

FEDERAL UTILITY PARTNERSHIP WORKING GROUP SEMINAR

November 7-8, 2019
Washington, DC

Department of Homeland Security Resilience Update

Hosted by:



Why does DHS need a resilience framework?

- Ongoing response to extreme weather, natural and man-made disasters.
- Systems more vulnerable to loss of power and damage to infrastructure.
- Ensures incorporation of resilience into DHS's critical infrastructure required to complete their mission.



Resilience Drivers

National Defense Authorization Act (2018)

Presidential Executive Orders

- E.O. 13834 - Enhance resilience of Federal infrastructure and operations

DHS Directives

- FEMA – National Preparedness Report
- Directive 023-03 – Climate Resilience
- Directive 020-01 – Energy & Water Management (Energy Security)
- Directive 008-03 – Continuity Programs

PPD-21 (2013)

DHS Internal Memoranda

Component Plans for Resilience

Goal Setting

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



Resilience Framework

Framework applies **common principles** across DHS Operations to **identify, assess, prioritize, and protect** DHS's Critical Infrastructure.



Resilience Focus Areas



Energy and Water

- Maintain a continuous power and water supply.
- Enable energy and water systems to adapt to changing conditions.
- Withstand and rapidly recover from disruption.



Facilities

- Ensure buildings, structures, and land assets withstand changing conditions.
- Adapt to and continually operate during a disruption.
- Rapidly recover from disruption.



Information and Communication Technology

- Ensure hardware, software, internal telecommunications infrastructure, programming and information systems adapt to changing conditions.
- Withstand and rapidly recover from disruption.



Transportation

- Maintain continuously available mobile assets (air, marine, and ground) that can adapt to changing conditions.
- Mobilize resources to assist mission.
- Withstand and rapidly recover from disruption.

Federal Utility Partnership Working Group
November 7-8, 2019 Washington, DC

Resilience Baseline Assessment Scoring Tool

- Excel-based tool
- Linear progression
- Self-contained
- Compares multiple assets and sites
- Component agnostic
- Simple inputs and outputs
- Resilience Factor metric



Tool

RESILIENCE BASELINE ASSESSMENT SCORING TOOL

Developed for the Department of Homeland Security by the National Renewable Energy Laboratory

Version 2.6

(Updated: 5/21/2019)

UNCLASSIFIED / FOR OFFICIAL USE ONLY

The **RESILIENCE BASELINE ASSESSMENT SCORING TOOL** is an Excel-based tool, designed to assist Department of Homeland Security (DHS) Component Agencies developing their internal resilience plans. This tool is to be used alongside the DHS Resilience Framework and the DHS Component Plan for Resilience template. The **OUTPUT** of this tool is a summary report that identifies a Component's highest priority Mission Essential Assets (MEA) based on a **RESILIENCE FACTOR SCORE**. Additionally, the summary report shows the Component's resilience stakeholder's contact information, and compares hazards and vulnerabilities at each evaluated site.

(click icon or image to enlarge)



Resilience Framework



Show Essential Terms

Show Resilience Factor Definition

TOOL GUIDANCE

1. ENGAGE STAKEHOLDERS:

Go to Tab 1.

Component Plans for Resilience are expected to be prepared at the Component Headquarters level. However, Component Headquarters should delegate authority and prioritize resilience efforts to support critical missions and assets. Stakeholders at the Component Headquarters level should be identified in the Plan for Resilience and work as an integrated team in the resilience planning process. This tool facilitates this process by prompting you to enter the roles/titles and contact information of each stakeholder. Key stakeholders may include: continuity leads, energy managers, facilities managers, transportation managers, site operations managers, emergency management managers, cybersecurity managers, and any external stakeholders that are relevant to resilience planning. Key decision-makers including finance, procurement, and legal may also be included. At minimum, all infrastructure focus area stakeholders should be identified. This list may be modified to include additional members as appropriate.

2. IDENTIFY CRITICAL MISSION AND CONDUCT CRITICALITY ASSESSMENT:

Go to Tab 2.

The DHS Continuity Planning process, which mandates the completion of a Business Process Analysis (BPA) and a Business Impact Analysis (BIA) per FCD-2, helps to identify the mission essential assets (MEAs) that support your Component's mission essential function(s) (MEFs). This process also assigns a level of criticality to these MEAs on a scale of 1-4, from "Low Consequence" (1) to "Very High Consequence" (4). Classifying your Component's MEAs in this way is a crucial first step toward identifying where investments should be targeted. Tab 2 of this tool aligns with the DHS Continuity Planning process described above. It is designed to allow Components to copy and paste the MEFs, MEAs, and Criticality Levels from the BIA. In order to maintain confidentiality, MEAs shall be entered using unique and secure identifiers. Please coordinate with your Continuity Team Lead, identified in Tab 1, to use the results obtained in the BIA and BPA to fill in the data for Step 2.

Data Output

- Prioritized list of assets based on Resilience Factor.
- Data organized into tables for simple summary and entry in resilience plans.
- Site-level data to assist with vulnerability and hazard assessments.
- Space for capturing narratives, notes, and comments.

Table 1: Resilience Factor Table

Component PMEFs/MEFs	Component MEAs	Level of Criticality	Hazards Score	Vulnerability Score	Resilience Factor
PMEF #1	Sample Asset 1	4	High	High	86
PMEF #2, MEF #2	Sample Asset 2	3	Medium	Medium	59
PMEF #3, MEF #33	Sample Asset 3	2	Low	Low	36

Table 2: Engage Stakeholders

Role/Title	Name	Contact E-mail
Resilience Lead	Individual 1	Individual.1@email.gov
Continuity POC	Individual 2	Individual.2@email.gov
SME 1	Individual 3	Individual.3@email.gov
SME 2	Individual 4	Individual.4@email.gov
SME 3	Individual 5	Individual.5@email.gov

Table 3: Site Hazards

Site Name	Wildfire	Volcano	Tornado	Snowfall	Landslide	Hurricane	Earthquake	Drought	Heatwave	Avalanche	Flood
Sample Site 1	Low	None	High	Medium	Medium	Medium	Low	None	High	None	High
Sample Site 2	Low	None	Medium	Low	Medium	Low	Low	None	Medium	None	High
Sample Site 3	Low	None	Medium	Low	Medium	Low	Low	None	Low	None	Low

Table 4: Site Vulnerabilities

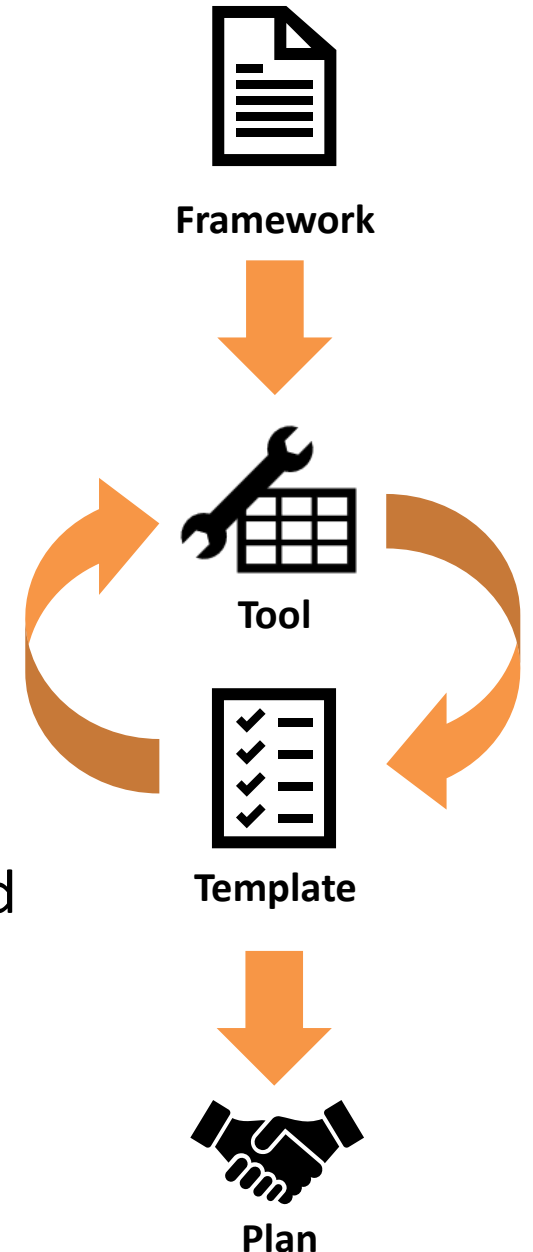
Site Name	Energy and Water	Facilities	Information and Communication Technologies	Transportation
Sample Site 1	●	●	●	●
Sample Site 2	●	●	●	●
Sample Site 3	●	●	●	●

Table 5: Asset Narratives

Component MEAs	Resilience Factor	Implementation Narrative
Sample Asset 1	86	Sample text, sample text, sample text
Sample Asset 2	59	Sample text, sample text, sample text
Sample Asset 3	36	Sample text, sample text, sample text

Resilience Planning for a Federal Agency

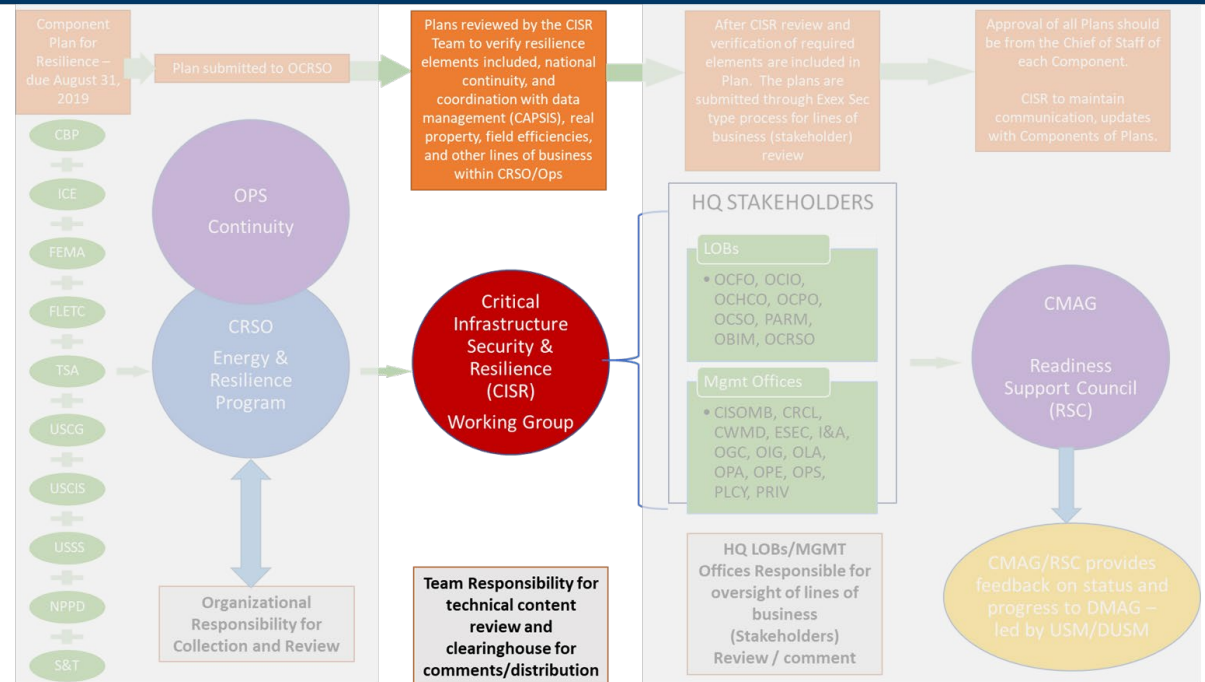
- Consistent processes and documentation
- Resilience champion
 - ✓ At headquarters
 - ✓ At management
 - ✓ At the component(s)
- Coordination
 - ✓ Weekly Critical Infrastructure Security and Resilience (CISR)
 - ✓ Monthly Tiger Team working groups
 - ✓ Monthly or as needed one-on-one meetings with components
- On-call technical support and assistance
- Partnerships
 - ✓ DHS Continuity group
 - ✓ DOE FEMP
 - ✓ National Laboratories (NREL, INL)
 - ✓ DOD
- Establish timelines, deadlines, and deliver



Resilience Plan Updates

Component	Plan Pages	Review Date
CBP	34	10/1/2019
CISA	12	10/1/2019
FEMA	25	10/1/2019
FLETC	19 +annex	10/9/2019
ICE	21	10/9/2019
S&T	15 +apndx	10/9/2019
TSA	6	10/30/2019
USCIS	23	10/30/2019
USCG	22	10/30/2019
USSS	n/a	Not submitted

Review/Validation of Plans

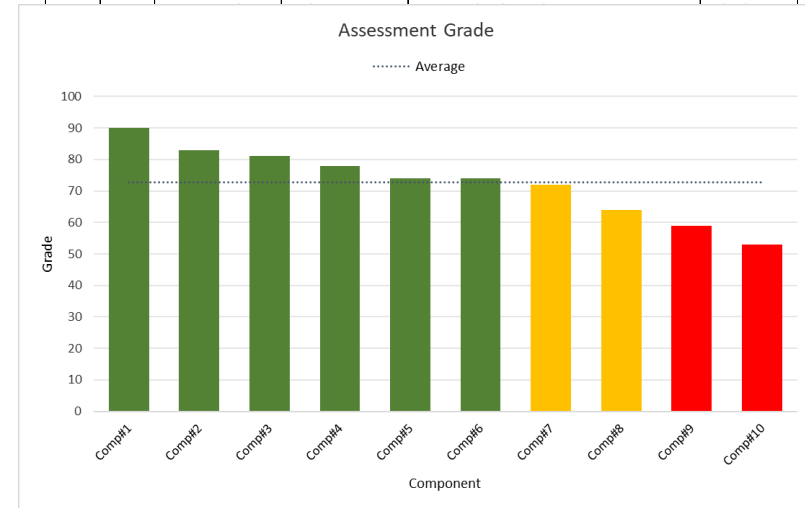


Validation Process

- Components to receive feedback on their plans starting October 31st.
- Components and CISR steering committee to have one-on-one meetings to discuss feedback.
- Finalized plans to be submitted for HQ stakeholder review.

Areas of Focus: Process Plan
 Document Title: CBP Plan for Resilience_Signed_FINAL.pdf
 Component: CBP

Index	Page	Section	Comment Name	Comment Description	Reviewer
2	1	I) Introduction - Purpose	Defining MEAs	Mission Essential Assets (MEAs) are defined as any critical infrastructure, physical or cyber, that performs a Mission Essential Function (MEF), as such, MEAs refer to more than just facility assets.	David LoVullo
14	3	Purpose	MEA Definition	MEA is defined as only a facility when it could be a system, or piece of equipment that supports a MEF	Ashley Harrigan
15	5	Guidance and Tools	BIA	I would find a way to include CBP BIA as one of the guidance documents	Ashley Harrigan
3	6	Step 6: Integrate Resilience Readiness Solutions	Risk-based decision making	Not 100% accurate to say that resilience planning is the same as risk mitigation; though they are related. Resilience planning notably would include adaptability and recoverability.	David LoVullo
9	6	DHS Resilience Focus Area	Good understanding	CBP demonstrates a good understanding of the four critical infrastructure focus areas.	Michael Young
4	7	DHS RBAS Tool	More resilient and less resilient	We can't definitely say that the Resilience Factor scores are more or less "resilient" rather, we can say that they are higher or lesser priority in our planning efforts.	David LoVullo
5	7	Tab 2: Identify Critical Mission	Real Property ID	It is no longer required to use Real Property ID systems from CAPSIS when entering MEA identifiers, this guidance was updated around May 2019.	David LoVullo



DHS Resilience Goals

- Consistent methodological approach across components and geographic locations – Result template and RBAS tool
 - ✓ Component Plans for Resilience received in August 2019
- Leverage existing datasets and processes
 - ✓ Establish policy and procedures for prioritizing funding to support resilience
- Promote all-hazards approach
 - ✓ Use of partnerships to incorporate best practice systems and tools

