Identifying Infrastructure Dependencies and Interdependencies

National Protection and Programs Directorate

September 6, 2018
The Nation’s Risk Managers

The National Protection and Programs Directorate (NPPD) is the pinnacle of national risk management for cyber and physical infrastructure.
Today's Risk Landscape

America remains at risk from a variety of threats:
16 Critical Infrastructure Sectors & Corresponding Sector-Specific Agencies

CHLICAL | IP
COMMERCIAL FACILITIES | IP
COMMUNICATIONS | DHS (CS&C)
CRITICAL MANUFACTURING | IP
DAMS | IP
DEFENSE INDUSTRIAL BASE | DOD
EMERGENCY SERVICES | IP
ENERGY | DOD
FINANCIAL | DOT
FOOD & AGRICULTURE | DOA & FDA
GOVERNMENT FACILITIES | DHS (FPS)
HEALTHCARE & PUBLIC HEALTH | HHS
INFORMATION TECHNOLOGY | DHS (CS&C)
NUCLEAR REACTORS, MATERIALS AND WASTE | IP
TRANSPORTATION SYSTEMS | (TSA & USCG)
WATER | EPA

Homeland Security
The Significance of Critical Infrastructure

Critical infrastructure refers to the assets, systems, and networks, whether physical or cyber, so vital to the Nation that their incapacitation or destruction would have a debilitating effect on national security, the economy, public health or safety, and our way of life.
Many Stakeholders, Many Strengths

Comparative Advantage
- Engaging in collaborative process
- Applying individual expertise
- Bringing resources to bear
- Building the collective effort
- Enhancing overall effectiveness
**Functions and Risk Management**

### Monitor
- Track how operational conditions impact function
- Share information and indicators of emerging systemic risk conditions

### Identify
- Document national functions
- Convene stakeholder groups connected by functions
- Identify and validate scenarios of concern

### Manage
- Develop collaborative strategies
- Coordinate risk management and monitoring plans

### Assess
- Conduct cross-sector risk assessments
- Improve risk analysis with shared data
## NISAC Strategic Framework

**Mission**: Provide homeland security decision makers with timely, relevant, high-quality analysis of cyber and physical risks to critical infrastructure across all sectors, during steady-state operations and crisis action.

**Vision**: A premier source of expert, innovative analysis and modeling that informs the Nation’s most significant cyber and physical infrastructure homeland security decisions.

### Support Focus Areas
- **Dependency and Interdependency Analysis**
- **Cyber Analysis**
- **Risk-Informed Prioritization**
- **Efficient and Effective Use of Resources**
- **Stakeholder Communication and Collaboration**
- **Information Technology Solutions**

### Objectives

#### Analytic Core Capabilities
- Modeling and Simulation
- Data Analysis
- Risk Analysis
- Domain Subject Matter Expertise

#### Enabling Core Capabilities
- Program Management
- Information Technology

**Values**: Innovation • Collaboration • Customer Service • Excellence
Infrastructure Dependencies

- Impacts to one infrastructure asset can cascade to other assets and systems
- Dependencies among infrastructure systems are complex
- Publicly-available data is sparse
- System owners and operators are reluctant to share detailed asset-level data
Example: Phillips 66 Bayway

Linden Cogen
345kv UG Line
Goethals Substation
AHA Dependency Framework

- Developed by Idaho National Laboratory
- Creates a knowledge framework that learns from data and expert knowledge
- Integrates structured and unstructured datasets
- Provides both geospatial and graph visualization capability due to problem space complexity
- Enables functions-based consequence analysis useful for continuity of operations
AHA Enables Risk Decisions

• Actionable information – Getting the best available information to the right person at the right time, and in a form they can efficiently use
  – Helps proactively answer the “What if”, for when an infrastructure fails
  – Provides scale-independent functional dependency modeling
  – Includes knowledge management & knowledge transfer
  – Can become useful for decision support
AHA Technical Approach
CASCADE
Example: Irma Tampa Impacts
Los Alamos National Laboratory developed an algorithm to automatically estimate training data starting from a real network.

Customized the algorithm for potable water systems: EPANET input files.

Developed a code to visualize an approximated graph of the training data.
Santa Fe Water System Example

Real Network

Grid

Coarse-Grained Graph Flow Rates

Training Data

Edges thickness = log(flow rate)

N = 25x25

N = 100x100
Water System Training Data

- Two types of training data
  - Infrastructure-related training data
    - Obtained from real networks
    - Used only to train the model
    - Correspond to an aggregation of flows of service (water, electricity)
  - Not infrastructure-related training data
    - Proxy variables
    - Publicly available
    - Used also as inputs to generate the coarse-grained model
    - Relevant data varies depending on the infrastructure

<table>
<thead>
<tr>
<th>Proxy Variables</th>
<th>Data source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Population density</td>
<td>CENSUS</td>
</tr>
<tr>
<td>Business type density*water factors</td>
<td>LANL database estimated from US Bureau of Economic Analysis/USGS</td>
</tr>
<tr>
<td>Elevation</td>
<td>Digital Elevation Models (DEM), USGS</td>
</tr>
<tr>
<td>Road</td>
<td>OpenStreetMap</td>
</tr>
</tbody>
</table>
## Draft NISAC Research Interests

<table>
<thead>
<tr>
<th>Dependency and Interdependency Analysis</th>
<th>Cyber Analysis</th>
<th>Risk-Informed Prioritization</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Objective 1.1</strong>: Capability to identify or assign dependency relationships for lifeline sectors and assets within regionally significant industrial clusters, across all U.S. regions.</td>
<td><strong>Objective 2.1</strong>: Strengthen DHS’ ability to assess the impact of cyber attacks and cyber disruptions on critical infrastructure operations.</td>
<td><strong>Objective 3.1</strong>: Implement an approach to use National Critical Functions to understand dependencies and the effects of infrastructure disruptions on these functions.</td>
</tr>
<tr>
<td><strong>Objective 1.2</strong>: Improve DHS’s ability to provide accurate and timely analysis of the impacts of disruptions to the lifeline critical infrastructure systems.</td>
<td><strong>Objective 2.2</strong>: Develop methodologies to characterize the criticality of Federal networks and better estimate the consequences of their disruption.</td>
<td><strong>Objective 3.2</strong>: Improve DHS’ capacity to identify and communicate areas of greatest strategic infrastructure risk.</td>
</tr>
<tr>
<td><strong>Objective 1.3</strong>: Improve data, information, and heuristics related to infrastructure dependencies.</td>
<td><strong>Objective 2.3</strong>: Improve DHS’s ability to anticipate emerging cyber risk by using innovative and advanced techniques to analyze evolving cyber threats, vulnerabilities, and trends.</td>
<td><strong>Objective 3.3</strong>: Capability to analyze and communicate nationally, regionally, and functionally significant systemic risks—including cyber risks—across and within infrastructure sectors.</td>
</tr>
<tr>
<td><strong>Objective 1.4</strong>: Provide DHS analysts and field personnel with analytic tools to understand infrastructure dependencies.</td>
<td></td>
<td><strong>Objective 3.4</strong>: Improve homeland security decision makers understanding of how to apply risk-informed priorities.</td>
</tr>
</tbody>
</table>