Introduction to DHS Resilience Framework:

Partnering with other agencies

Sandrine Schultz – FEMP Resilience Team
FEMP Resilience Planning Map (RPM) – A prioritized systematic approach to Resilience Planning
What is my agency’s definition of resilience?
• What are my threats and vulnerabilities?
• Is resilience only applied to critical assets?
• Can my preventive maintenance list be funded under the Resilience program (prevention= resilience)
• Critical assets depend on day to day operations; domino effect (Kathleen’s triangle)
• How do I engage with other managers and address interruption of their operations if mine goes down (interdependencies)
• Do they have solutions in place to ensure their operations are not interrupted if mine are?
• When and how do I engage with external stakeholders?
• I need to determine how long I can maintain operations in the event of an interruption?
• Do I include projects in current IPL for operations, energy or environment?
Portfolio Resilience Planning and Implementation

Access on the FEMP Portfolio Resilience Planning and Implementation web page

Arriving Soon !!!!
FEMP Partnerships

• DHS Partnership – MOU Signed in February 18

• Achievements
  – DHS Resilience Framework document sent to Exec Sec August 6th, 2018
  – Established resilience performance metrics and monitoring guidelines
  – In the process of identifying best practices for resilience technologies and solutions
    • USCG Portsmouth Virginia (FEMP and NREL)
    • FLETC Glynco Georgia (FEMP and NREL)
    • NETC FEMA Maryland (FEMP and NREL)
  – Providing associated technical support and engaging with selected DHS Component Pilot Sites.
  – Deploying solutions and processes for resilience planning in the Resilience Planning Map (RPM)
  – Leveraging lessons learned and templates for the Pre-Energy Exchange RPM training class
Vital mission to secure the nation from the many threats we face

- We have more than 240,000 employees
- We are made up of Operational and Support Components
- We are the third largest Cabinet department
Organization

U.S. Department of Homeland Security

SECRETARY
DEPUTY SECRETARY

Chief of Staff

Executive Secretariat

Military Advisor

Chief Financial Officer

MANAGEMENT Directorate

SCIENCE & TECHNOLOGY Directorate

NATIONAL PROTECTION & PROGRAMS Directorate

POLICY

GENERAL COUNSEL

LEGISLATIVE AFFAIRS

PUBLIC AFFAIRS

INSPECTOR GENERAL

HEALTH AFFAIRS

INTERGOVERNMENTAL AFFAIRS

INTELLIGENCE & ANALYSIS

OPERATIONS COORDINATION & PLANNING

CITIZENSHIP & IMMIGRATION SERVICES OMBUDSMAN

CHIEF PRIVACY OFFICER

CIVIL RIGHTS & CIVIL LIBERTIES

DOMESTIC NUCLEAR DETECTION OFFICE

FEDERAL LAW ENFORCEMENT TRAINING CENTER

U.S. Customs & Border Protection

U.S. Citizenship & Immigration Services

U.S. Coast Guard

Federal Emergency Management Agency

U.S. Immigration & Customs Enforcement

U.S. Secret Service

Transportation Security Administration
Organization: Operational Components

- Customs Border Protection
- National Protection and Programs Directorate
- Federal Emergency Management Agency
- Immigration and Customs Enforcement
- Federal Law Enforcement Training Center
- Science and Technology Directorate
- Transportation Security Administration
- U.S. Citizenship and Immigration Services
- U.S. Coast Guard
- U.S. Secret Service
Why is the resilience framework needed?

• Ongoing response to extreme weather, natural and man-made disasters
• Our systems more vulnerable to loss of power and damage to our infrastructure
• Ensures the incorporation of resilience into the Department’s critical infrastructure required for essential functions.
Resilience Drivers

Output
- Develop a roadmap implementing resilience.
- Demonstrate interdependencies and solutions between focus areas: information communication technology, energy/water, facilities, transportation
- Establish metrics for resilience performance
- Monitor success and best practices for resilience within DHS

New Executive Order 13834 - enhance the resilience of Federal infrastructure and operations

FEMA – National Preparedness Report
Directive 023-03 – Climate Resilience
Directive 008-03 – Continuity Programs
National Defense Authorization
Presidential Directives
DHS Directives
PPD-21 (2013)
DHS Internal Memoranda
Component Plans for Resilience

Unclassified//For Official Use Only
DOE-DHS Memorandum of Understanding

BETWEEN THE
DEPARTMENT OF ENERGY
AND THE
U.S. DEPARTMENT OF HOMELAND SECURITY

COLLABORATION IN A STRATEGIC PARTNERSHIP TO ADVANCE FEDERAL CRITICAL INFRASTRUCTURE RESILIENCE

I. Purpose

The purpose of this memorandum of understanding (MOU) is to establish a mechanism for cooperation and partnership between the U.S. Department of Energy (DOE), Office of Energy Efficiency and Renewable Energy (EERE), Federal Energy Management Program (FEMP) and the U.S. Department of Homeland Security (DHS) Chief Readiness Support Officer (CRSO), hereinafter also referred to each as a “Party” or collectively as “the Parties.” The Presidential Policy Directive/PPD-21 advances a national unity of effort to strengthen and maintain security, functioning, and resilient critical infrastructure. This partnership will strengthen coordination of and amplify existing efforts dedicated to advancing the Nation’s critical infrastructure by developing a resilience framework to apply across the Homeland Security Enterprise. This MOU is intended as an umbrella agreement under which particular activities are executed including, but not limited to, developing the DHS Resilience Framework, establishing resilience performance metrics and monitoring guidelines, identifying best practices for resilience technologies and solutions, and providing associated technical support.

Goals specified:

- Joint development of Resilience Framework
- Establish Resilience Performance Metrics & Monitoring Guidelines
- Identify Best Practices for Resilience Technologies & Solutions
- Provide Associate Technical Support
- Engaging with Selected DHS Component Pilot Sites
Each Component participate in all Resilience Framework Tiger Team activities to the greatest extent possible, with representatives for each of the focus areas.

Activities:
- Development of the DHS Resilience Framework
- Providing feedback on various pieces of the framework
- Development of your own Component Plan for Resilience
- Planning and execution of projects that incorporate resilience for mission assurance.

**Components will be required to submit their Plan for Resilience to OCRSO by August 31, 2019.**
DHS Resilience Framework

Resilience Framework: signed August 2018

Providing a Roadmap for the Department in Operational Resilience and Readiness

Claire M. Grady
Under Secretary for Management

15 Aug 2018

Date

14
Resilience Focus Areas

**Critical Infrastructure**

**Energy and Water**
Maintain a continuous power and water supply, and enable energy and water systems to adapt to changing conditions and withstand and rapidly recover from disruption.

**Facilities**
Ensure that buildings, structures, and land assets can adapt to and continually operate during a disruption, and rapidly recover.

**Information and Communication Technology**
Ensure that hardware, software, internal telecommunications infrastructure, programming, and information systems can adapt to changing conditions and withstand and rapidly recover from disruption.

**Transportation**
Maintain continuously available mobile assets (air, marine, and fleet) that can adapt to changing conditions and mobilize resources to assist the mission, and withstand and rapidly recover from disruption.
• Determine which systems and applications are most critical to stakeholders
• Identify criticality: recovery time objective and maximum tolerable downtime
• (how long systems can be down before their loss begins to negatively affect mission)
Critical Infrastructures Interdependencies

Resilience Interdependencies Among Infrastructure

All four infrastructure focus areas are interdependent to each other. A site's mission can be vulnerable to threats and hazards due to cascading effects of single-system disruptions or outages. Resilient sites understand these interdependencies and mitigate risks at each node to support their mission functions.
Resilience Framework Method

Framework applies common principles across DHS Operations to identify, assess, prioritize, and protect DHS’ Critical Infrastructure
Continuity requirements must be incorporated into the operational activities of all Components to ensure the sustainment of mission essential functions.

Critical mission activities and assets are those activities and assets so vital that their incapacity or destruction would have a debilitating impact on security.
Through the continuity process a business impact analysis is conducted. The results of the BIA integrate with intelligence and threat reporting, inform risk management activities to ensure the continued performance of essential functions, emphasizing the performance of MEFs and PMEFs. (i.e. What are the Gaps that exist?)

A Business Impact Analysis is essential in identifying and prioritizing what is critical to the Department by prioritizing services that must continue during an emergency, as well as during normal operations.
Integration of Resilience and Continuity

For critical infrastructure protection, risk management requires leveraging resources to address the most critical assets that are most vulnerable and have greatest threat exposure. Assess Liabilities identifies the hazards, threats, risks, and vulnerabilities of the Mission Essential Assets. The end goal of assessing liabilities is to determine the level of risk that exists under each critical infrastructure.

Liabilities should be evaluated based on the degree of mission impact and the extent to which a liability will cause interruption.

Resilience Relationship – Assess Liabilities

Unclassified//For Official Use Only
Risk management involves the consideration and implementation of strategies and measures to reduce the challenges identified in the risk assessment and seeks to answer the following questions:

- What can be done?
- What are the trade-offs in terms of costs and benefits for each option?
- What impact will these options have on future efforts to mitigate risk?

Resilience Relationship – Resolve Gaps & Determine Resilience Readiness
The Resilience Readiness Planning Assessment provides Stakeholders with guidance on how to prepare, ensure vulnerabilities of critical assets are identified and mitigated, and ensure mission continuity and readiness.
In Conclusion...

• Aligns with Executive Order 13834 “enhance the resilience of Federal infrastructure and operations”

• Aligns with DHS Secretary strategy for prioritization of mission

• Establishes roadmap for Components & other Agencies

• Easily transfers to other Civilian Agencies