CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

# CISA UPDATES

## NASS SUMMER CONFERENCE 2022

**CISA**
July 18, 2022

# Overview

## Core CISA Support to SLTT & Election Subsector

## Highlighted Resources

- Crossfeed
- Insider Threat Mitigation
- Tabletop the Vote 2022, Exercises & Training
- CISA Products, Spanish-language Translations

## Coordinated Vulnerability Disclosure Program

# Core SLTT Resources

## Alerts & Information Sharing
- MS-ISAC & EI-ISAC
  - Albert Sensors, MDBR, EDR
- Threat Briefings, Security Clearance Program
- E-Day Ops Center & EI-ISAC Virtual Sit. Room

## Cybersecurity Services & Incident Response
- Vulnerability Scanning, Remote Penetration Testing, Critical Product Evaluation, etc.
- .gov

## Cybersecurity & Protective Security Advisors

## Exercises & Trainings

Making .gov More Secure by Default

.gov

When the public sees information on a .gov website, they need to trust that it is official and accurate. This trust is warranted, because registration of a .gov domain is limited to bona fide US-based government organizations. Governments should be easy to identify on the internet and users should be secure on .gov websites.

HTTPS is a key protection for websites and web users. It offers security and privacy when connecting to the web, and provides governments the assurance that what they publish is what is delivered to users. In the last few years,

CISA CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

Leveraging the .gov Top-level Domain

The .gov domain is a top-level domain (TLD) that was established to make it easy to identify US-based government organizations on the internet. All three branches of the US Government, all 50 states, and many local governments use .gov for their domains.

The DotGov Program, based at the US General Services Administration (GSA), manages the .gov TLD.

Why should State and Local Election Officials be interested in .gov?

Since a .gov domain is only available to bona fide US-based government organizations, using it signals trust and credibility. This can help a state or local election office establish its digital services (e.g., websites, emails) as official, trusted sources for voter information.

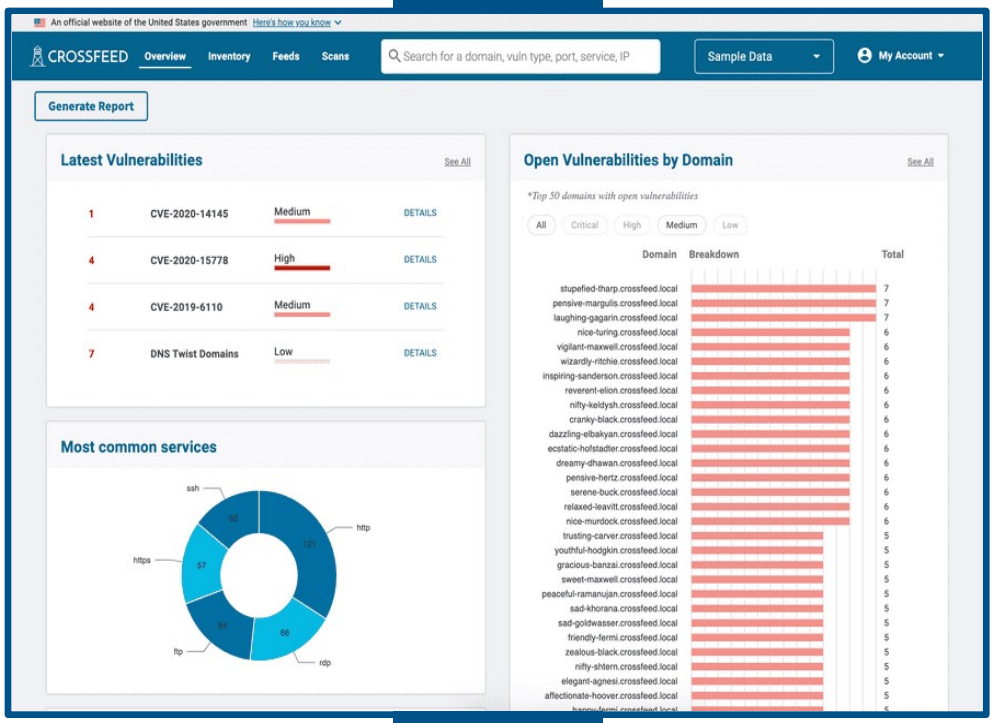
# Crossfeed

## Overview

- Collects open-source data to provide a snapshot of a state's potential risks and online assets

## Benefits

- Free vulnerability scanning
- Data aggregated on a dashboard
- Attacker's perspective of assets
- Clear understanding of threat vectors




Crossfeed enrollment is open to state election offices only. The open-source tool is available at: github.com/cisagov/crossfeed

# Insider Threat Mitigation

**Insider Threat:** the potential for an insider to use their authorized access or special understanding of an organization to harm that organization.

**Resources for All CI Sectors:**

- Insider Threat Mitigation Guide
- Self-Assessment Tool
- Videos

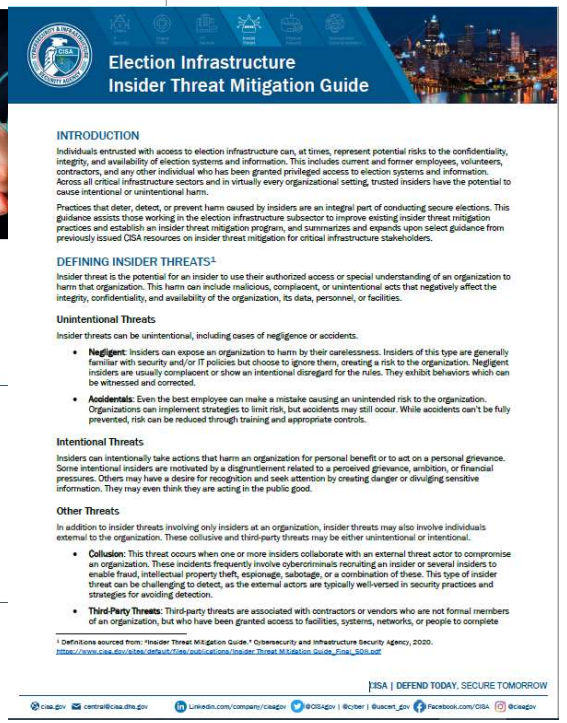
**Resources for Election Infrastructure Stakeholders:**

- Election Infrastructure Insider Threat Mitigation Guide
- Training

**Insider Threat Mitigation Guide**

NOVEMBER 2020

Cybersecurity and Infrastructure Security Agency



**Election Infrastructure Insider Threat Mitigation Guide**

**INTRODUCTION**

Individuals entrusted with access to election infrastructure can, at times, represent potential risks to the confidentiality, integrity, and availability of election systems and information. This includes current and former employees, volunteers, contractors, and any other individual who has been granted privileged access to election systems and information. Across all critical infrastructure sectors and in virtually every organizational setting, trusted insiders have the potential to cause intentional or unintentional harm.

Practices that deter, detect, or prevent harm caused by insiders are an integral part of conducting secure elections. This guidance assists those working in the election infrastructure subsector to improve existing insider threat mitigation practices and establish an insider threat mitigation program, and summarizes and expands upon select guidance from previously issued CISA resources on insider threat mitigation for critical infrastructure stakeholders.

**DEFINING INSIDER THREATS[1]**

Insider threat is the potential for an insider to use their authorized access or special understanding of an organization to harm that organization. This harm can include malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, or facilities.

**Unintentional Threats**

Insider threats can be unintentional, including cases of negligence or accidents.

- **Negligent:** Insiders can expose an organization to harm by their carelessness. Insiders of this type are generally familiar with security and/or IT policies but choose to ignore them, creating a risk to the organization. Negligent insiders are usually complacent or show an intentional disregard for the rules. They exhibit behaviors which can be witnessed and corrected.
- **Accidentals:** Even the best employee can make a mistake causing an unintended risk to the organization. Organizations can implement strategies to limit risk, but accidents may still occur. While accidents can't be fully prevented, risk can be reduced through training and appropriate controls.

**Intentional Threats**

Insiders can intentionally take actions that harm an organization for personal benefit or to act on a personal grievance. Some intentional insiders are motivated by a disgruntlement related to a perceived grievance, ambition, or financial pressures. Others may have a desire for recognition and seek attention by creating danger or divulging sensitive information. They may even think they are acting in the public good.

**Other Threats**

In addition to insider threats involving only insiders at an organization, insider threats may also involve individuals external to the organization. These collusive and third-party threats may be either unintentional or intentional.

- **Collusion:** This threat occurs when one or more insiders collaborate with an external threat actor to compromise an organization. These incidents frequently involve cybercriminals recruiting an insider or several insiders to enable fraud, intellectual property theft, espionage, sabotage, or a combination of these. This type of insider threat can be challenging to detect, as the external actors are typically well-versed in security practices and strategies for avoiding detection.
- **Third-Party Threats:** Third-party threats are associated with contractors or vendors who are not formal members of an organization, but who have been granted access to facilities, systems, networks, or people to complete

[1] Definitions sourced from: "Insider Threat Mitigation Guide." Cybersecurity and Infrastructure Security Agency, 2020. https://www.cisa.gov/sites/default/files/publications/Insider Threat Mitigation Guide_Final_508.pdf

CISA | DEFEND TODAY, SECURE TOMORROW

# Exercises & Trainings

**Exercises**

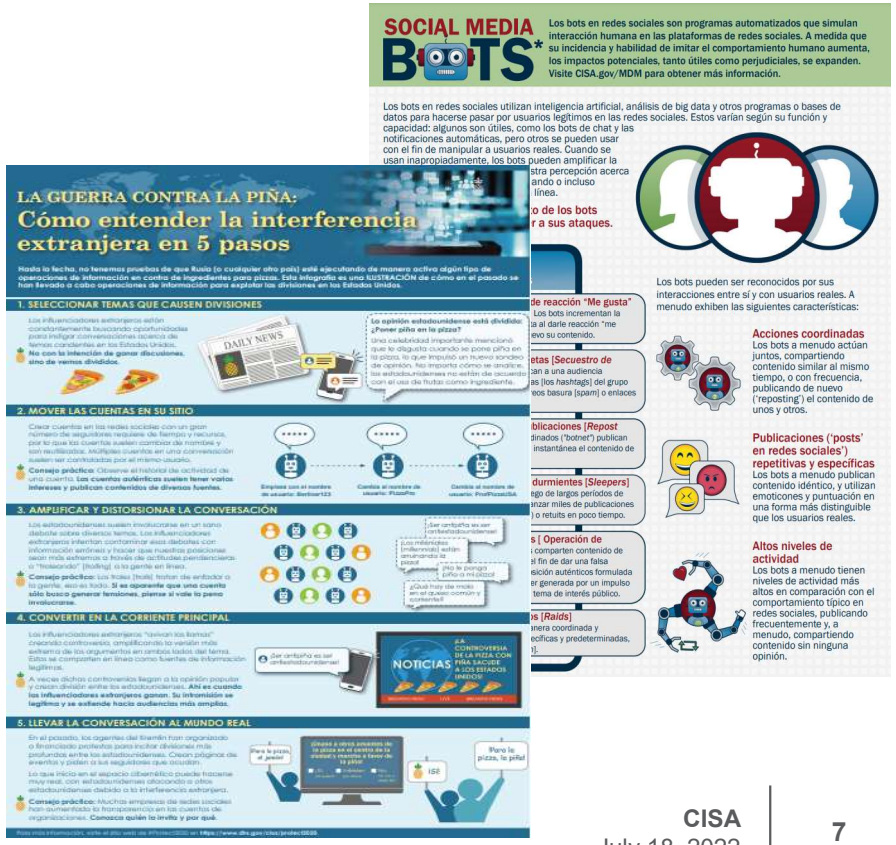
- Tabletop the Vote 2022
- “Tabletop in a box”– new election packages
- State-based exercises

**Training**

- Election Security Overview
- Insider Threat Mitigation
- Building Trust Through Secure Practices
- Phishing
- Ransomware

# Spanish-Language Translations

- Social Media Bots Infographic Set
- Disinformation Stops with You Infographic
- Information Manipulation Infographic
- Election Infrastructure Cyber Risk Assessment & Infographic
- and more at cisa.gov/election-security-library



# CISA Coordinated Vulnerability Disclosure

## CVD Process

- Coordinate the remediation and public disclosure of newly identified cybersecurity vulnerabilities in products and services with affected vendor(s)

## 5-Step Process

- Collection
- Analysis
- Mitigation Control
- Application of Mitigation
- Disclosure

## Goal

To ensure that CISA, the affected vendor(s) and/or service provider(s), and the vulnerability reporter all disclose simultaneously, to ensure that users and administrators receive clear and actionable information in a timely manner.

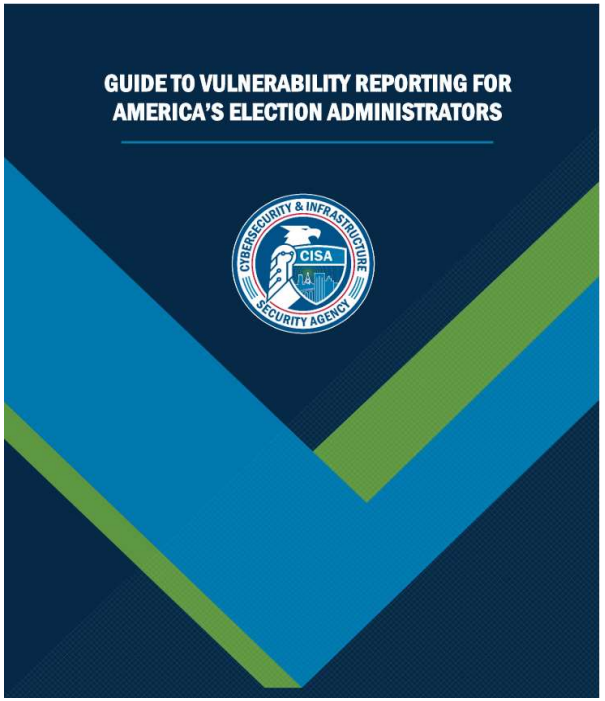
# CISA Coordinated Vulnerability Disclosure

## Disclosure Timeline

- Timeframes for mitigation development, as well as the type and schedule of disclosure, may be affected by various factors:
  - Active exploitation
  - Threats of an especially serious nature
  - Situations that require changes to established standards may result in changes to the disclosure timeline

## Related Resource

- Guide to Vulnerability Reporting for Election Administrators
  - Considerations for adopting a Vulnerability Disclosure Policy (VDP)




**Kim Wyman**
Senior Election Security Advisor
Cybersecurity and Infrastructure Security Agency
Kim.Wyman@cisa.dhs.gov

**Contact CISA:**
electionsecurity@cisa.dhs.gov