NCCIC | National Cybersecurity and Communications Integration Center

INTERNATIONAL PORT SECURITY WORKSHOP

April 26, 2017

John M. Felker
Director, NCCIC

NCCIC

UNCLASSIFIED

NCCIC Overview

The NCCIC's mission is to:

Reduce the likelihood and severity of cyber and communications

Support security and resilience of the Nation's critical infrastructure and government systems incidents

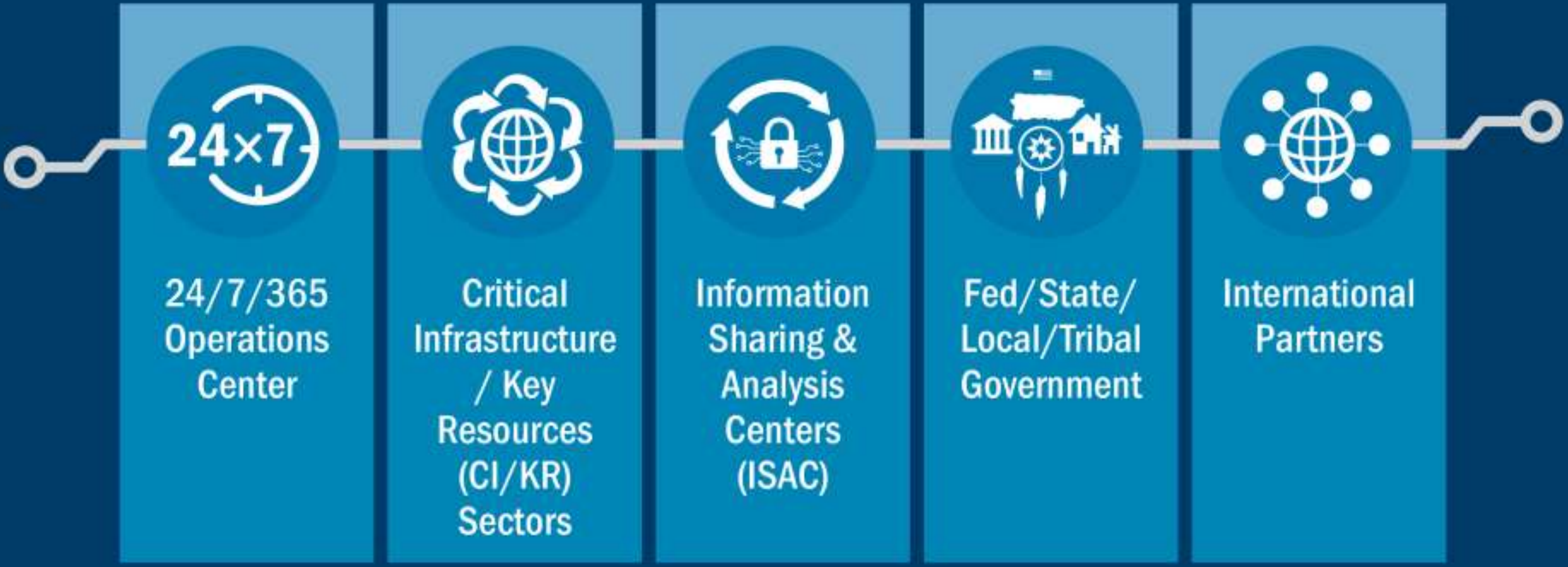
Core Functions

NCCIC performs a suite of functions that provide customers with comprehensive risk management capabilities, products, and services. These functions include:

- Information sharing
- Operational planning, training, and exercises
- Risk and vulnerability assessments
- Data synthesis and analysis
- Watch floor operations
- Hunt, incident response, and recovery

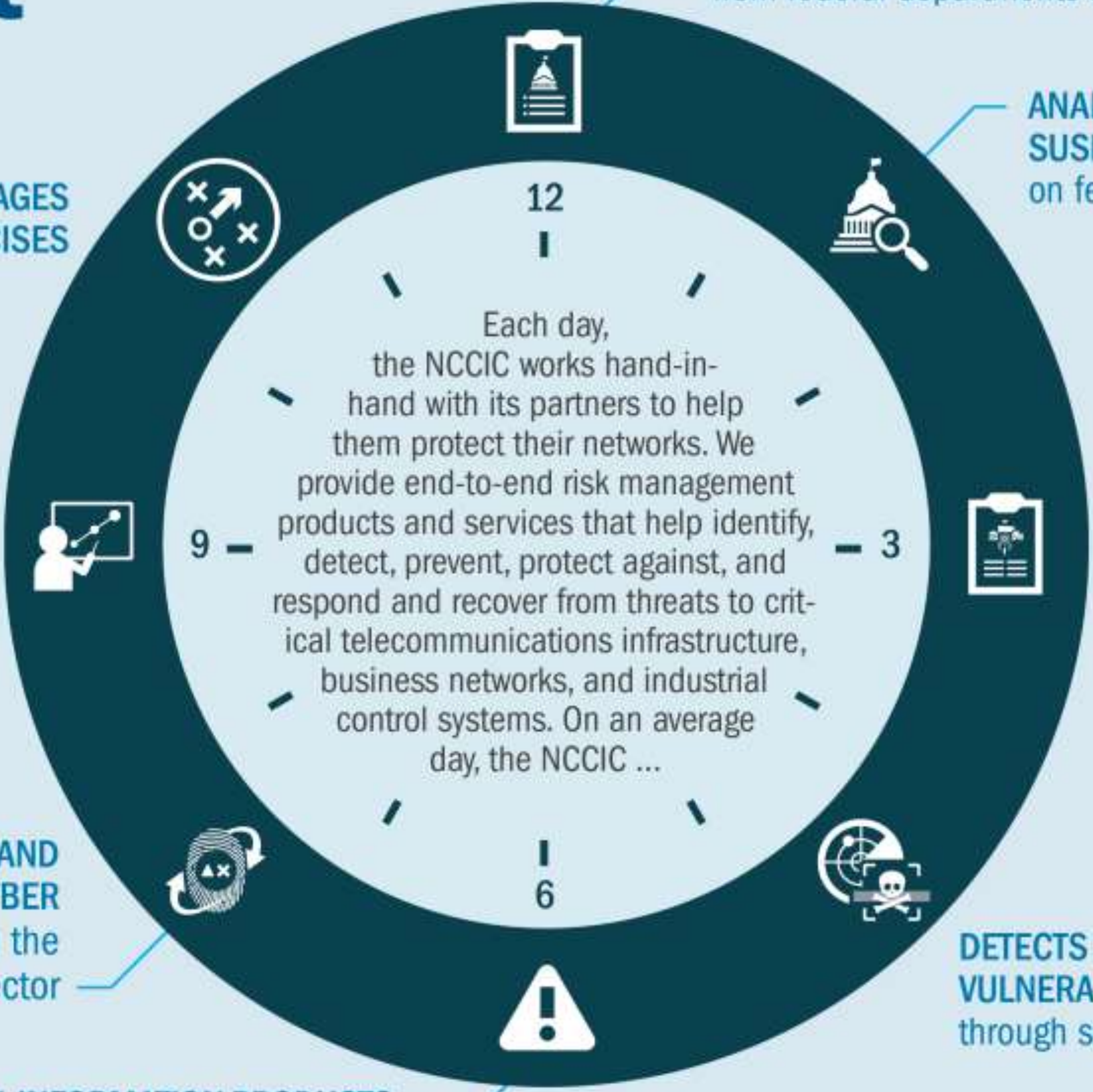
NCCIC Pillars and Capabilities

NCCIC In-House and Virtual Capabilities



- 24/7/365 Operations Center
- Critical Infrastructure / Key Resources (CI/KR) Sectors
- Information Sharing & Analysis Centers (ISAC)
- Fed/State/Local/Tribal Government
- International Partners

A Day at NCCIC



Each day, the NCCIC works hand-in-hand with its partners to help them protect their networks. We provide end-to-end risk management products and services that help identify, detect, prevent, protect against, and respond and recover from threats to critical telecommunications infrastructure, business networks, and industrial control systems. On an average day, the NCCIC ...

Receives **117 INCIDENT REPORTS** from federal departments and agencies

ANALYZES 207 SUSPICIOUS ALERTS on federal networks

RECEIVES 181 state and local incident reports

DETECTS 360 VULNERABILITIES through scanning

DISTRIBUTES 61 INFORMATION PRODUCTS such as newly identified vulnerabilities and threat alerts

SHARES NINE CLASSIFIED AND 127 UNCLASSIFIED CYBER THREAT INDICATORS with the private sector

Helps students complete **41 ICS TRAINING MODULES** online

Is **TRAINING 42 PEOPLE** in its state-of-the-art industrial controls system laboratory

PLANS OR MANAGES TWO CYBER EXERCISES

You’ve been hacked or you don’t know you’ve been hacked!

Cyber threats could

- commandeer a ship,
- shut down a port or terminal,
- alter manifests or container numbers,
- disclose sensitive pricing documents,
- cause lost business and
- produce third-party liability.

Potential for worldwide economic and security implications/ impact:
loss of revenue,
loss of life,
environmental
damage.

Maritime industry not yet the focus of hackers and criminals

As mature industries shore up cyber defenses, **attacks will be redirected** to softer targets (the unprepared!)

Human error (USB or email introduced malware; insider threat)

Systems (ICS, AIS, GPS, ECDIS) targeted via always on Internet connection

Partnerships and Information Sharing

Know your maritime cyber-specific risks and inter-dependencies

Conduct a risk assessment to identify your vulnerabilities

Incorporate cybersecurity into business practices and operations

Educate your workers to increase cyber awareness

Partner with Port players and share information to

- Develop a strategic Plan addressing cyber elements
- Defend against cyber attacks and vulnerability exploits
- Improve port infrastructure
- Prepare for emergent cyber threats

Maritime Cyber Security: Be Aware

Cyber attackers are motivated, innovative, and efficient.

Interconnectivity makes everyone is a target.

Know your enemy.

Know your friend:
The NCCIC works closely with the Coast Guard in recording reports of suspicious cyber activity or breach of cybersecurity at MTSA entities.

Homeland Security

For more information:

www.DHS.gov/about-national-cybersecurity-communications-integration-center

www.DHS.gov/Cyber

www.DHS.gov/Office-Cybersecurity-and-Communications

Questions?

Email: ncciccustomerservice@hq.dhs.gov

Phone: 888-282-0870

U.S. DEPARTMENT OF HOMELAND SECURITY

NCCIC