Infrastructure Assessments and Analysis

Steve Cauffman and Will McNamara
Cybersecurity and Infrastructure Security Agency
Who We Are

The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation’s risk advisor, working with partners to defend against today’s threats and collaborating to build more secure and resilient infrastructure for the future.
CISA fosters collaborative partnerships that enable partners in the government and private sector to make informed and voluntary risk management decisions and investments.

Every day, CISA employees: Share information with critical infrastructure partners and stakeholder and serve as the national hub for cybersecurity and communications information data sharing in near-real-time.

Sector outreach: CISA works with government officials and critical infrastructure stakeholders to plan, develop and facilitate exercises that build capacity, improve security and bolster resilience.
CISA Regional Offices and Outreach Staff

Courtesy of DHS
# Infrastructure Security Division

Infrastructure Security Division leads the coordinated effort to reduce risks posed to our critical infrastructure, whether from man-made or natural causes. Infrastructure Security Division also leads the nation’s preparedness efforts for these attacks.

## MISSION PRIORITIES:

<table>
<thead>
<tr>
<th>Priority</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure critical infrastructure from terrorist attacks.</td>
<td>Work with government and private sector partners to increase security around soft targets and crowded places through training, exercises, assessments and other resources.</td>
</tr>
<tr>
<td>Work with government and private sector partners to increase security</td>
<td>Collaborate with government partners to share security best practices, conduct assessments and share information related to school safety.</td>
</tr>
<tr>
<td>Prevent complex or hybrid attacks in a converging cyber-physical threat</td>
<td>Manage regulatory compliance of securing chemical facilities through the Chemical Facility Anti-Terrorism Standards program.</td>
</tr>
</tbody>
</table>
Infrastructure Assessments and Analysis

- CISA/Infrastructure Security Division’s (ISD) Office of Infrastructure Assessments and Analysis provides a set of programs and teams that are mutually supportive and operate collectively to achieve ISD’s objective of creating more secure and resilient infrastructure.

- The Office’s top-line responsibilities of assessment and analysis are:
  - Performed by its Assessments and Planning teams working collaboratively with CISA regional personnel and infrastructure partners;
  - The execution of which is enabled by System Engineering that provides tools and capabilities and Information Protection that ensures the ability to collect and share data;
  - The outcomes of which are documented and promulgated through Training and other resources; and,
  - All of which are supported through centralized Program Management.
• Resilience: “The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions”
Resilience Challenges

• Increasing complexity and coupling
• Evolving business practices
• Organizational structures
• Lack of transparency

“...the nature of the critical infrastructure risk environment precludes any one entity from managing risks entirely on its own...” (National Infrastructure Protection Plan 2013)
Regional Analysis Methodology

**Top-Down Approach**
- System of Systems-level Modeling and Failure Analysis
- Individual System-level Modeling and Failure Analysis
- Asset and System-level Assessments
- Service Provider Interviews
- Asset-level Interviews
- Open-source Research

**Bottom-Up Approach**
# Types of Dependencies

<table>
<thead>
<tr>
<th>Class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>Operations depend on material output(s) of other infrastructure through a functional and structural linkage between the inputs and outputs of two assets. In other words, a commodity produced by one infrastructure is needed as an input by another infrastructure for its operation.</td>
</tr>
<tr>
<td>Cyber</td>
<td>Operations depend on information and data transmitted through the information infrastructure via electronic or informational links. Outputs from the information infrastructure serve as inputs to other infrastructure, with the relevant commodity being information.</td>
</tr>
<tr>
<td>Geographic</td>
<td>Operations depend on the local environmental, where an event can trigger changes in the state of operations in multiple infrastructure assets or systems. A geographic dependency occurs when elements of infrastructure assets are in close spatial proximity (e.g., a joint utility right-of-way).</td>
</tr>
<tr>
<td>Logical</td>
<td>Operations depend on the state of other infrastructure via connections other than physical, cyber, or geographical. Logical dependency is attributable to human decisions and actions and is not the result of physical or cyber processes.</td>
</tr>
</tbody>
</table>

*Source: Rinaldi, Peerenboom, and Kelly 2001*
Upstream Dependencies

Overview of Upstream Dependencies for Port Terminals, Source: Regional Resiliency Assessment Program Dependency Analysis Framework, 2017
## Interdependencies

<table>
<thead>
<tr>
<th>Sector</th>
<th>Sector Dependency on Drinking Water</th>
<th>Drinking Water Dependency on Sector</th>
</tr>
</thead>
</table>
| Chemical                    | □ Manufacturing operations  
□ Office operations                                           | □ Chlorine and other treatment chemicals  
□ Office operations                                                   |
| Commercial Facilities       | □ Facility operations                                                                                     | □ Bottling                                                                |
| Communications              | □ Equipment cooling  
□ Common rights-of-way                                           | □ Emergency communications with responders  
□ General operations  
□ SCADA  
□ Monitoring                                                             |
| Critical Manufacturing      | □ Water as a product constituent  
□ Equipment cooling                                              | □ Operational and process equipment                                        |
| Dams                        | □ N/A                                                                                                  | □ Storage; reservoirs  
□ Flood mitigation                                                   |
| Defense Industrial Base     | □ Office operations  
□ Equipment cooling                                           | □ Production of parts                                                 |
| Emergency Services          | □ Continuity of operations  
□ Firefighting and hazardous material (HAZMAT) spill and event responses  
□ Decontamination services  
□ Emergency water supplies  
□ Equipment maintenance                                                            | □ Special weapons and tactics and tactical operations  
□ Coordination with the ICS  
□ Law enforcement  
□ Explosive ordnance disposal  
□ Emergency (medical and firefighting) responders  
□ HAZMAT responders |

*Interdependencies between Sectors and Drinking Water Supply (excerpt), Source: Puerto Rico Infrastructure Interdependency Assessment, May 2018*
Infrastructure Assessments and Analysis

Resilience Services

• Assessments: Develops and manages an assessment methodology to identify critical infrastructure vulnerabilities, support collaborative security planning, and provide recommendations to enhance protective measures and risk mitigation strategies.
  • **Regional Resiliency Assessment Program (RRAP)**
    • Assessment of specific infrastructure within a designated geographic area and a regional analysis of the surrounding infrastructure that address a range of infrastructure resilience issues.
  • **Infrastructure Survey Tool (IST)**
    • Voluntary, web-based vulnerability survey conducted by Protective Security Advisors to identify and document the overall security and resilience of the facility.
  • **Infrastructure Visualization Platform (IVP)**
    • Data collection and presentation medium that provides immersive imagery, geospatial, and hypermedia data of critical facilities, surrounding areas, and transportation routes.
  • **Security Assessment on First Entry (SAFE)**
    • Assessment that analyzes the current security posture of an infrastructure and identifies high level options for facility owners and operators to mitigate relevant threats.
Infrastructure Assessments and Analysis

Resilience Services (cont.)

• **Planning**: Works with public and private sector partners to enhance infrastructure security and resilience to all threats and hazards by building security and resilience elements into infrastructure investment strategies, plans, policies, designs, and procedures.
  • Capabilities:
    • A network of resilience subject matter experts who provide guidance on best practices
    • Decision support tools to assist with investment decisions during infrastructure planning and maintenance operations, as well as recovery efforts
    • Experts who can provide technical assistance and analysis to support critical infrastructure recovery efforts, and who can be deployed to the field as needed
    • Community-focused resilience workshops, technical assistance exercises, and training
    • Research and analysis on key issues related to infrastructure investment decisions
Infrastructure Assessments and Analysis

Resilience Services (cont.)

- Capabilities and resources based on assessments
  - Response and recovery operations (Emergency Support Function #14 and Infrastructure Systems-Recovery Support Function)
  - Special event security planning
  - Derivative assessment products, summaries, derivative analysis
  - Assessment methodology and associated guidance and training
Integrated Services

<table>
<thead>
<tr>
<th>Assessments</th>
<th>Infrastructure Scale</th>
<th>Geographic/Governance Scale</th>
<th>Planning</th>
</tr>
</thead>
<tbody>
<tr>
<td>RRAP</td>
<td>Network</td>
<td>State/Region</td>
<td>State HMP, THIRA, SPR, regional transportation resilience/long term planning, etc.</td>
</tr>
<tr>
<td>MASA, RRAP (some)</td>
<td>System</td>
<td>Community/Municipality (ies)</td>
<td>Community Planning, IRPF, Municipal-level mitigation, resilience, etc.</td>
</tr>
<tr>
<td>IST, SAFE</td>
<td>Asset</td>
<td>Owner/Operator</td>
<td>Asset mitigation, security, risk management, continuity</td>
</tr>
</tbody>
</table>

Asset mitigation, security, risk management, continuity
Planning is performed to address resilience gaps identified by assessments. In addition, planning processes also identify knowledge gaps or infrastructure issues/challenges that require assessment.

Assessments typically performed to support planning on some level. Assessments can be performed specifically to inform an existing planning process. This includes disaster planning efforts.
Collected infrastructure assessment data/knowledge, resilience gaps and solutions, mitigation approaches, planning knowledge—everything required to perform or that is derived from our integrated assessment and planning capabilities—translates directly into disaster response and recovery applications. Preparing for disasters also entails assessment and planning.

Mission of new organization is thus: perform assessments in steady state, support resilience planning in steady state, and apply expertise to emergencies. Assessments, Planning, and Emergency Preparedness are our core mission areas/competencies.
Assessments Spectrum

- Single Sites
  - SAFE
  - IVP
  - IST
  - MASA

- Clusters & Single Systems

- Complex Networks
  - RRAP

Dependency Analysis

- Mostly Security Focus
  - Least Complex

- Mostly Resilience Focus
  - Most Complex
Infrastructure Assessment Capabilities

Assessing Interdependencies

Hazard & Impact Modeling and Simulation

Analyzing Supply Chain Risks

Characterizing infrastructure operations

Interactive Systems Mapping

Photos Courtesy of DHS
Security Assessment at First Entry (SAFE)

Designed to assess current security posture and identify options for consideration, produce a report, in under 2 hours

- Physical security and planning focused
- High level options for consideration

Audience is for facilities with little to no knowledge in basic security

- Houses of worship
- Schools
- Rural health clinics

Uses standard language vulnerabilities and options for consideration from the IST
Infrastructure Survey Tool (IST)

Voluntary surveys of a facility’s physical security, security forces, security management, protective measures, information sharing, business continuity, cybersecurity and dependencies

- Helps inform protection planning and resource allocation
- Identifies vulnerabilities and trends for infrastructure and across sectors
- Provides web-based protective measures / resiliency dashboards and written report
- Provides an analysis of common characteristics observed, and options for consideration issued, by Protective Security Advisors by sector or within a geographic area.
Infrastructure Visualization Platform (IVP)

- The IVP is a data collection and presentation medium
- The IVP supports critical infrastructure security, special event planning, and response operations by incorporating immersive imagery, geospatial, and hypermedia data of critical facilities and surrounding areas
- We conduct 100+ IVPs a year, across the Regions
Regional Resiliency Assessment Program

• The goal of the RRAP is to generate greater understanding and action among public and private sector partners to improve the resilience of a region’s critical infrastructure
  • Resolves infrastructure security and resilience knowledge gaps
  • Informs risk management decisions
  • Identifies resilience-building opportunities and strategies
  • Improves critical partnerships among stakeholders
Infrastructure Development and Recovery (IDR)

**Mission**
- To develop, coordinate, and support the implementation of integrated security and resilience solutions across the critical infrastructure community, with a focus on infrastructure development, maintenance, and recovery following disruptive events.

**Goals**
- Promote a consistent, coordinated and holistic approach to supporting critical infrastructure security and resilience efforts focused on infrastructure development, maintenance, and recovery across ISD and throughout the Federal Government.
- Provide an integrated approach to supporting decision-making that enhances resilience, seeking to mitigate risk from interdependencies and cascading failures associated with a range of threats and hazards.
- Encourage the incorporation of resilience strategies and policies into the planning, design, construction, and upkeep of critical infrastructure.
Infrastructure Resilience Planning Framework

- Infrastructure Resilience Planning Framework (IRPF)
  - Includes comprehensive, step-by-step planning guidance, templates, and other resources to inform long-term planning and investment decisions
  - Five steps from stakeholder engagement to risk assessment and implementation
  - Can incorporate methods from Regional Resiliency Assessment Program (RRAP) projects and outcomes from other plans/initiatives
  - Can be used in other local and regional plans, such as Federal Emergency Management Agency (FEMA) mitigation planning and recovery and regional economic development plans
  - On-line access and links in development

Courtesy of DHS
IRPF Process

Provides a generalized process to identify and prioritize infrastructure, evaluate risk, and develop and implement a plan for enhanced resilience

Lay the Foundation
- Define and scope effort
- Form collaborative working group
- Collect/review existing data, plans, studies, mapping, and other resources

Critical Infrastructure Identification
- Identify physical and cyber infrastructure
- Prioritize infrastructure
- Identify interdependencies among infrastructure systems

Risk Assessment
- Identify threats and hazards to physical and cyber infrastructure
- Assess interactions among risks to infrastructure systems
- Prioritize risk to infrastructure systems
- Assess vulnerability of prioritized infrastructure to risk

Community Infrastructure Resilience Plan Development
- Validate/refine goals and objectives for resilient critical infrastructure
- Identify potential resilience solutions to mitigate risks
- Identify and assess existing resources and capabilities to implement mitigation measures
- Select resilience solutions for implementation
- Develop implementation strategy

Community Infrastructure Resilience Plan Implementation and Maintenance
- Execute the Community Infrastructure Resilience Plan
- Monitor, evaluate, and assess the effectiveness
- Update the Plan to incorporate lessons learned, new best practices, etc.
Critical Infrastructure Resilience Toolkit (CIRT)

The CIRT is an online version of the IRPF, with the same complementary suite of tools and resources focused on infrastructure security and resilience:

- CIRT website currently being developed
- Pilot will inform site development and priorities

*Courtesy of DHS*
Develop Decision Tools: CIRT

- CIRT is comprised of a suite of tools and resources focused on infrastructure security and resilience designed to inform infrastructure investment, development and operational decisions across sectors and jurisdictions. Development includes:
  - Infrastructure Resilience Planning Framework
  - Quick Guide on Cybersecurity for Infrastructure Development
  - Drought Resilience Decision Guide
  - Interactive Web Site Under Development
  - Regional Service Delivery Model
Lay the Foundation

Provides guidance on how to develop initial buy-in, form a collaborative working group, collect and review existing data and plans, studies that may be relevant to the project.

**Sub-steps**
- Identify a project champion
- Define and scope the effort
- Collect and review existing resources
- Form a collaborative working group

**Tools**
- Stakeholder Recommendations/ Contact Sheet
- Invitation Template

**Resources**
- Sample Data Collection Resources
- Sample Goals and Objectives
- ARUP City Resilience Framework
Critical Infrastructure Identification

Provides guidance on how to identify and prioritize infrastructure that is critical to the community, and identify dependencies and interdependencies for the assets.

Sub-steps
• Identify infrastructure
• Prioritize infrastructure
• Identify dependencies and interdependencies

Tools
• Infrastructure Assets Matrix
• Infrastructure Prioritization Criteria
• UCIP Critical Infrastructure Identification and Prioritization Tool
• Dependency Identification Worksheet

Resources
• Dependency Analysis Framework
## Critical Infrastructure Asset Prioritization Score Sheet

### Criterion: Economic Importance

This criterion assesses the infrastructure asset’s economic importance and the potential impact to the local, regional, and national economy if damaged in a disaster or incident.

<table>
<thead>
<tr>
<th>Mission Descriptions</th>
<th>Scale (0-4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The local economy would not likely be impacted.</td>
<td>0</td>
</tr>
<tr>
<td>The regional economy would not be affected with the local economy would be moderately impacted.</td>
<td>1</td>
</tr>
<tr>
<td>The regional economy would be moderately affected while the local economy would be seriously impacted.</td>
<td>2</td>
</tr>
<tr>
<td>Impact on the national economy is likely and the regional economy would be severely impacted.</td>
<td>3</td>
</tr>
<tr>
<td>The national economy would be severely impacted.</td>
<td>4</td>
</tr>
</tbody>
</table>

### Asset Name | Mission Score | Explanation
--- | --- | ---
1. Example: Electra Power Plant | 3 | The power plant generates electrical power that is transmitted and distributed to the community and the region, which includes a major national port. Damage to the power plant would result in impacts to the local and regional economy, as well as impact the national economy.

Source DHS/CISA
Identify Dependencies

Notional dependency network for a water system. Courtesy of DHS/CISA
Dependencies in Infrastructure Analysis

Courtesy of DHS
# Dependency Analysis Capability

<table>
<thead>
<tr>
<th>Question</th>
<th>Time/Percentage of Impact</th>
<th>Electric</th>
<th>Natural Gas</th>
<th>Water</th>
<th>Wastewater</th>
<th>Comms</th>
<th>Information Technology</th>
<th>Trans.</th>
</tr>
</thead>
<tbody>
<tr>
<td>If this is lost (WITHOUT considering alternatives), how soon would the facility be severely impacted?</td>
<td>Minutes/Hours/Days</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Once this is lost (WITHOUT considering any alternates), what percentage of normal business functions are lost or degraded?</td>
<td>1-33%, 34-66%, 67-99%, or offline</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Once this is lost (AND considering alternatives), what percentage of normal business functions are lost or degraded?</td>
<td>1-33%, 34-66%, 67-99%, or offline</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are there external regulations/policies that mandate the facility shut down after total loss including alternatives?</td>
<td>Yes/No</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>If yes, after how long?</td>
<td>Minutes/Hours/Days</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Once service is restored, how long would it take before full resumption of operations?</td>
<td>Minutes/Hours/Days</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Courtesy of DHS*
Risk Assessment

Provides guidance on approaches for assessing risk to critical infrastructure that can inform the identification and prioritization of mitigation measures.

**Sub-steps**
- Identify threats and hazards
- Assess consequences
- Prioritize risks
- Assess vulnerabilities

**Tools**
- N/A

**Resources**
- Risk Assessment Methodologies
- Risk Information and Analysis Resources
  - Example: Drought Primer
## Risk Assessment

<table>
<thead>
<tr>
<th>Priority Infrastructure</th>
<th>Support Needed</th>
<th>Phase 1</th>
<th>Phase 2</th>
<th>Phase 3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Short Term (Hours)</td>
<td>Intermediate (Weeks)</td>
<td>Long Term (Months)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - 24</td>
<td>24 - 48</td>
<td>48 - 72</td>
</tr>
<tr>
<td>Priority Infrastructure 1</td>
<td>R, S, MS C</td>
<td>90%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Priority Infrastructure 2</td>
<td>R</td>
<td>30%</td>
<td>90%</td>
<td></td>
</tr>
<tr>
<td>Priority Infrastructure 3</td>
<td>MS</td>
<td></td>
<td>30%</td>
<td>60%</td>
</tr>
<tr>
<td>Priority Infrastructure 4</td>
<td>C</td>
<td>30%</td>
<td></td>
<td>60%</td>
</tr>
<tr>
<td>Priority Infrastructure 5</td>
<td></td>
<td>60%</td>
<td>90%</td>
<td></td>
</tr>
</tbody>
</table>

*Courtesy of DHS*
Develop Actions

Supports the identification and prioritization of mitigation strategies to address priority risks and achieve community critical infrastructure resilience goals.

Sub-steps
- Validate/refine goals and objectives
- Identify resilience solutions
- Identify and assess resources and capabilities
- Select resilience solutions
- Develop implementation strategy

Tools
- Capability Assessment Worksheet
- Resilient Solution Evaluation Worksheet
- Alternative Evaluation Options
- Infrastructure Resilience Plan Outline

Resources
- Resilient Solutions Resources
- Sample Solution Identification Process
# Identify Mitigation Options

**Natural Hazards**

<table>
<thead>
<tr>
<th>Disaster Type</th>
<th>Solution Sources</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flood-Drought</td>
<td>Sectoral Applications Research Program (SARP), NOAA <a href="http://cpo.noaa.gov/ClimatePrograms/ClimateandSocialInteractions/SARPProgram/ExtremeEventsExtremeEvents.aspx">http://cpo.noaa.gov/ClimatePrograms/ClimateandSocialInteractions/SARPProgram/ExtremeEventsExtremeEvents.aspx</a></td>
<td>The Sectoral Applications Research Program (SARP) supports interdisciplinary research to advance understanding of how climate change affects different economic sectors. There are various case studies that examine past practices and lessons learned. There are also resources available for webinars and workshops.</td>
</tr>
<tr>
<td>Winter Storm</td>
<td>Prepare Your Organization for Winter Storm Playbook, FEMA</td>
<td>Tools and Resource guide of best practices for community leaders to prepare for and administer post-major winter storm event activities.</td>
</tr>
</tbody>
</table>

**Source** DHS/CISA
Implementation and Maintenance

Provides information on how communities can implement the prioritized resilience solutions through existing community planning mechanisms, and potential funding and technical assistance sources.

Sub-steps
- Execute the plan
- Monitor, evaluate, and assess the effectiveness of the plan
- Update the plan

Tools
- Compendium of Programs and Mechanisms for Funding
- Plan Review Worksheet

Resources
- IRPF Plan Integration
Funding and Finance Resources

I am looking for credit financing and matching funds for a small project in Kansas.

43 funding sources found (3 filters applied):

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Economic Development Agency (EDA) Economic Development Grants</td>
<td>NEW Assists eligible recipients in developing economic development plans and studies designed to build capacity and guide the economic prosperity and resiliency of an area or region.</td>
<td>Department of Commerce</td>
</tr>
<tr>
<td>Public Health Emergency Preparedness Cooperative Agreements</td>
<td>NEW The Public Health Emergency Preparedness (PHEP) provides funding for public health departments across the nation to upgrade their ability to effectively respond to a range of public health threats.</td>
<td>CDC</td>
</tr>
<tr>
<td>Public Health Emergency</td>
<td>The Public Health Emergency Preparedness (PHEP) provides funding</td>
<td>Federal</td>
</tr>
</tbody>
</table>

Source: DHS/CISA
IRPF Integration with Hazard Mitigation Planning (HMP)

1. Organize the Planning Process and Resources
2. Assess Risks
3. Develop a Mitigation Strategy
4. Adopt and Implement the Plan

Courtesy of DHS
Infrastructure in HMP Processes

- HMP guidance references critical infrastructure but contains limited information about how to evaluate them and dependencies between assets and systems.
- Evaluating infrastructure as an interdependent system enables better investment decisions.

### Example

<table>
<thead>
<tr>
<th>Critical Facilities</th>
<th>High Potential Loss Facilities</th>
<th>Infrastructure Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hospitals and medical facilities</td>
<td>Nuclear power plants</td>
<td>Water and wastewater</td>
</tr>
<tr>
<td>Police and fire stations</td>
<td>Dams</td>
<td>Power utilities</td>
</tr>
<tr>
<td>Emergency operations centers</td>
<td>Military and civil defense installations</td>
<td>Transportation (roads, railways, waterways)</td>
</tr>
<tr>
<td>Evacuation shelters</td>
<td>Locations housing hazardous materials</td>
<td>Communication systems/centers</td>
</tr>
<tr>
<td>Schools</td>
<td></td>
<td>Energy pipelines and storage</td>
</tr>
<tr>
<td>Airports/heliports</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: FEMA Local Mitigation Planning Handbook
# HMP – IRPF Integration

<table>
<thead>
<tr>
<th>HMP Step</th>
<th>IRPF Step</th>
<th>Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organize the planning process and resources</td>
<td>Lay the foundation</td>
<td>• Identify Critical Infrastructure (CI) participants</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Identify existing infrastructure and risk resources</td>
</tr>
<tr>
<td>Assess risks</td>
<td>Identify infrastructure</td>
<td>• Identify and prioritize CI</td>
</tr>
<tr>
<td></td>
<td>Assess risk</td>
<td>• Identify dependencies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Assess vulnerability of systems and consequences of failure</td>
</tr>
<tr>
<td>Develop a mitigation strategy</td>
<td>Develop actions</td>
<td>• Identify mitigation options for CI priorities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Prioritize CI mitigation options</td>
</tr>
<tr>
<td>Adopt and implement plan</td>
<td>Implementation and maintenance</td>
<td>• Support integration of CI mitigation options into plans</td>
</tr>
</tbody>
</table>

*Source: DHS/CISA*
Conclusions

• DHS/CISA has developed a robust suite of capabilities for assessing the security and resilience of infrastructure from individual facilities to regional infrastructure systems.
• Resilience assessment and planning requires a shift from an asset focus to systems perspective.
• Key to these capabilities is a well-developed methodology for understanding dependency/interdependency relationships.
• Assessments and resilience planning can be combined to develop prioritized plans to enhance resilience, making efficient use of resources.
Questions?

Will McNamara  
CISA/ISD/RRAP Coordinator  
Email: William.McNamara@cisa.dhs.gov  
Phone: (703) 235-9552

Stephen Cauffman  
CISA/ISD/IDR Section Chief  
Email: Stephen.Cauffman@cisa.dhs.gov  
Phone: (703) 235-9532