CLEARFORCE
Protecting Organizations from People Risk

2024 U.S. Federal Elections & How to Mitigate the Risk of Insider Threat

Guidance to State Election Officials from the FBI, CISA, DHS, and the US EAC

Introduction

The Federal Bureau of Investigation (FBI), in coordination with the Department of Homeland Security's (DHS) Office of Intelligence and Analysis (I&A), the Cybersecurity and Infrastructure Security Agency (CISA), and the U.S. Election Assistance Commission (EAC) prepared a guidance and recommendations document for State Election Officials to help them detect and defend against insider threat concerns that could materialize during the 2024 election cycle. It is important that election stakeholders at all levels are aware of the risks posed by insider threats and the steps they can take to identify and mitigate these threats. This CISA briefing document outlines recent examples of election security-related insider threats, discusses potential scenarios that could arise during the election cycle, and provides **recommendations for how to mitigate the risk posed by insider threats.**

Document Highlights

The CISA briefing is a strong blueprint for State Elections Officials, Secretaries of State, Election Boards, or private organizations responsible for managing federal elections. This includes any organization that is hiring or managing the workforce, overseeing voter registration, managing election logistics, and ensuring compliance with both state and federal election laws. Throughout the election cycle, many people are involved in administering or carrying out responsibilities that support elections, including election workers, officials from other divisions of government, vendors, contractors, temporary workers, and volunteers.

The CISA briefing highlights and explains the **human risk associated with federal elections** including:

- What Constitutes Insider Threat and How Insiders Present Risk
- Building an Insider Threat Program
- Foreign Adversary Exploitation and Examples
- Continuous Monitoring
- Incident Reporting & Investigation Forms
- Physical & System Controls
- Standard Procedures & Best Practices

Read the full CISA briefing guide here:
https://www.cisa.gov/sites/default/files/2024-06/2024%20General%20Elections_Insider%20Threat_6.11.24_footnote_508c.pdf

ClearForce Insider Threat Solutions for Election Security

ClearForce delivers Insider Threat solutions to government and commercial organizations, including out of the box software and data services, aligned to the specific federal guidance provided in the document that can be implemented rapidly in support of election security and risk protection.

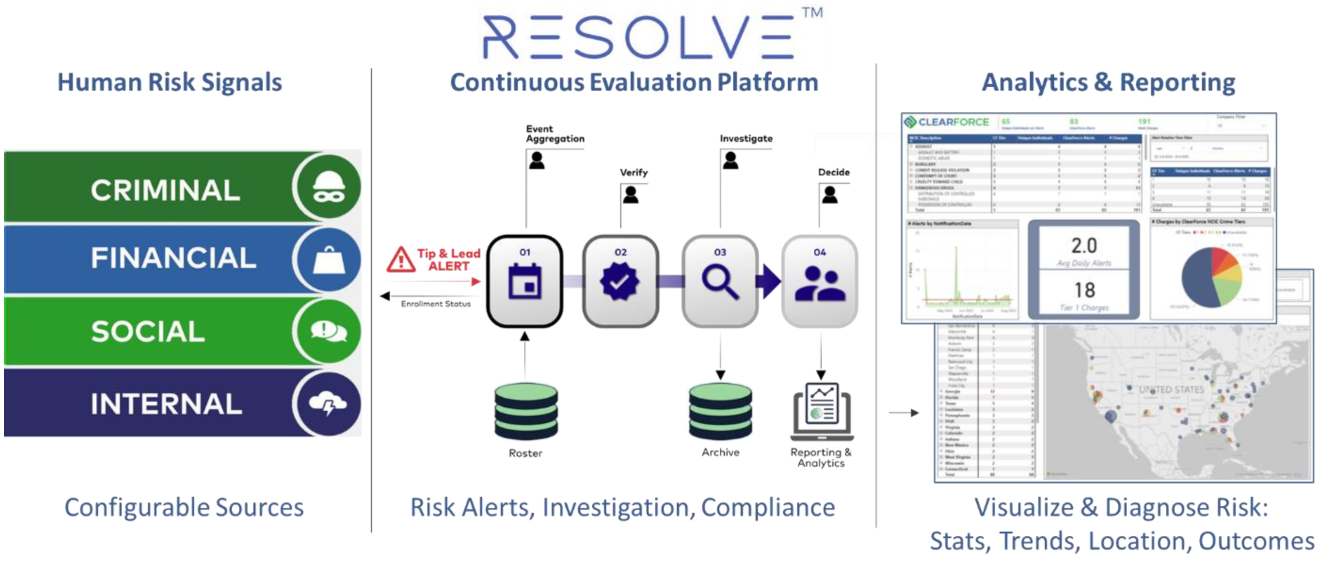
(1) **Continuous Monitoring**: The patented Resolve^{TM} Continuous Monitoring platform delivers automated continual real-time alerts of people-based events, anomalies, and risk patterns identified in criminal, court records, financial, social media, dark web, and internal incident data. This includes full legally compliant investigation and case management functionality for Insider Threat alert investigation and data collection with notes, attachments and audit trail.

(2) Web Based Internal Incident Reporting & Investigation Forms: The ClearForce Internal Incident Portal provides web-based insider threat reporting and investigation templates. The forms are easily configured to meet the federal examples provided. Everything is captured in a real-time web application and stored centrally. This reduces the complexity of managing disparate pdf documents.

(3) Deep Public Record Investigative Search: ClearForce delivers in-depth investigative reports to encompass critical details in support of research and investigations including identity resolution and association, criminal records, known addresses, vehicle information, phone numbers, emails, IP addresses, employment history, property ownership, known associates, and known business affiliations. The granularity of these profiles will uncover a wide variety of evidenced-based insider threat risk indicators.

(4) Workforce Risk Assessments: ClearForce utilizes its risk data analytics platform to perform one-time or periodic workforce risk assessments. The risk assessment looks back into a workforce or supply chain to identify risk in the organization across an established set of Insider Threat signals. The lookback period can be configured for months or years. The results and details are delivered in formalized reports and on-line dashboards.

(5) Insider Threat Program & Best Practices: ClearForce offers a specialized managed service of experts to help you stand up or expand your Insider Threat Program to address human and digital related threats within your workforce, supply chain, and volunteer networks.



www.clearforce.com