

The Office of Infrastructure Protection

National Protection and Programs Directorate
Department of Homeland Security

Protective Security Coordination Division Assessments

George Mason University Symposium on Grid Security

October 25, 2017



Homeland
Security

Department of Homeland Security

- The Department of Homeland Security (DHS) is charged with providing “strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure” (Presidential Policy Directive – 21)
- The National Protection and Programs Directorate’s (NPPD) Office of Infrastructure Protection (IP) is the Department’s lead in the national coordination effort



**Homeland
Security**

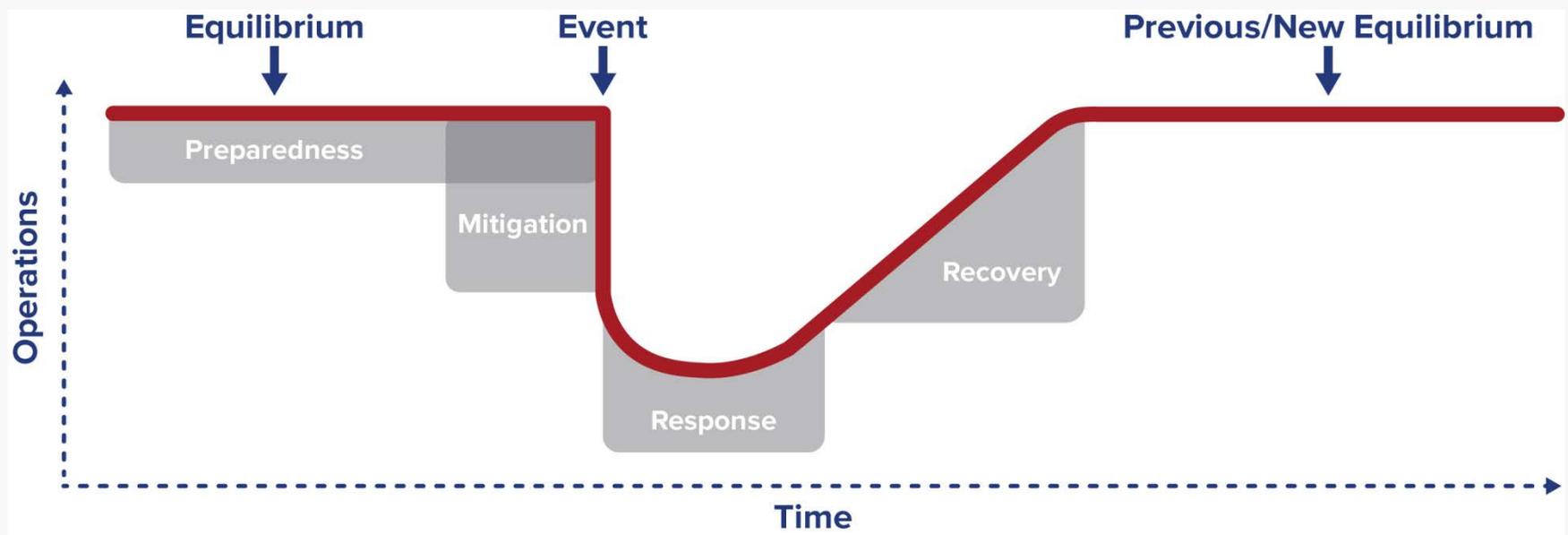
Infrastructure Protection and Resilience

2004



Homeland Security

Infrastructure Resilience



- Resilience: “the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions”



Assessments Overview



**Homeland
Security**

Infrastructure Survey Tool

- The Infrastructure Survey Tool (IST) is a voluntary, Web-based vulnerability survey facilitated by Protective Security Advisors to identify and document the overall security and resilience of a single facility
- Resulting survey information is provided to owners and operators of the facility
- Dashboards also highlight areas of potential concern and feature options to view the impact of potential enhancements to protection and resilience measures



Infrastructure Survey Tool (cont.)

- IST question set covers a variety of security features and resiliency characteristics:
 - Significant areas and assets
 - Physical security practices and barriers
 - Business continuity, security, and emergency plans
 - Dependency on electricity, natural gas, water, wastewater, communications, transportation, and information technology (IT)



Infrastructure Survey Tool (cont.)

- The tool allows DHS and facility owners and operators to:
 - Identify security gaps
 - Compare a facility's security in relation to similar facilities
 - Track progress toward improving critical infrastructure security
- Generates the Protective Measures Index (PMI) and Resilience Measurement Index (RMI)
- Since DHS started collecting this data, there have been more than 6000 surveys conducted
 - 800+ surveys in the energy sector, 600+ on electric power facilities



Resiliency Measures Index (RMI)

Preparedness

- Awareness
- Planning

Mitigation Measures

- Mitigating Construction
- Alternate Site
- Resources Mitigation Measures

Response Capabilities

- Onsite Capabilities
- Offsite Capabilities
- Incident Management and Command Center Characteristics

Recovery Mechanisms

- Restoration Agreements
- Recovery Time



IT Dependency

- The IT dependency questions cover IT management, cybersecurity practices, and data backup at a very high level
 - Questions cover both IT and OT cyber systems
- Some questions include:
 - Does the facility have an IT manager?
 - Does it participate in cybersecurity information sharing forums?
 - Does it have a cybersecurity plan?
 - Does it perform cyber assessments?
 - Does the facility backup its critical data?



Regional Resiliency Assessment Program

- The Regional Resiliency Assessment Program (RRAP) performs cooperative assessments of specific critical infrastructure within a designated geographic area and a regional analysis of the surrounding infrastructure to address a range of infrastructure resilience issues that could have regionally and nationally significant consequences
- Participation is voluntary and project outcomes are non-regulatory
 - Strong partnerships with Federal, State, local, tribal, and territorial government officials and private sector organizations are essential



Regional Resiliency Assessment Program (cont.)

- 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
 - Resolve infrastructure security and resilience knowledge gaps
 - Inform risk management decisions
 - Identify resilience-building opportunities and strategies
 - Improve critical partnerships among stakeholders



Benefits of the RRAP

- Data, analysis, and Key Findings can support existing or new infrastructure resilience enhancement efforts
 - Identify critical cross-sector issues, operational dependencies/chokepoints, planning/communications gaps, etc.
 - Confirm known resilience issues; propose solutions inclusive of less traditional partners
- Unique opportunity for relationship building, enhanced coordination and broader awareness among diverse yet interconnected stakeholders

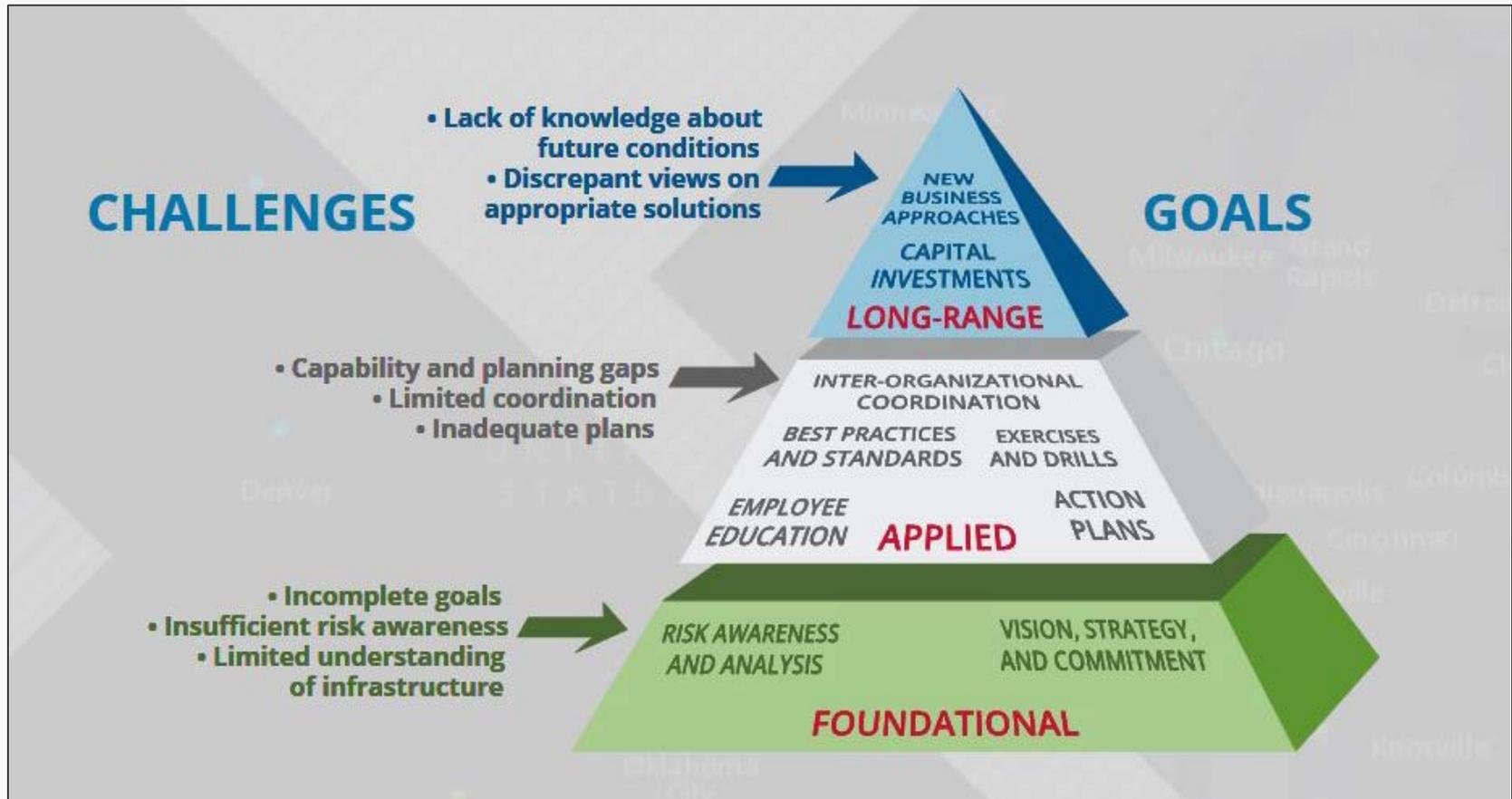


Knowledge Gaps

- What infrastructure exists in a region?
- How does the infrastructure operate and what does it need?
- How important is the infrastructure to the region?
- How are infrastructure systems interconnected?
- What hazards could most disrupt regional infrastructure?
- What capability and planning gaps exist in the region?
- Are there opportunities to strengthen resilience?



Resilience Building Solutions



RRAP History

- Conducted 80 projects through Fiscal Year 2017 which have covered a diverse set of critical infrastructure topics, sectors and regions
 - Energy is a commonly explored sector, given its criticality to other sectors
 - Eight RRAP projects focused on Electricity Subsector
- Major categories of findings have included:
 - Identification and enhanced assurance of infrastructure dependencies
 - Mitigation of physical vulnerabilities
 - Closing gaps in planning, procedures, analysis and training



So what?

- Though IST information is at a high-level, aggregated data can show general trends of capabilities and gaps
- IST information on a facility's dependencies, including time to detrimental impact and backup capabilities, can inform emergency response requirements
- RRAP projects tend to be “case studies”, looking at specific sectors of infrastructure within a specific geographic location
- Findings of past RRAP projects and ISTs can be analyzed and distilled into common themes, which may provide insight into sector trends





Homeland Security

For more information, visit:
www.dhs.gov/critical-infrastructure

Daniel Genua

Headquarters PSA

daniel.genua@hq.dhs.gov