TLP:WHITE

DHS | DEPARTMENT OF HOMELAND SECURITY

CYBERSECURITY

AWARENESS BRIEFING:

PROTECTING ENTERPRISE NETWORK INFRASTRUCTURE DEVICES

9/24/18

NCCIC

DISCLAIMER

This report is provided “as is” for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this bulletin or otherwise. This document is marked TLP:WHITE. Subject to standard copyright rules. TLP:WHITE information may be distributed without restriction. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

For more information on the Traffic Light Protocol,
see ***https://www.us-cert.gov/tlp***.

Welcome

Reggie McKinney
Department of Homeland Security

AGENDA

Welcome: Reggie McKinney, DHS Cyber

NCCIC Overview: Denise, DHS Cyber/NCCIC

Panel Presentations:

- Matt, *Network Analyst,* DHS Cyber/NCCIC
- Justin, *Network Analyst,* DHS Cyber/NCCIC
- Brad, *Network Analyst,* DHS Cyber

NCCIC Resources: Denise

Q&A

Closing: Reggie McKinney

TLP:WHITE

National Cyber Security Awareness Month

Commemorating its 15th year, **N**ational **C**ybersecurity **A**wareness **M**onth **(NCSAM)** 2018 is a collaborative effort between government and industry to ensure every American has the resources they need to stay safer and more secure online, and increase the country’s resiliency during cyber incidents.

Improve our Nation’s Cybersecurity

NCSAM 2018 will emphasize cybersecurity as a shared responsibility, and will encourage Americans to incorporate these core actions into their daily digital activity.

Strengthen the Nation’s Cybersecurity Ecosystem

Contribute and commit to strengthening the Nation’s cyber ecosystem

Tackle it Together

Cybersecurity is a cross-cutting, cross-sector problem, so we have go to tackle it together

Build up the Cybersecurity Workforce

Increase and strengthen the cybersecurity workforce across all sectors

Protect Critical Infrastructure

Heighten resilience and understand how to best protect critical infrastructure from cyber threats

National Cybersecurity
Awareness Month

www.dhs.gov/ncsam

TLP:WHITE

Housekeeping

Questions can be submitted in the chat box throughout the webinar and during the Q&A.

Please complete the short survey following the webinar.
We appreciate your feedback.

TLP:WHITE

NCCIC | NATIONAL CYBERSECURITY & COMMUNICATIONS INTEGRATION CENTER

NCCIC OVERVIEW

U.S. DEPARTMENT OF HOMELAND SECURITY

NCCIC

NCCIC Overview

Vision and Mission

Secure and robust cyber and communications infrastructure, resilient against attacks and disruption

Reduce the risk of systemic cybersecurity and communications challenges in our role as the Nation’s flagship of cyber defense, incident response and operational integration center

Mission Essential Functions (MEFs)

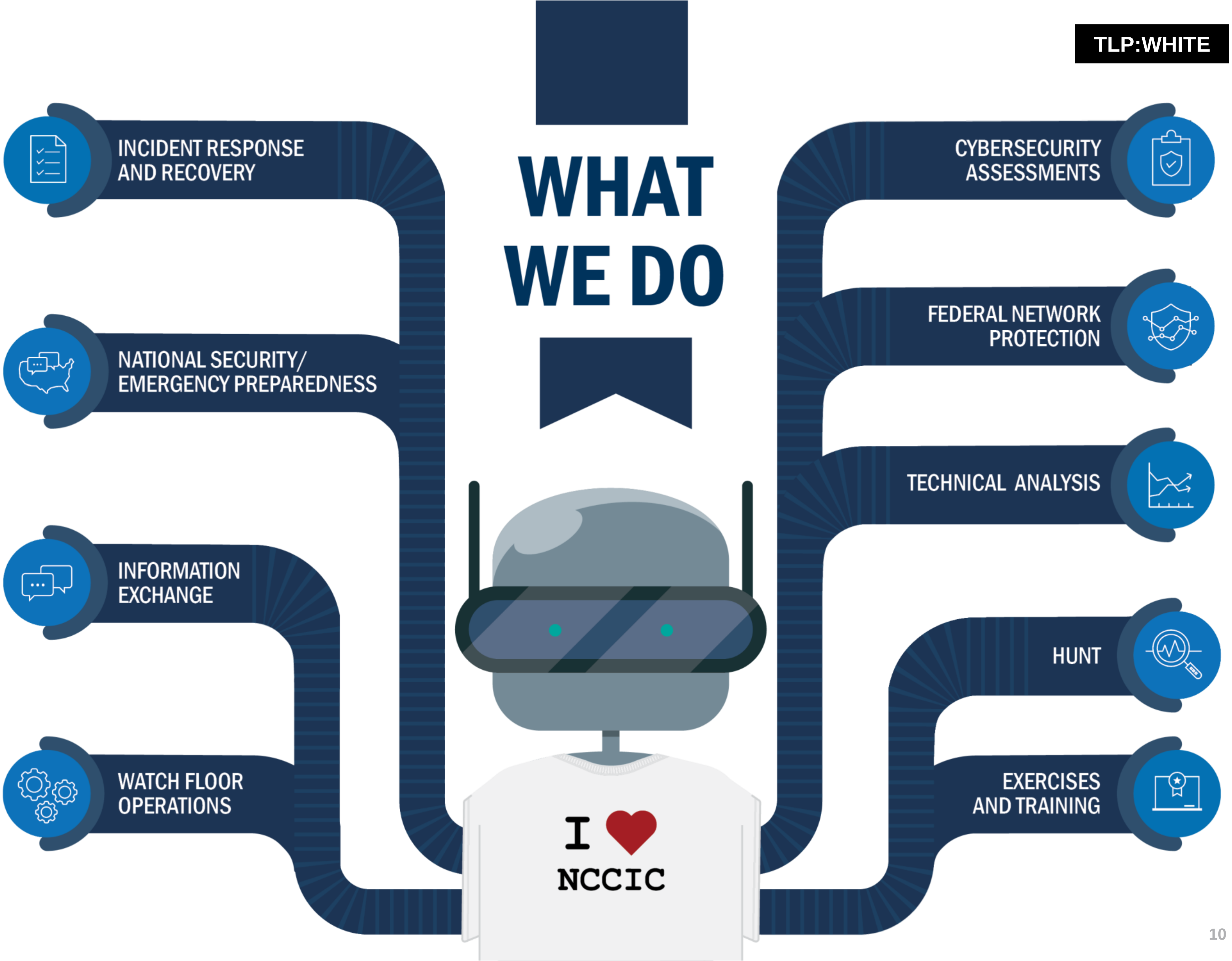
Incident Management: Manage cyber and communications incidents in real time to mitigate impacts and reduce risks to critical systems

Analysis: Conduct analyses to recognize threats and vulnerabilities, identify countermeasures, and develop situational awareness

Capacity Building: Build capacity across all levels of government and the private sector to improve management of cyber and communications risks

Information Sharing: Share information about cyber and communications risks to support stakeholder decisions and actions

WHAT WE DO



- INCIDENT RESPONSE AND RECOVERY
- NATIONAL SECURITY/ EMERGENCY PREPAREDNESS
- INFORMATION EXCHANGE
- WATCH FLOOR OPERATIONS
- CYBERSECURITY ASSESSMENTS
- FEDERAL NETWORK PROTECTION
- TECHNICAL ANALYSIS
- HUNT
- EXERCISES AND TRAINING

TLP:WHITE

DHS | DEPARTMENT OF HOMELAND SECURITY

CYBERSECURITY

THREATS & EXPOSURES

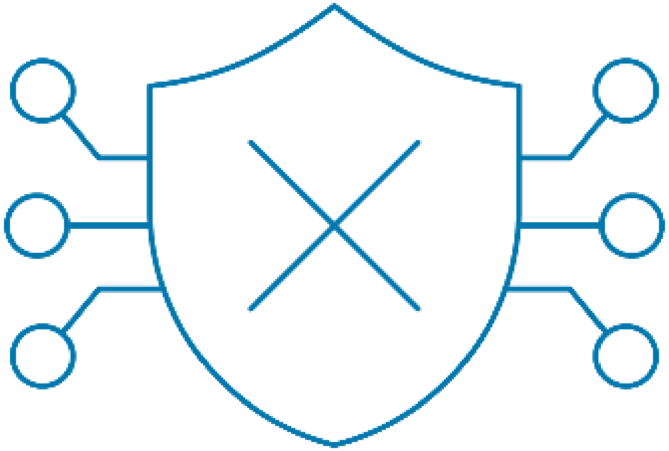
Matt

Network Analyst

NCCIC

NCCIC

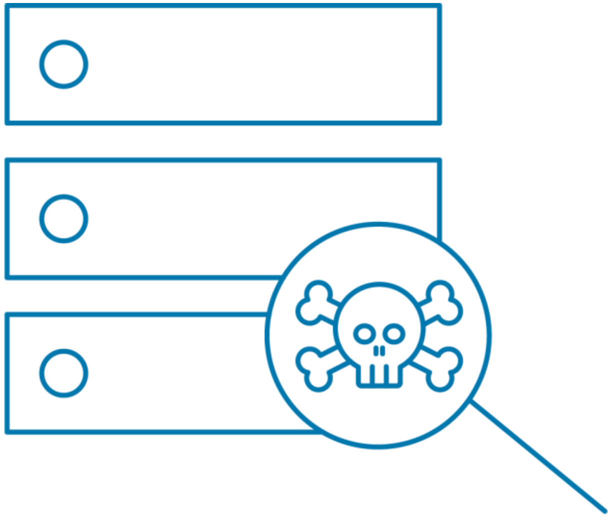
Why Network Infrastructure Devices



1. **Routers and Switches** are the backbones of networks. Firewalls and Network Intrusion Detection Systems provide access control and monitoring.
2. **Maintenance** is often lacking.
3. **Own the router**, own the traffic.

TLP:WHITE

Threats to Enterprise Networking Devices

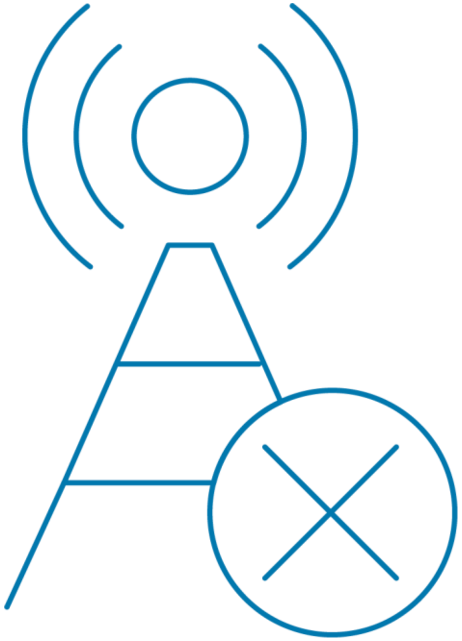


1. **Denial of Service** (DoS) attacks which threaten the availability of the device and its dependent networks.

---

2. **Compromise** of the device which threatens the integrity and confidentiality of the device and any supported networks.

DoS Attacks



Most DoS attacks fall into two broad categories:

1. **Volume-based** attacks which succeed due to the size of the attack.

2. **Low-Volume** attacks which cause the target device to lock up or experience degradation via one or a small number of packets.

DoS Attacks

Recent Vulnerabilities which allow low-volume DoS attacks:

- **CVE-2018-5390 (SegmentSmack for Linux)**
- **CVE-2018-6922 (SegmentSmack for FreeBSD)**
- **CVE-2018-5391 (FragmentSmack)**

Device Compromise

Attacker can:

- Monitor, modify, deny traffic
- Bypass approved infrastructure
- Maintain persistent access and expand

Networking Device Attack Surfaces

Stolen credentials

Software vulnerabilities

Lack of hardening

Notable Threats and Attacks

- IOS ROMMON replacement
- “SYNful Knock”
- “EXTRABACON” exploit (CVE-2016-6366)
- Cisco Smart Install abuse

TLP:WHITE

DHS | DEPARTMENT OF HOMELAND SECURITY

CYBERSECURITY

MITIGATION RECOMMENDATIONS

Justin
Network Analyst
NCCIC

NCCIC

Trends we are seeing in the field

End of Life (EOL) network devices

Default/weak security configurations

Unsecure remote-administrative practices

Poor security monitoring

The old “Network Operations” mentality

End of Life (EOL) network devices

Network devices (routers, switches, firewalls, etc) that are EOL and no longer supported by vendor.

- Network devices no longer getting vendor security patches.
- EOL devices don’t support modern security features or services.

Accurately account for every network device on the enterprise network.

- Goal is %100 visibility of every network device in the enterprise.
- Don’t forget remote offices and external boundary circuit/ISP connections.

Network devices not getting replaced during update/tech refresh cycles.

Ensure network device age and EOL vendor dates are accounted for in IT lifecycle management.

Default/weak security configurations

Devices put onto networks with “out of the box” configurations.

- Unused/unneeded services not removed/turned off.
- Default or weak administrator accounts/credentials.
- Default or weak SNMP settings.

Device hardened guidance provided by vendors/ government/DOD not implemented.

Deploying network devices into the enterprise environment should be a planned and thought out process.

- Resist “out of the box” implementations.
- Justify every service/feature that is needed to run on network devices.
- Develop hardened/secure configuration baselines.
  - Continually audit enterprise network environment for deviations from secure baseline.

Excellent security/ hardening guidance provided by some network vendors, government, and DoD (DISA STIGS).

- Current threat environment requires draconian security configurations.

Unsecure Remote-Administration Practices

Network devices still being managed by unsecure/ unencrypted remote administrative protocols.

- Telnet and HTTP still being used.
- SNMP v1/2c still in use to manage network devices.
- FTP/TFTP used externally.
- Administrator access directly over the internet.

Lack of multi factor authentication for administrator accounts

- Local administrator group accounts.

Poor security practices in the storage and transfer of network device configurations.

Network device administration should only be conducted over secure means.

- SSHv2, HTTPS
- SNMPv3 (authPriv mode, MIB whitelisting)
- Secure Copy (SCP), HTTPS
- Administrator access over encrypted out of band management channels.

Implement multi factor (i.e. hardware token & username/ pass) for all network device administration.

- Emergency local administrator account with unique passwords for each device.

Device configurations should be transferred to/from network devices over encrypted channels.

- Never email unencrypted network device configurations.
- Configurations should be stored encrypted.

Poor Security Monitoring

Network device logging not implemented or insufficient.

Lack of visibility of configuration changes to network devices.

Network devices should be configured to send logs off device to a central location.

All configuration changes should be logged and monitored (TACACS+ AAA).

Lack of visibility for administrator access to network devices.

Lack of visibility on the transfer of configuration files both to and from network devices.

Administrator access should be logged and monitored (TACACS+, RADIUS, etc).

The transfer of configurations files to/from network devices should be logged and monitored.

- External NetFlow to boundary network devices

The old “Network Operations” mentality

Network device security monitoring still being controlled by network operations section.

- Network device security monitoring secondary task to “operations”.

Network device anomalies investigated from a “troubleshooting” mindset only. No thought of adversarial threats to network devices.

- Unscheduled/unexplained network device reboot

Network device security monitoring should move to the Security Operations Center (SOC).

Train SOC analyst in network device security/monitoring.

Unscheduled/unexplained reboot

- Log review and software integrity checks performed.

TLP:WHITE

FEDERAL RESPONSE

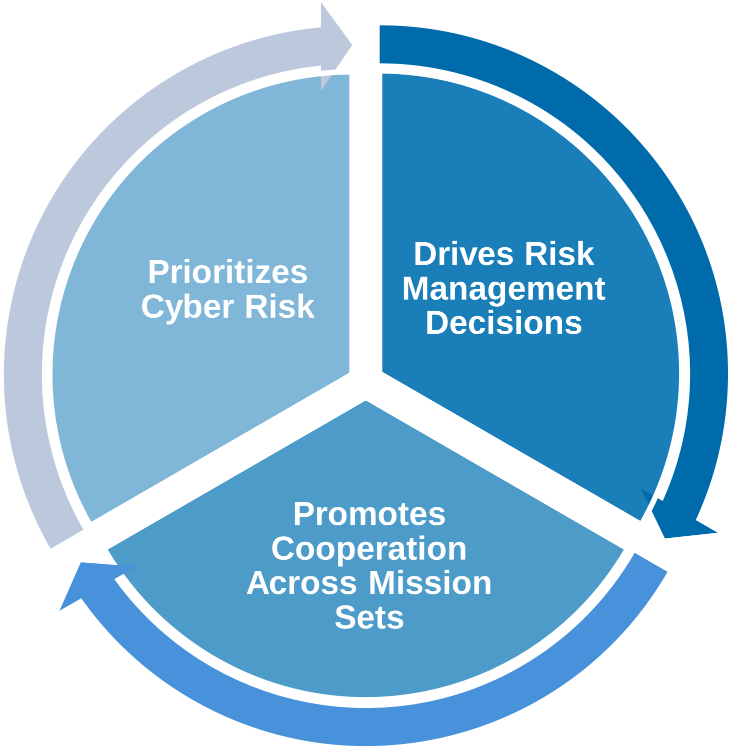
Brad
Network Analyst
DHS Cyber

DHS Binding Operational Directives (BODs)

Background:

- A binding operational directive (BOD) is a compulsory direction to Federal Civilian Executive Branch agencies (non-DOD and IC) for the purposes of safeguarding federal information and information systems from known or reasonably suspected information security threats, vulnerabilities, or risks.

Benefits:



Prioritizes Cyber Risk

Drives Risk Management Decisions

Promotes Cooperation Across Mission Sets

BOD 16-02:

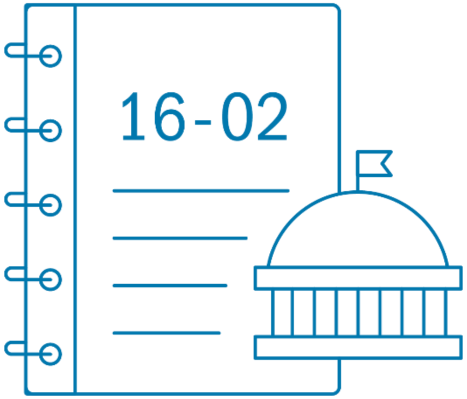
Threat to Network Infrastructure Devices

BOD Issuance:

- DHS, in coordination with interagency partners, issued BOD 16-02 on Sept. 27, 2016 in response to identified threats to network infrastructure devices on Federal .gov networks.
    - In-scope network infrastructure devices included routers and firewalls.
- BOD 16-02 provided mitigation steps to preemptively address risk and exposure across the .gov before vulnerabilities were exploited by adversaries.

BOD 16-02:

Impact to Federal Agencies



- Targeted effort helped agencies prioritize activities and ensured the same level of protections were being applied to internal routers and firewalls as endpoints, such as desktop computers and laptops.

- Demonstrated current state of interagency collaboration in rapidly securing thousands of in-scope devices against exploitation.

- Cross-agency effort highlighted the Federal government’s improvement in hardware and software asset management in order to effectively identify all vulnerable network infrastructure devices.

- Identified and led to replacement of End of Life (EOL) systems.

- Promoted agencies’ patch and configuration management policies, programs.

TLP:WHITE

NCCIC | NATIONAL CYBERSECURITY & COMMUNICATIONS INTEGRATION CENTER

NCCIC SERVICES

NCCIC

Information Sharing and Analysis

Automated Indicator Sharing (AIS)

Machine-to-machine: Indicators & Defensive Measures

Cybersecurity Information Sharing & Collaboration Program (CISCP)

Voluntary: CI/Federal Government

National Cyber Awareness System (NCAS)

Subscriptions for Products

National Vulnerability Database (NVD)

Repository: Managed Automation

Traffic Light Protocol (TLP)

Sensitive Information to trusted Stakeholders

Enhanced Cybersecurity Services (ECS)

Voluntary for System Protection

NCCIC Portal

Secure Communications Platform

NCCIC

24/7/365
OPERATIONS

Contact NCCIC

Email: nccicustomerservice@hq.dhs.gov

Phone: 1-888-282-0870

TLP:WHITE

Audience Q&A

Ask a question via the chat box.

Please complete the short survey following the webinar.
We appreciate your feedback.

U.S. DEPARTMENT OF HOMELAND SECURITY NCCIC

TLP:WHITE

Thank you for joining us today!

U.S. DEPARTMENT OF HOMELAND SECURITY

NCCIC