

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



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.

CISA
July 18, 2022

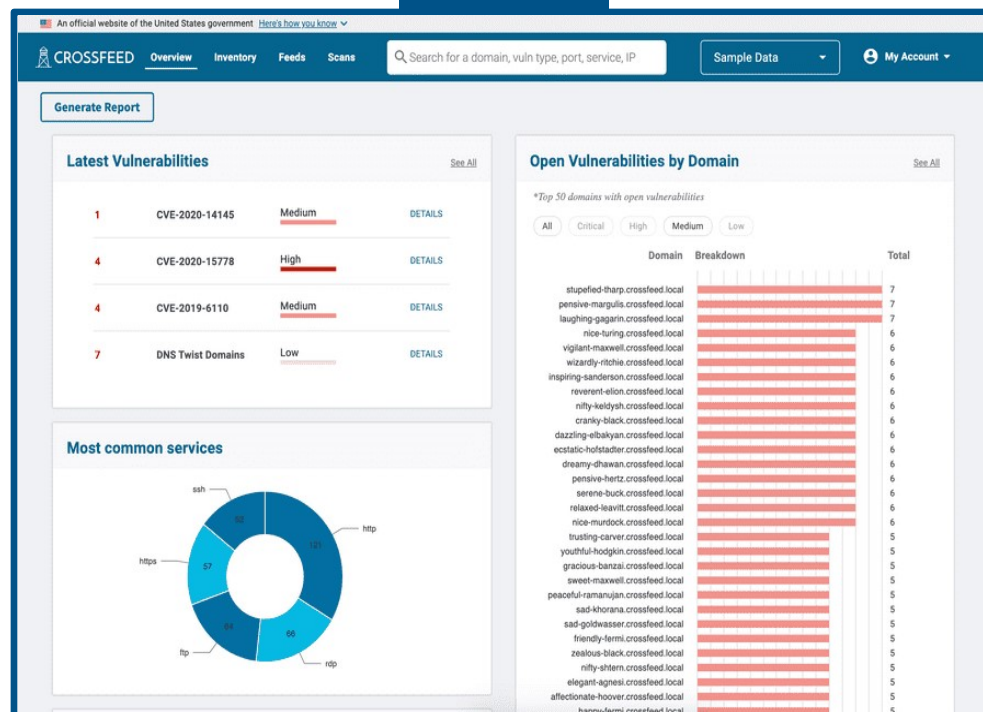
Crossfeed

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 sector 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 THREATS¹

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, compliant, 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 disappointment 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_2020.pdf

CISA | DEFEND TODAY. SECURE TOMORROW

CISA.gov | central@cisa.dhs.gov | LinkedIn.com/company/cisagov | @CISAgov | @ciscer | @ciscertgov | Facebook.com/CISA | @cisagov

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](https://www.cisa.gov/election-security-library)



SOCIAL MEDIA BOTS

Los bots en redes sociales son programas automatizados que simulan interacción humana en las plataformas de redes sociales. A medida que su incidencia y habilidad de imitar el comportamiento humano aumenta, los impactos potenciales, tanto útiles como perjudiciales, se expanden. Visite [CISA.gov/MDM](https://www.cisa.gov/MDM) para obtener más información.

Los bots en redes sociales utilizan inteligencia artificial, análisis de big data y otros programas o bases de datos para hacerse pasar por usuarios legítimos en las redes sociales. Estos varían según su función y capacidad; algunos son útiles, como los bots de chat y las notificaciones automáticas, pero otros se pueden usar con el fin de manipular a usuarios reales. Cuando se usan inapropiadamente, los bots pueden amplificar la mala percepción acerca de un tema, alando o incluso atacando a una línea.



o de los bots para ataques.

Los bots pueden ser reconocidos por sus interacciones entre sí y con usuarios reales. A menudo exhiben las siguientes características:

Reacción "Me gusta"
Los bots incrementan la cantidad de reacciones que les da al darles reacción "me gusta" a su contenido.

Acciones coordinadas
Los bots a menudo actúan juntos, compartiendo contenido similar al mismo tiempo, o con frecuencia, publicando de nuevo ("reposting") el contenido de unos y otros.

Publicaciones ("posts" repetitivas y específicas)
Los bots a menudo publican contenido idéntico, y utilizan emoticonos y puntuación en una forma más distinguible que los usuarios reales.

Publicaciones ("posts" repetitivas y específicas)
Los bots a menudo publican contenido idéntico, y utilizan emoticonos y puntuación en una forma más distinguible que los usuarios reales.

Altos niveles de actividad
Los bots a menudo tienen niveles de actividad más altos en comparación con el comportamiento típico en redes sociales, publicando frecuentemente y, a menudo, compartiendo contenido sin ninguna intención.

Operación de "dormientes" (Sleepers)
Los bots a menudo actúan juntos, compartiendo contenido similar al mismo tiempo, o con frecuencia, publicando de nuevo ("reposting") el contenido de unos y otros.

Publicaciones ("posts" repetitivas y específicas)
Los bots a menudo publican contenido idéntico, y utilizan emoticonos y puntuación en una forma más distinguible que los usuarios reales.

Altos niveles de actividad
Los bots a menudo tienen niveles de actividad más altos en comparación con el comportamiento típico en redes sociales, publicando frecuentemente y, a menudo, compartiendo contenido sin ninguna intención.

LA GUERRA CONTRA LA PIÑA: Cómo entender la interferencia extranjera en 5 pasos

Nota de la noche, no tenemos previsto de que Rusia lo cualquier otro país) esté ejecutando de manera activa algún tipo de operaciones de información en contra de ingredientes para pizza. Esta infografía es una RECREACIÓN de cómo en el pasado se han llevado a cabo operaciones de información para explotar los intereses en los Estados Unidos.

- 1. SELECCIONAR TEMAS QUE CAUSEN DIVISIONES**
Los influencers extranjeros están cada vez más frecuentemente explotando la capacidad de llegar a audiencias grandes de temas controvertidos en las redes sociales. No con la intención de ganar afiliaciones, sino de generar división.
Consejo práctico: Los influencers extranjeros están cada vez más frecuentemente explotando la capacidad de llegar a audiencias grandes de temas controvertidos en las redes sociales. No con la intención de ganar afiliaciones, sino de generar división.
Consejo práctico: Los influencers extranjeros están cada vez más frecuentemente explotando la capacidad de llegar a audiencias grandes de temas controvertidos en las redes sociales. No con la intención de ganar afiliaciones, sino de generar división.
- 2. MOVER LAS CUENTAS EN SU SITIO**
Crear cuentas en las redes sociales con un gran número de seguidores requiere tiempo y recursos, por lo que las cuentas suelen ser operadas por bots. Muchos bots actúan en una conversación realista con usuarios reales.
Consejo práctico: Crea una historia de actividad de una cuenta. Los usuarios auténticos suelen tener varias interacciones y publicar contenido de diversas fuentes.
- 3. AMPLIFICAR Y DISTORSIONAR LA CONVERSACION**
Los influencers extranjeros suelen emplear un lenguaje altamente emocional en un intento de atraer a otros usuarios. Los influencers extranjeros a menudo intentan controlar una discusión con información errónea y hacer que nuevas posiciones sean más atractivas a través de técnicas de "redacción" ("hooking") o "gancho" en línea.
Consejo práctico: Los bots (bots) tratan de enfocarse en la parte más emocional de una discusión. Así es como los influencers extranjeros ganan. Su comportamiento legítimo y se enfoca hacia audiencias más amplias.
- 4. CONVERTIR EN LA CORRIENTE PRINCIPAL**
Los influencers extranjeros "mueven los botones" creando controversia, amplificando lo que es más atractivo de los argumentos en uno lado de la línea. Esto se convierte en una fuente de información legítima.
Consejo práctico: A veces dichos controversias llegan a la opinión popular y crean división entre los estadounidenses. Así es como los influencers extranjeros ganan. Su comportamiento legítimo y se enfoca hacia audiencias más amplias.
- 5. LLEVAR LA CONVERSACION AL MUNDO REAL**
En el pasado, los agentes del tiranismo han organizado o financiado protestas para hacer divisiones más profundas entre los estadounidenses. Crear profundos divisiones y poder en las relaciones que existen.
Consejo práctico: Muchos eventos de acción social han sido financiados y financiados en las cuentas de organizaciones. Conoce quién lo lleva y por qué.

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.



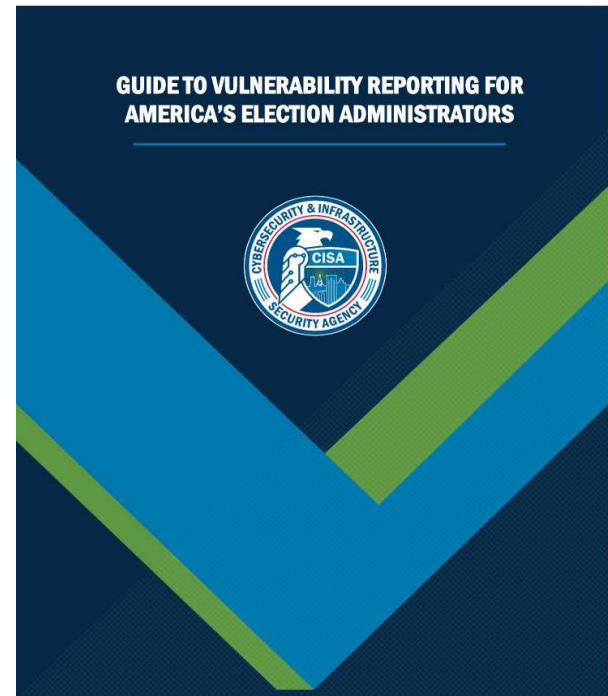
CISA Coordinated Vulnerability Disclosure

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