Cybersecurity and Infrastructure Security Agency
National Risk Management Center

National Risk Management Center (NRMC)

March 2019

Overall Classification: Unclassified

CISA
CYBER+INFRASTRUCTURE

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.

CISA
CYBER+INFRASTRUCTURE

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.

CISA
CYBER+INFRASTRUCTURE

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

CISA
CYBER+INFRASTRUCTURE

National Critical Functions – Current Status

- Set of functions is currently being finalized and is expected to be 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 set of NCF 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.

CISA
CYBER+INFRASTRUCTURE

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.

CISA
CYBER+INFRASTRUCTURE

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.

CISA
CYBER+INFRASTRUCTURE

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

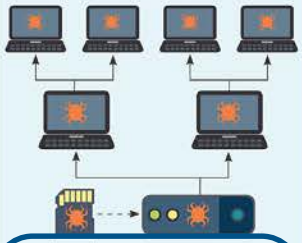
Vulnerabilities introduced during Design are often unintentional and can potentially affect all users of the components. Malicious actors could integrate vulnerabilities into components that may be installed in millions of pieces of equipment.

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.

CISA
CYBER+INFRASTRUCTURE

5G Risk Overview

- The NRMC Analysis Division is conducting an assessment of the risks 5G adoption could introduce in the United States.
- NRMC has conducted an initial review of the potential vulnerabilities of 5G, and the likelihood of those vulnerabilities being exploited.
- NRMC 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.
- NRMC is conducting this analysis at a high level, and does not assess specific threats or technical vulnerabilities and risks.

CISA
CYBER+INFRASTRUCTURE

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.

CISA
CYBER+INFRASTRUCTURE

Other Areas of Risk Management Focus

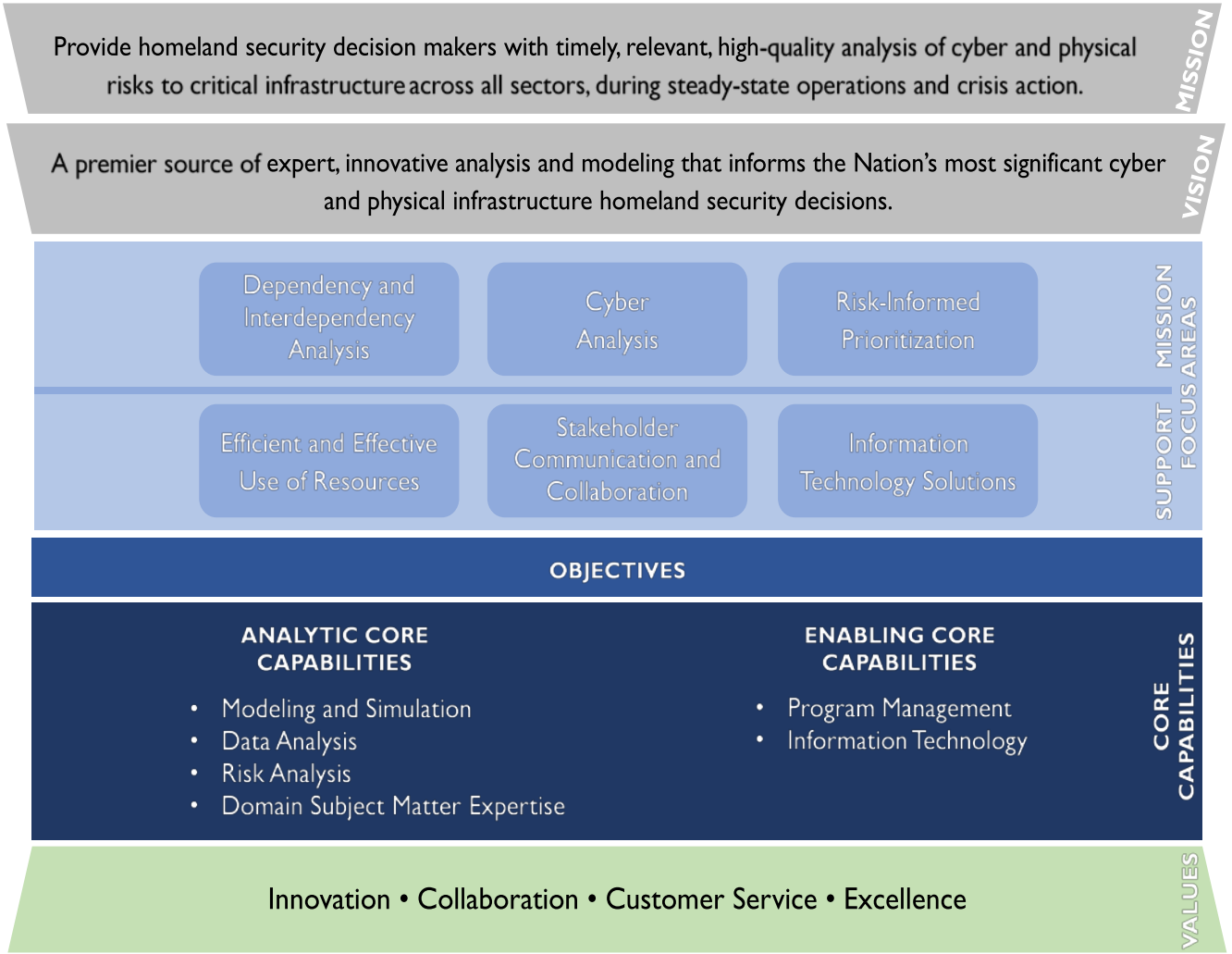
- The NRMC is also working on a range of issues outside core initiatives to address long-term critical infrastructure risks in partnership with industry. They include:
  - Renewing liaison efforts with undersea cable owners and operators to mitigate risk through increased information sharing.
  - Enabling risk mitigation decision making about use of Unmanned Aerial Systems.
  - **Assessing resilience gaps in Position, Navigation and Timing services.**
  - Support analysis on CFIUS issues.
- The NRMC provides CISA with capabilities to connect analysis, planning and partnerships on systemic risk issues and help “secure tomorrow” while enabling technology innovation.

CISA
CYBER+INFRASTRUCTURE

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 NRMC and comprised of a diverse group of expert performers, including the National Laboratories.
- The NRMC 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.

NISAC Strategy



CISA
CYBER+INFRASTRUCTURE

Recent and upcoming DHS PNT

- Information Sheets “Are you Managing your time?”
- Development of best practices for testing your timing architecture (participants wanted)
- NIST Workshop on Conformance Standards
- GPS Roll Over
- 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