David Stern

Lead - SLTT Partnerships
CISA

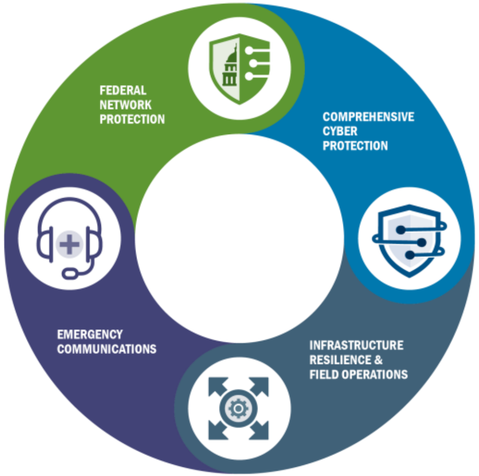
December 16, 2020

Cybersecurity and Infrastructure Security Agency (CISA)

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

We are the Nation's Risk Advisors

The Cybersecurity and Infrastructure Security Agency (CISA) is the pinnacle of national risk management for cyber and physical infrastructure


FEDERAL NETWORK PROTECTION
COMPREHENSIVE CYBER PROTECTION
INFRASTRUCTURE RESILIENCE & FIELD OPERATIONS
EMERGENCY COMMUNICATIONS

VISION

Secure and resilient critical infrastructure for the American people.

MISSION

Lead the national effort to understand and manage cyber and physical risk to our critical infrastructure.

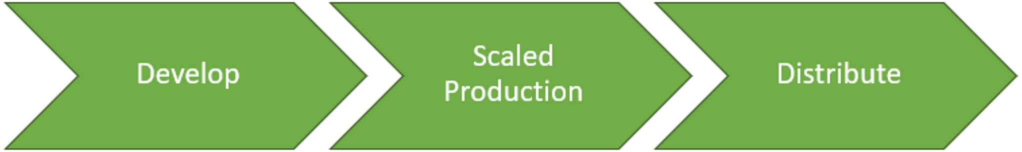
Threat Landscape

WHO: Threat Actors		
Nation States	Criminals	Other

WHY: Motivations			
Industrial	Military	Financial	Ideological / Political / Prestige

WHAT: Target Assets					
Intellectual Property	Trustworthy Data	Public Confidence	Reliable Manuf & Delivery	Cyber Physical Systems	Human Life

HOW: Methods | Capabilities					
Shodan/MetaSploit	Phishing	Ransomware	Information Operations	Destructive Malware	Physical Attacks



Develop

Scaled Production

Distribute

Adversary Goals

Adversaries could try to

- **Delay or inhibit** our ability to produce & deliver viable countermeasures
- **Disrupt critical systems** for illicit financial gain
- **Undermine confidence** in US COVID response efforts and trust in the final vaccines or countermeasures

To achieve these goals, they may

- **Tamper** with, **destroy**, or **deny access** to data & systems (e.g. SLTT health department IT systems, cold chain/storage, clinical data, SCADA systems)
- **Discredit** the veracity of scientific research and related organizations, persons
- **Steal Intellectual Property**
  - Research, clinical trials, manufacturing & scale-up

How does this affect SLTT orgs?

State and local Departments of Health and other health-related SLTT organizations will play a key role in cold chain, cold storage, distribution, and administration of the vaccine and may become targets.

AA20-302A: Ransomware Activity Targeting the Healthcare and Public Health Sector (Oct 28, 2020)

CISA, FBI, and HHS - Credible info of an increased imminent cybercrime threat to U.S. hospitals and healthcare providers:

- CISA, FBI, and HHS assess malicious cyber actors are targeting the HPH Sector with TrickBot and BazarLoader malware, often leading to ransomware attacks, data theft, and the disruption of healthcare services
- Review or establish patching plans, security policies, and business continuity plans to ensure they address current threats posed by malicious cyber actors
- Implement ransomware prevention and response measures immediately: https://www.cisa.gov/publication/ransomware-guide

AA20-302A can be found at: https://us-cert.cisa.gov/ncas/alerts/aa20-302a

Recommended Actions

- Identify systems that are critical to COVID-19 response and may be of interest to adversaries
- Identify who is responsible for maintaining security of the systems identified to be critical
- Discuss with cybersecurity professionals whether adequate protections are in-place based on risk

Multi-State Information Sharing and Analysis Center (MS-ISAC)

MS-ISAC: Funded by CISA, the MS-ISAC serves as a central resource for situational awareness, information sharing, and incident response for SLTT governments. The ISAC also shares risk information to support national cybersecurity situational awareness with CISA. Membership is **free** and includes SLTT governments, public utilities, universities, K-12 schools, hospitals, ports, airports, etc.

Join at: https://learn.cisecurity.org/ms-isac-registration

Nationwide Cybersecurity Review (NCSR): OPEN NOW

- Conducted by MS-ISAC on CISA's behalf, based on NIST Cybersecurity Framework.
- Anonymous, annual self-assessment to measure gaps/capabilities of SLTT govt cybersecurity programs.
- Evaluates cybersecurity maturity across the nation while providing actionable feedback and metrics directly to individual respondents.
- Requirement for Homeland Security Grant Program (SHSP/UASI) recipients.

CISA Services (1/2)

Vulnerability Scanning - CISA scans for internet-facing vulnerabilities and notifies partners via weekly report. CISA also conducts proactive notifications when a new critical vulnerability is disclosed or CISA observes targeting of a particular vulnerability.

CISA/MS-ISAC Ransomware Guide - https://www.cisa.gov/publication/ransomware-guide

CISA Services (2/2)

Malicious Domain Blocking and Reporting (MDBR) - A no-cost Protective DNS service funded by CISA and offered through the MS-ISAC. This service can block resolution of malicious links in phishing emails and connections to domains used for malware and ransomware command and control:

https://www.cisecurity.org/ms-isac/services/mdbr/

Contact CISA

- Questions about CISA resources: CyberLiaison_SLTT@cisa.dhs.gov

- To Report an Incident:
  - https://us-cert.cisa.gov/report;
  - Central@cisa.gov; or
  - (888) 282-0870
  - CISA Cybersecurity Advisor: https://www.cisa.gov/cisa-regions