ELECTION SECURITY OVERVIEW
2021 NASS SUMMER CONFERENCE
Opening Remarks

CISA Leadership

Jen Easterly, Director
Threat Landscape

2016
- Russian APT cyber and influence activity

2020/2021
- E-Day: “Just another Tuesday on the Internet”
- Russian APT cyber and influence activity
- Iranian APT cyber and influence activity
- Enemies of the People
- Mis- and Disinformation
- SolarWinds
- Microsoft Exchange Server
- Colonial pipeline ransomware
- Kaseya ransomware
Cybersecurity Services

CISA Services
- Vulnerability Scanning (Cyber Hygiene)
- Remote Penetration Testing
- Phishing Campaign Assessment
- Critical Product Evaluation
- Crossfeed
- Cyber Resilience Review
- & more

CISA Election Security Trainings
- Election Security Overview
- Ransomware
- Phishing
- Building Trust through Secure Practices
Cybersecurity State Coordinators (CSC)

CSC Key Roles Outlined in the FY21 NDAA
- Serve as Federal cybersecurity risk advisor in the state
- Facilitate cyber threat info-sharing
- Raise awareness of Federal cybersecurity resources
- Support trainings and exercises
- Assist in developing vulnerability disclosure programs

Cybersecurity Advisors (CSAs) Roles Remain Unchanged
- Provide assistance to SLTT governments and CI owners/operators
- Introduce organizations to CISA products and services
- Provide preparedness, assessments, resources, messaging, incident coordination, etc.
Under CISA, .gov domains are available at **no cost** for qualifying organizations.

Increased use of .gov domains will **improve cybersecurity and trust** in public services across the United States.

It should be easy for the public to know they are engaged with a government agency.

Released new “**About. gov, for elections**” page on the DotGov website: [https://home.dotgov.gov/about/elections/](https://home.dotgov.gov/about/elections/).
Physical Security

CISA resources available to election officials

Protective Security Advisors
Physical Security Assessments
Physical Security at Voting Locations and Election Facilities Guide

Hometown Security page and resources: https://www.cisa.gov/hometown-security

Mitigating the Impacts of Doxing on Critical Infrastructure Guidance
Physical Security

Coordinated Federal Support

Report immediate threats to local law enforcement (9-1-1)

Report threats and violent acts to the FBI at 1-CALL-FBI (225-5324), prompt 1, then prompt 3

DOJ, DHS, FBI, and others are working together in recognition of increasing threats against election workers/administrators/officials
Chain of Custody Guidance

Released by CISA in August 2021

Chain of custody is a security consideration across critical infrastructure

Tracking control of data and assets to ensure transparency, accountability, and trust

Highlights **impacts and risks** from a broken chain of custody
- The integrity of the system and its data will be deemed untrustworthy
- A court of law can render the system and data inadmissible
- Inability to definitively determine if an actor has manipulated your systems or data
Chain of Custody Guidance

A Complex Topic Vastly Oversimplified

1. Identify
   - What do you care about?
   - Who is authorized to access and control it?

2. Protect
   - What can they do to the things you care about?
   - How do you keep non-authorized people from accessing it?

3. Detect
   - Is there enough evidence to know something happened?
   - Can you tell if something occurred and what it was?

4. Respond
   - How will you determine the impact?
   - How will you prevent further consequences?
   - Do you know what to do next?

5. Recover
   - What will it take to trust the asset again?