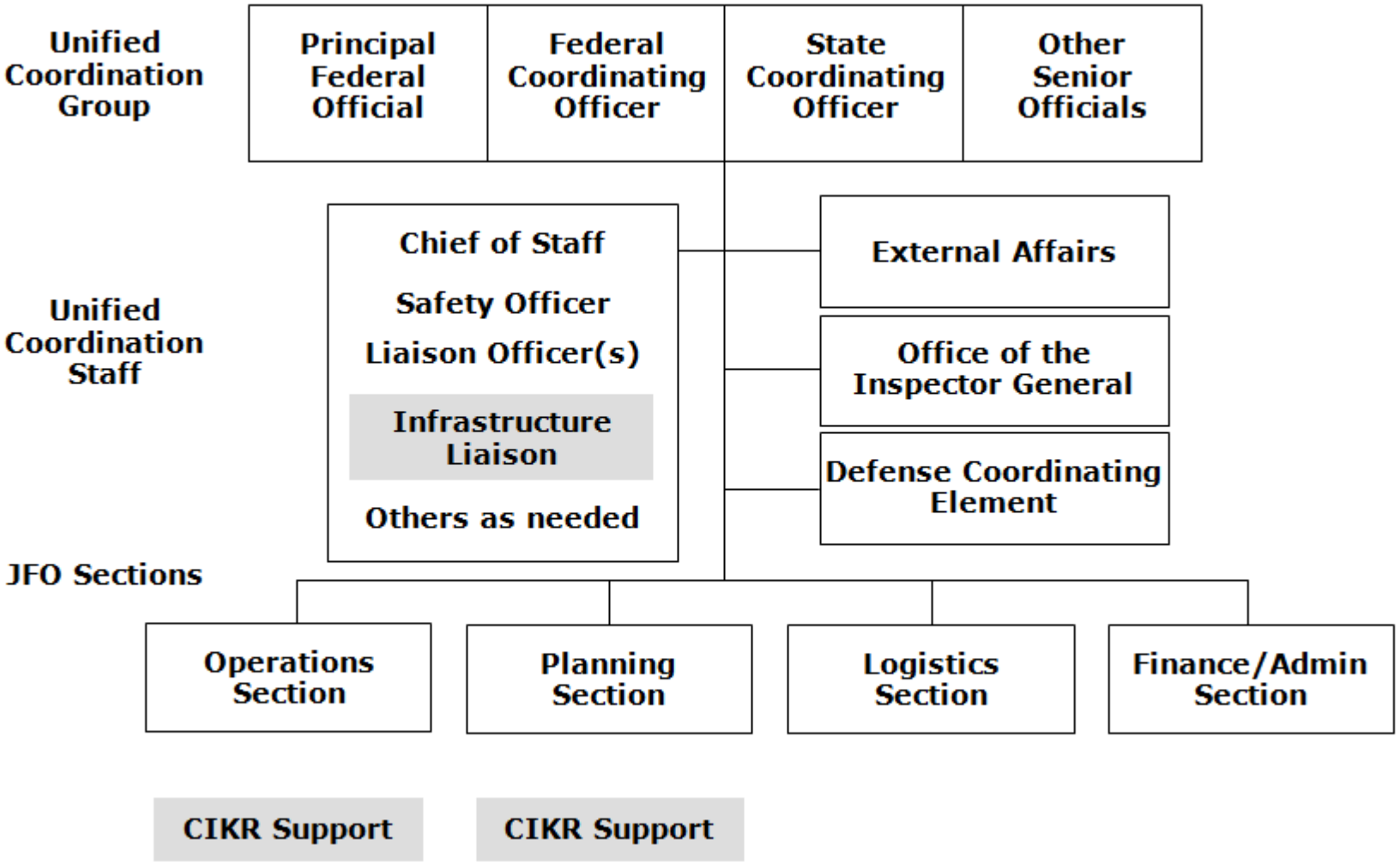
NRF CI Support Annex CONOPS

- Core Elements:
  - Situational awareness.
  - Impact assessments and analysis.
  - Information sharing.
  - Requests for assistance or information from private sector CIKR owners and operators.

NRF CI Support Annex CONOPS

- Coordination/Information Sharing Nodes
  - National Level: NOC, NRCC, NICC, NCCIC, SIOC, Federal EOCs
  - SLTT Level: EOCs, MACCs, Fusion Centers
  - Private Sector: ISACs, Business EOCs, Corporate and Facility EOCs
  - Field Level Coordination: JFO, SLTT EOCs, Fusion Centers, DHS Infrastructure Liaisons

Field Organization



Infrastructure Liaisons

- Advise the Unified Coordination Group on CI issues with national or regional implications or that involve multiple CIKR sectors.
- Act as coordination point for CI sectors, including private sector owners and operators that are not otherwise represented in the JFO.
- Serve as the senior advocate in the Unified Coordination Staff for CI issues not otherwise raised through the UCG.
- Advise the UCG regarding the prioritization of CI protection and restoration issues.
- Provide additional coordination and liaison capabilities to the CI sectors for the UCG in addition to the coordination and liaison functions provided by the various ESFs.
- Work with the JFO Section Chiefs and Branch Directors to coordinate between and among CIKR sectors and ESFs.
- Ensure that information obtained from the NICC and CIKR sectors is integrated into the overall COP for the incident.

Incident Response Actions

- Steady-state Situational Awareness & Reporting
- Alerts & Warnings
- Incident Notification
- Ongoing Situational Awareness & Reporting
- Assessment & Analysis
- Response Coordination & Assistance

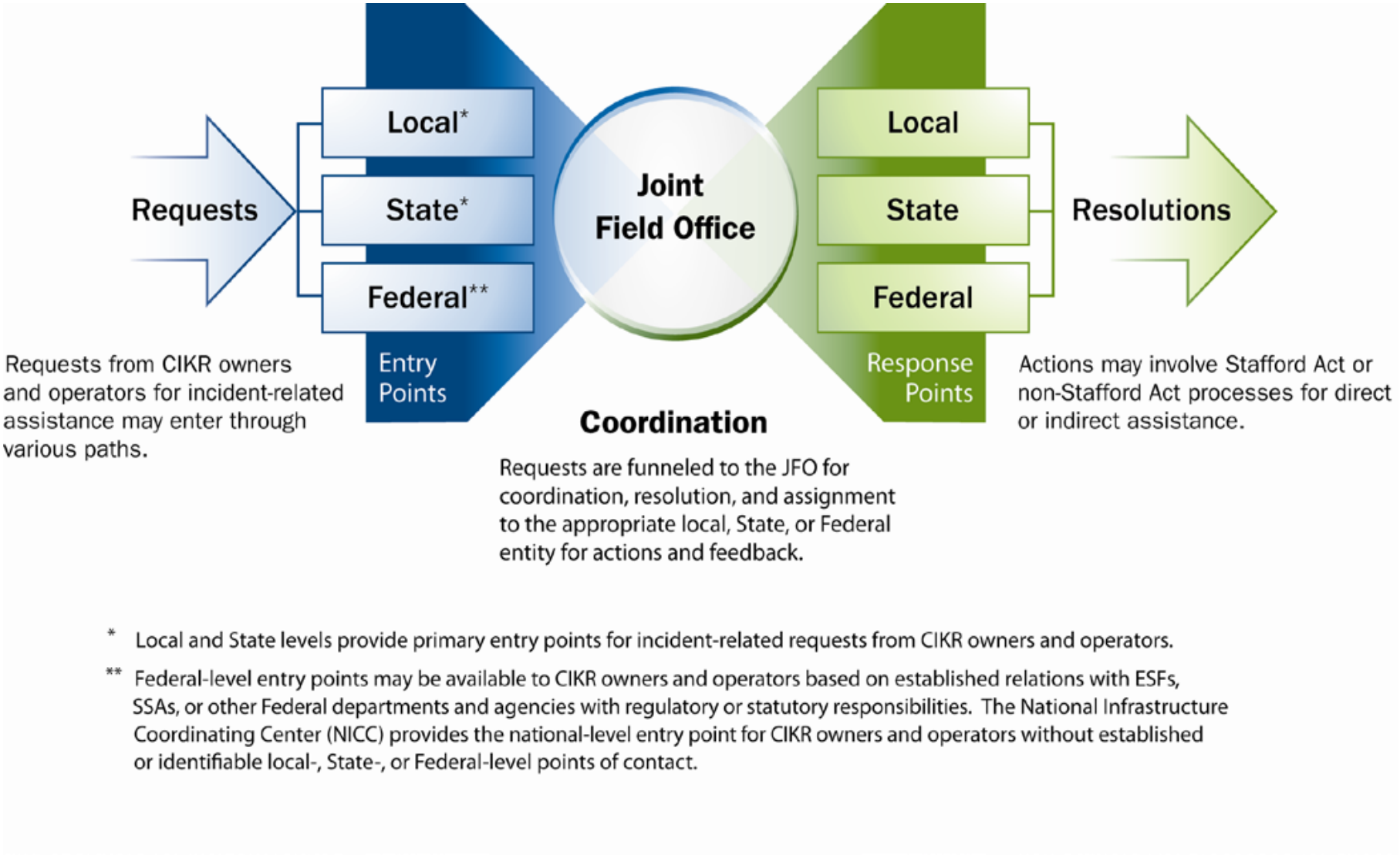
Government Assistance

- CI-related response and recovery activities operate within a framework of mutual aid and assistance. Incident-related requirements are addressed through direct actions by owners/operators or with FSLTT government assistance in certain specific circumstances.

- **Robert T. Stafford Disaster Relief and Emergency Assistance Act** permits consideration of private sector requests for assistance, but does not guarantee that needs or requests from private sector entities will be met in all cases.

- A private sector CI owner/operator may receive direct or indirect assistance from Federal Government sources when the need:
  - Exceeds capabilities of the private sector and relevant local, state, tribal, territorial, and insular area governments;
  - Relates to immediate threat to life and property;
  - Is critical to disaster response or community safety; and
  - Relates to essential Federal recovery measures.

Requests for Assistance



* Local and State levels provide primary entry points for incident-related requests from CIKR owners and operators.

** Federal-level entry points may be available to CIKR owners and operators based on established relations with ESFs, SSAs, or other Federal departments and agencies with regulatory or statutory responsibilities. The National Infrastructure Coordinating Center (NICC) provides the national-level entry point for CIKR owners and operators without established or identifiable local-, State-, or Federal-level points of contact.

Government Assistance (Cont.)

- The Defense Production Act (DPA) provides specific authority to expedite supply and strengthen production capabilities for CI response & restoration activities, including the following:
  - Priority ratings in the Defense Priorities and Allocations System on contracts and orders for industrial resources.
  - Financial incentives to expedite deliveries and expand supplies of materials and services.
  - Agreements by the private sector to share information to coordinate management of critical supplies.
  - Private sector experts in government emergency protection, response, and recovery activities.

- FEMA coordinates DPA authorities before and during an incident, including: providing priority ratings on contracts and orders for industrial resources in cooperation with the Department of Commerce or relevant SSAs; developing guidance and procedures; coordinating DPA plans and programs; and providing technical assistance for all appropriate Federal agencies under the NRF and NIPP.

Discussion Questions

- What are the key government and private sector incident management coordinating structures and nodes according to the NIPP, the NRF, and the National Prevention Framework (NPF)?
- What are the roles and responsibilities of the various NIPP partners vis-à-vis national incident management? What are their major needs?
- How is the CISR mission area addressed in the NRF and NPF?
- What are the principal elements of the Critical Infrastructure Support Annex to the NRF? How do they work?
- How are information and intelligence shared between the various public and private sector nodes of the NIPP Partnership Framework in an emergent threat scenario? During an incident in progress? Does the process work? How could it be improved?

Discussion Questions

- What actions do the sectors take in response to an emergent threat or National Terrorist Advisory System (NTAS) elevation? What are the near and long term ramifications across the sectors?
- How is situational awareness maintained among the various NIPP partners during incident response?
- How are private sector requests for assistance assessed and addressed during incident response operations?