Transportation Security Administration

Cybersecurity

TSA-HQTRS, Virginia
Air Cargo Division

TSA-ATL, Georgia
Compliance Office

October 18, 2022

Agenda

- Cybersecurity Definition, Cybersecurity Incident Definition and Cybersecurity Essentials
- CISA- “Shields up”
- IACSSP change 7 and CCSSSP change 11 (Cyber)
- Information Circulars (ICs)
- Questions

Cybersecurity Definition

Cybersecurity is the art of protecting networks, devices, and data connected to the internet from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

Cybersecurity Incident Definition

- Cybersecurity Incident – An event that, without lawful authority, jeopardizes, disrupts or otherwise impacts, or is reasonably likely to jeopardize, disrupt or otherwise impact, the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident on the system. This definition includes an event that is under investigation or evaluation by the "operator" as a possible cybersecurity incident without final determination of the event's root cause or nature (such as malicious, suspicious, benign).

Cybersecurity Essentials

Phishing vs. Ransomware:

- **Phishing** is the fraudulent attempt to scam users into surrendering personal information such as credit card numbers, passwords, and account data to commit identity theft or to provide a gateway for the attacker to launch malware onto a computer or network.

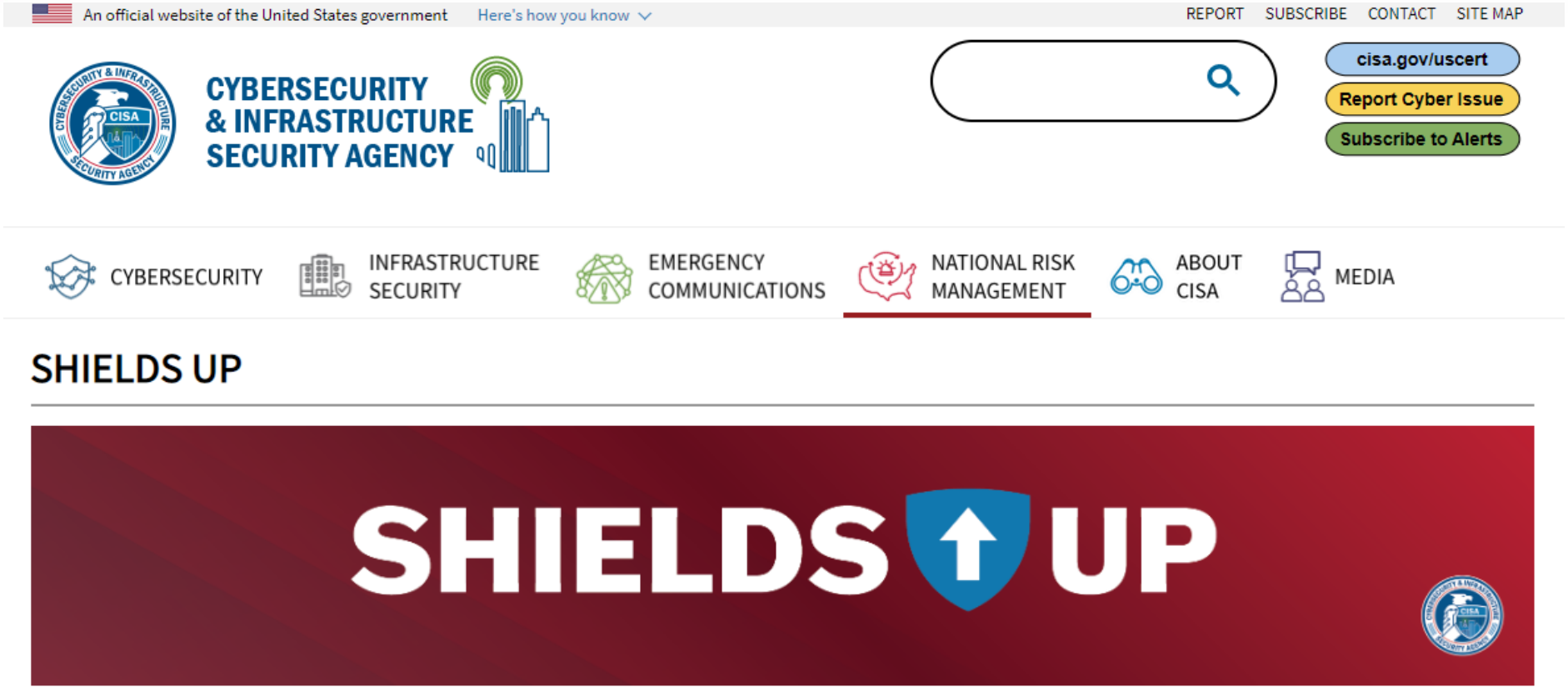
- **Ransomware** is malicious software that encrypts the victim's system or data, making it inaccessible unless a ransom payment is made. The most common methods for the spread of ransomware are through malicious email attachments, downloading files from the Internet, or by visiting an infected website that automatically downloads malicious code without the user's knowledge.

Cybersecurity Essentials

How to protect yourself:

- Never supply personal or confidential information via email.
- Never click on a link in an email that looks suspicious.
- Never download attachments from unidentified sources.
- Save and scan any attachments before opening them.
- Free stuff like games, ring tones, or screen savers can hide viruses or spyware. Do not download them unless you have verified and trust the source. Scan the file with security software.

CISA “Shields Up”



https://www.cisa.gov/shields-up

CISA

- The Shields-Up Advisory provides steps the organizations can take immediately to ensure that:

  - The likelihood of a damaging cyber intrusion is reduced.
  - A potential intrusion is quickly detected.
  - An organization is prepared to respond if an intrusion does occur, and;
  - An organization has maximized their resilience in the face of a destructive cyber incident.

- Security Coordinators are strongly encouraged to review the information on the Shields-Up website as the recent Joint Cybersecurity Advisories published on this topic. These alerts can be accessed at; https://www.cisa.gov/uscert/ncas/alerts

- Security Coordinators can also access the following link to add their company contact information for CISA updates and to subscribe directly for cybersecurity alerts and notifications. https://public.govdelivery.com/accounts/USDHSCISA/subscriber/new?qsp=CODE_RE

IACSSP change 7 and CCSSSP change 11

Indirect Air Carrier Standard Security Program

May 27, 2022

Certified Cargo Screening Standard Security Program

May 27, 2022

IACSSP and CCSSSP Cyber reporting

The IAC/CCSF must report the information as required as soon as practicable, but no later than 24 hours after a cybersecurity incident is identified. Reports must be made to CISA Central using CISA's

Reporting System form at:
https://us-cert.cisa.gov/forms/report or by calling (888) 282-0870.

If the required information is not available at the time of reporting, the IAC/CCSF must submit an initial report within the specified timeframe and supplement as additional information becomes available. All reported information will be protected in a manner appropriate for the sensitivity and criticality of the information and is Sensitive Security Information subject to the protections of part 49 CFR part 1520.

Informational Circulars (ICs)

U.S. Department of Homeland Security
Transportation Security Administration
6595 Springfield Center Drive
Springfield, Virginia 20598

INFORMATION CIRCULAR

NUMBER	IC 22-02
SUBJECT	Enhancing Cybersecurity in Cargo
EFFECTIVE DATE	February 25, 2022
EXPIRATION DATE	Indefinite
APPLICABILITY	Indirect Air Carriers regulated under 49 CFR Section 1548.5(a); and Certified Cargo Screening Facilities regulated under 49 CFR Section 1549.5(a)
LOCATIONS	United States
SUPERCEDES	N/A

U.S. Department of Homeland Security
Transportation Security Administration
6595 Springfield Center Drive
Springfield, Virginia 20598

INFORMATION CIRCULAR

NUMBER	IC 22-03
SUBJECT	Enhancing Cybersecurity in Air Cargo
EFFECTIVE DATE	March 23, 2022
EXPIRATION DATE	Indefinite
APPLICABILITY	Indirect Air Carriers regulated under 49 CFR Part 1548; and Certified Cargo Screening Facilities regulated under 49 CFR Part 1549
LOCATION	United States
SUPERSEDES	N/A

U.S. Department of Homeland Security
Transportation Security Administration
6595 Springfield Center Drive
Springfield, Virginia 20598

INFORMATION CIRCULAR

NUMBER	IC 22-05
SUBJECT	Cybersecurity Self-Assessments and Incident Response Plans
EFFECTIVE DATE	July 31, 2022
APPLICABILITY	Category III and IV Airport Operators regulated under 49 CFR part 1542.103; Aircraft Operators regulated under 49 CFR part 1544.101(d) and (f); Indirect Air Carriers regulated under 49 CFR part 1548; and Certified Cargo Screening Facilities (CCSFs) regulated under 49 CFR part 1549
LOCATION	All locations within the United States

Questions

"*Threat actors continue to target and exploit our nation's critical infrastructure to cripple our nation's economy. Knowing what's on your network is the first step for any organization to reduce this risk. CISA and TSA urges all organizations to gain a complete understanding of vulnerabilities that may exist on their networks. We all have a vital role to play in building a more cyber resilient environment and early vulnerability detection. Thank you.*"

Ron Varghese
Air Cargo Division
Transportation Security Administration
U.S. Dept. of Homeland Security
Washington D.C.
Ronoy.Varghese@tsa.dhs.gov