

The background of the slide is a nighttime cityscape with a network overlay. The city lights are visible through a semi-transparent dark blue layer. Overlaid on this is a network of white lines connecting various glowing nodes in shades of blue and cyan. The nodes are positioned at various points across the cityscape, suggesting a global or interconnected network.

National Risk Management Center (NRMC)

PNT Advisory Board

James Platt, CISA

June 2019

Overall Classification: Unclassified//For Official Use Only

National Risk Management Center (NRMC)

The NRMC is CISA's planning, analysis, and collaboration center working to identify and address the most significant risks to the Nation's critical infrastructure.

The NRMC works in close coordination with other divisions and components of CISA including the Cybersecurity Division, Infrastructure Security Division, Emergency Communications Division, and National Cybersecurity and Communications Integration Center.

National Critical Functions

The functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on either the Nation's homeland security, economic security, public health or safety, or any combination thereof.

NRMC Strategic Risk Management Process



National Critical Functions

- Better captures cross-cutting risks and associated dependencies.
- It's not who you are. It's the functions you produce or enable.
- Featured prominently in the National Cyber Strategy and DHS Cybersecurity Strategy.

National Critical Functions set the stage for:

1. Support for Infrastructure Prioritization
2. Conducting Subordinate Analysis
3. Informing Intelligence Collection Requirements
4. Setting Incident Management Priorities
5. Supporting Investments in Security and Resilience
6. Countering Foreign Influence

National Critical Functions – Current Status

- Set of functions published in April
- Tri Sector Executive Working Group set the foundation for NCF work.
- All 16 Sector Coordinating Councils, all associated Sector Specific Agencies, and the SLTT GCC participated heavily in this iterative process.
- The process itself was valuable and revealed several important insights – including widespread, cross-sector dependency on **PNT** and cloud computing.

Next steps:

The NCF Set will be used as an input for subsequent risk and dependency analysis and consequence modeling of scenarios that could potentially cause national-level degradation to NCF. This will create a tiered risk register to prioritize risk management activity.

National Critical Functions Set

CONNECT	DISTRIBUTE	MANAGE	SUPPLY
<ul style="list-style-type: none"> ▪ Operate Core Network ▪ Provide Cable Access Network Services ▪ Provide Internet Based Content, Information, and Communication Services ▪ Provide Internet Routing, Access, and Connection Services ▪ Provide Positioning, Navigation, and Timing Services ▪ Provide Radio Broadcast Access Network Services ▪ Provide Satellite Access Network Services ▪ Provide Wireless Access Network Services ▪ Provide Wireline Access Network Services 	<ul style="list-style-type: none"> ▪ Distribute Electricity ▪ Maintain Supply Chains ▪ Transmit Electricity ▪ Transport Cargo and Passengers by Air ▪ Transport Cargo and Passengers by Rail ▪ Transport Cargo and Passengers by Road ▪ Transport Cargo and Passengers by Vessel ▪ Transport Materials by Pipeline ▪ Transport Passengers by Mass Transit 	<ul style="list-style-type: none"> ▪ Conduct Elections ▪ Develop and Maintain Public Works and Services ▪ Educate and Train ▪ Enforce Law ▪ Maintain Access to Medical Records ▪ Manage Hazardous Materials ▪ Manage Wastewater ▪ Operate Government ▪ Perform Cyber Incident Management Capabilities ▪ Prepare for and Manage Emergencies ▪ Preserve Constitutional Rights ▪ Protect Sensitive Information ▪ Provide and Maintain Infrastructure ▪ Provide Capital Markets and Investment Activities ▪ Provide Consumer and Commercial Banking Services ▪ Provide Funding and Liquidity Services ▪ Provide Identity Management and Associated Trust Support Services ▪ Provide Insurance Services ▪ Provide Medical Care ▪ Provide Payment, Clearing, and Settlement Services ▪ Provide Public Safety ▪ Provide Wholesale Funding ▪ Store Fuel and Maintain Reserves ▪ Support Community Health 	<ul style="list-style-type: none"> ▪ Exploration and Extraction Of Fuels ▪ Fuel Refining and Processing Fuels ▪ Generate Electricity ▪ Manufacture Equipment ▪ Produce and Provide Agricultural Products and Services ▪ Produce and Provide Human and Animal Food Products and Services ▪ Produce Chemicals ▪ Provide Metals and Materials ▪ Provide Housing ▪ Provide Information Technology Products and Services ▪ Provide Materiel and Operational Support to Defense ▪ Research and Development ▪ Supply Water
<p>National Critical Functions: The functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.</p>			

ICT Supply Chain Risk Management Task Force

- NRMC Director serves as the government co-chair.
- Task Force includes 20 members each from the IT Sector, Communications Sector, and the interagency.
- Task Force recently launched four main work streams:
 - Developing a common framework for the bi-directional sharing of supply chain risk information between government and industry.
 - Identification of processes and criteria for threat-based evaluation of ICT supplies, products, and services.
 - Identification of market segment(s) and evaluation criteria for Qualified Bidder and Manufacturer List(s).
 - Producing policy recommendations to incentivize the purchase of ICT from original equipment manufacturers or authorized resellers.
- Task Force intends to be one of the primary touch points between government and industry for the newly created Federal Acquisition Security Council.

ICT Supply Chain Risk Management Task Force

- **Industry Members**: Accenture, AT&T, BSA, CenturyLink, Charter Communications, Cisco Systems, Comcast, Cox, CTIA, CyberRx, Cybersecurity Coalition, Cyxtera, Dell, FireEye, General Dynamics Information Technology, HP, IBM, Iconectiv, IT-ISAC, Information Technology Industry Council, Intel, Interos Solutions, Microsoft, National Association of Broadcasters, NCTA, NTCA, NTT, Palo Alto Networks, Pioneer, Samsung, Sprint, Synopsys, Threatsketch, TIA, T-Mobile, USTelecom, and Verizon Wireless.
- **Government Members**: Commerce, DOD, Energy, DHS (CISA, OPO, CIO), DOJ, Treasury, FBI, FCC, GSA, NASA, NSA, OCC, NRC, ODNI, SSA.

SUPPLY CHAIN RISKS for Information and Communication Technology

U.S. critical infrastructure relies on Information and Communications Technology (ICT)—defined by the National Institute of Standards and Technology as “the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information”—for daily operations and functionality. The Design, Development and Production, Distribution, Acquisition and Deployment, Maintenance, and Disposal phases of the ICT supply chain are susceptible to the malicious or inadvertent introduction of vulnerabilities such as malicious software and hardware; counterfeit components; and poor product designs, manufacturing processes, and maintenance procedures.

Exploitation of ICT supply chain vulnerabilities can lead to: system reliability issues, data theft and manipulation, malware dissemination, and persistent unauthorized access within networks. This infographic provides leaders at all levels of government and industry insight into how vulnerabilities can be introduced into the ICT supply chain, and the consequences of their exploitation.



1. DESIGN

Vulnerabilities introduced during Design are often unintentional and can potentially affect all users of the components. Malicious actors could integrate vulnerabilities into components that may be installed in millions of pieces of equipment.



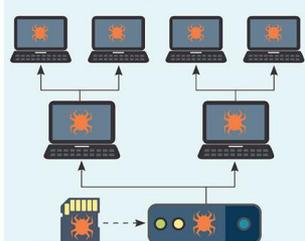
HIJACKED CELLULAR DEVICES

2016—A foreign company designed firmware used by a U.S. cell phone manufacturer. The phones made encrypted records of text and call histories, phone details, and contact information and transmitted that data to a foreign server every 72 hours.



2. DEVELOPMENT AND PRODUCTION

Vulnerabilities introduced during this phase are often inadvertent and can be costly to fix if not identified when testing initial prototypes. Well-designed products may still have malicious components introduced during manufacturing and assembly in a way that is potentially difficult to identify.



INFECTED SWITCH FLASH CARDS

2012—A third party factory that produced switches designed by a U.S. company installed infected compact flash cards during production. The U.S. company warned that using an infected component could compromise the system and potentially spread the malware within the network.



3. DISTRIBUTION

Components transported between production facilities and customers often do not fall under the purview of the personnel responsible for their design or production. Vulnerabilities introduced during Distribution are likely to be malicious and affect a limited number of components and customers compared to earlier phases.



END USER DEVICE MALWARE

2012—Researchers from a major U.S. software company investigating counterfeit software found malware pre-installed on 20% of devices they tested. The malware was installed in new desktops and laptop computers after they were shipped from a factory to a distributor, transporter, or reseller.



4. ACQUISITION AND DEPLOYMENT

Malicious insiders may insert vulnerabilities or replace equipment with vulnerable components during acquisition or installation. Vulnerabilities introduced during this phase likely affect only a limited number of customers.



COUNTERFEITS SOLD TO U.S. NAVY

2015—A U.S. citizen imported thousands of counterfeit integrated circuits from China and Hong Kong, and resold them to U.S. customers, including Defense contractors supplying them to the U.S. Navy for use in nuclear submarines.



5. MAINTENANCE

ICT components receiving Maintenance are susceptible to vulnerabilities introduced through physical or network access, and from exploitation of previously unknown or unpatched vulnerabilities. Vulnerabilities introduced during Maintenance might be targeted against specific entities, but can affect many customers in the case of software updates.



MALWARE EMBEDDED WITHIN SOFTWARE SECURITY TOOL

2017—Malicious actors attacked a security software company by infiltrating its network and inserting code into security software. Installs and updates to the application landed in millions of personal computers. The attack targeted predominant IT company networks.



6. DISPOSAL

ICT components that are improperly disposed of can contain sensitive company or customer data. Malicious actors can also attempt to refurbish components and try to resell them as new. Used parts may be less reliable and prone to failure, or have malware installed.



SENSITIVE FEDERAL DATA LOSS

2010—An internal audit discovered that a federal agency was selling computers containing proprietary information. Certain devices failed sanitation verification tests and resulted in the release of sensitive federal agency data.

5G Risk Overview

- The NRMCA Analysis Division is conducting an assessment of the risks 5G adoption could introduce in the United States.
- NRMCA has conducted an initial review of the potential vulnerabilities of 5G, and the likelihood of those vulnerabilities being exploited.
- NRMCA is working with industry and other partners to better understand how potential 5G vulnerabilities are being mitigated and how likely those vulnerabilities could be exploited.
 - This will be used to develop a more complete risk characterization.

EMP/GMD Risk Assessments

- Established and staffed DHS/CISA EMP Coordinator position.
- Developed analysis framework that incorporates SSAs and other interagency partners.
- Developed DHS R&D requirements that support analysis framework for prioritization by DHS S&T.
- Coordinating with the NSC, CISA components and interagency partners to develop R&D and analysis portfolios to implement the EMP Executive Order and the DHS EMP Strategy.

Next steps:

- Technical collaboration with DOE and DOD to develop standardized EMP threats to enable integrated analyses by interagency partners.
- Initiate projects to scope EMP vulnerabilities in key infrastructure systems.

Analytic Horsepower - NISAC

- The National Infrastructure Simulation and Analysis Center (NISAC) conducts modeling, simulation, and analysis of cyber and physical risks to critical infrastructure, during steady-state operations and crisis action.
- NISAC is developed and managed by the NRMCC and comprised of a diverse group of expert performers, including the National Laboratories.
- The NRMCC is aggressively working to ensure NISAC projects improve CISA's ability to identify, assess, prioritize, and provide deep insight into strategic risks to National Critical Functions.

Recent and upcoming DHS PNT

- Information Sheets “Are you Managing your time?”
- Development of best practices for testing your timing architecture (participants wanted)
- Conformance Standards
- Multi-GNSS vulnerabilities and opportunities
- Support to National Defense Authorization Acts
 - FY 17
 - FY 18
- National Timing Security and Resilience Act



CISA
CYBER+INFRASTRUCTURE

National Risk Management Center