NATIONAL RISK
MANAGEMENT CENTER
DHS Position Navigation and Timing Update
CGSIC September 2021

“DEFEND TODAY,
SECURE TOMORROW.”
We are the Nation’s Risk Advisor

The Cybersecurity and Infrastructure Security Agency (CISA) is the pinnacle of national risk management for cyber and physical infrastructure.
Cybersecurity and Infrastructure Security Agency (CISA)

**VISION**
Secure and resilient infrastructure for the American people.

**MISSION**
CISA partners with industry and government to understand and manage risk to our Nation’s critical infrastructure.

**OVERALL GOALS**

**GOAL 1**
**DEFEND TODAY**
Defend against urgent threats and hazards
- seconds | days | weeks

**GOAL 2**
**SECURE TOMORROW**
Strengthen critical infrastructure and address long-term risks
- months | years | decades
National Risk Management Center

The NRMC is a planning, analysis, and collaboration center. CISA coordinates with the critical infrastructure community to identify; analyze; prioritize; and manage risks to National Critical Functions, which are vital to the United States.

MISSION PRIORITIES:

- Analyzes most strategic risks to our Nation’s critical infrastructure
- Leads public/private partnership initiatives to manage priority areas of national risk
- Collaborates with the private sector and other stakeholders to better understand future threats.
NRMC’s Top Initiatives

<table>
<thead>
<tr>
<th>Initiative</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5G</td>
<td>Securing the next generation of wireless technology which transforms U.S. telecommunication networks and empowers critical services.</td>
</tr>
<tr>
<td>Election Security</td>
<td>Ensuring America’s election infrastructure is resilient as we #Protect2020.</td>
</tr>
<tr>
<td>Electromagnetic Pulse &amp; Geomagnetic Disturbance</td>
<td>Mitigating potential nuclear and space weather events that can affect large areas of our Nation.</td>
</tr>
</tbody>
</table>
NRMC’s Top Initiatives Cont’d

ICT Supply Chain Risk Management
Reducing risk of vulnerabilities in the ICT supply chain, that if exploited, can affect all users of that technology.

Pipeline Cybersecurity
In-depth review and evaluation of the control system’s network design, configuration, and interdependencies for more than 2.7 million miles of pipelines.

Positioning, Navigation, and Timing
Understanding how positioning, navigation, and timing services is used across all NCFs.
Critical Infrastructure Risks

In today’s rapidly evolving threat environment, sources of strategic risk are widespread and include:

- Cyber and Physical Security Threats
- Convergence of Previously Siloed Threat Vectors
- Insider Threats
- Malicious Exploits of Emerging Technology
- Misinformation and Disinformation
- Nation-State Aggression
- Pandemics and Natural Disasters
- Supply Chain Vulnerabilities
It’s less about who you are and more about the functions you produce or enable.

NCFs better capture cross-cutting risks and associated dependencies.

<table>
<thead>
<tr>
<th>CONNECT</th>
<th>DISTRIBUTE</th>
<th>MANAGE</th>
<th>SUPPLY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operate Core Network</td>
<td>Distribute Electricity</td>
<td>Conduct Elections</td>
<td>Exploration and Extraction Of Fuels</td>
</tr>
<tr>
<td>Provide Cable Access Network Services</td>
<td>Maintain Supply Chains</td>
<td>Develop and Maintain Public Works and Services</td>
<td>Fuel Refining and Processing Fuels</td>
</tr>
<tr>
<td>Provide Internet Based Content, Information, and Communication Services</td>
<td>Transmit Electricity</td>
<td>Educate and Train</td>
<td>Generate Electricity</td>
</tr>
<tr>
<td>Provide Internet Routing, Access and Connection Services</td>
<td>Transport Cargo and Passengers by Air</td>
<td>Enforce Law</td>
<td>Manufacture Equipment</td>
</tr>
<tr>
<td>Provide Radio Broadcast Access Network Services</td>
<td>Transport Cargo and Passengers by Road</td>
<td>Manage Hazardous Materials</td>
<td>Produce and Provide Human and Animal Food Products and Services</td>
</tr>
<tr>
<td>Provide Satellite Access Network Services</td>
<td>Transport Cargo and Passengers by Vessel</td>
<td>Manage Wastewater</td>
<td>Produce Chemicals</td>
</tr>
<tr>
<td>Provide Wireless Access Network Services</td>
<td>Transport Materials by Pipeline</td>
<td>Operate Government</td>
<td>Provide Metals and Materials</td>
</tr>
<tr>
<td>Provide Wireline Access Network Services</td>
<td>Transport Passengers by Mass Transit</td>
<td>Perform Cyber Incident Management Capabilities</td>
<td>Provide Housing</td>
</tr>
</tbody>
</table>

James Platt  
September 17, 2021
Considering PNT in Risk Management

- Responsible use of PNT services” means the deliberate, risk-informed use of PNT services, including their acquisition, integration, and deployment, such that disruption or manipulation of PNT services minimally affects national security, the economy, public health, and the critical functions of the Federal Government.
PNT EO

EO 13905: ...the Secretary of Homeland Security, in coordination with the heads of SSAs, shall develop a plan to test the vulnerabilities of critical infrastructure systems, networks, and assets in the event of disruption and manipulation of PNT services.

Engineering Considerations

- What are your critical Systems, Networks and Assets?
- Do they use, or are they dependent, on external PNT sources?
- What level of precision do I need?
- Can you identify the disruption or manipulation of PNT services?
- How do you maintain critical functions if external PNT is impaired?
PNT EO

EO 13905: ...the Secretary of Homeland Security, in coordination with the heads of SSAs, shall develop a plan to test the vulnerabilities of critical infrastructure systems, networks, and assets in the event of disruption and manipulation of PNT services.

PNT SME Considerations

- What sources of PNT are available?
- What are their performance characteristics?
- Can you identify the disruption or manipulation of PNT services?
- How can you make the PNT services more resilient?
NRMC Resources

Visit us online:  
www.cisa.gov/national-risk-management

Download outreach products/resources:  
www.cisa.gov/nrmc-resources