

## Department of Justice (DOJ) Request for Information (RFI): Insider Threat Program Technical Solutions

### INTRODUCTION:

The Department of Justice (DOJ) is seeking information from qualified vendors with a product (not services) for Insider Threat Programs. This Request for Information (RFI) is issued as an Industry Day to gather insights into technical capabilities, best practices, and innovative technical solutions for preventing, identifying, monitoring, and mitigating insider threats. This event is to focus on IT solutions and products, and not support services. The DOJ is not seeking proposals currently but rather is interested in learning about the range of available technologies for Insider Threat Programs.

### BACKGROUND:

The DOJ Insider Threat Program is dedicated to the proactive identification, deterrence, and mitigation of insider risks that could compromise sensitive information, disrupt DOJ operations, or endanger national security. The DOJ Insider Threat Program seeks comprehensive technology solution(s) that integrates advanced monitoring, behavior analytics, real-time reporting, and incident response/mitigating capabilities to ensure both security, safeguarding privacy, and compliance with federal standards.

### LOGISTICS DETAILS:

Vendor participation in this event is contingent on having a technical product(s) and staffing an information table on the product(s).

- **Location:** Washington, DC area
- **Time:** March 4, 2025, from 9:30 am to 4:30 pm. Setup begins at 7:30 am.
- **Personnel:** Recommend at least 2 people per vendor but no more than 3 people per vendor.
- **Equipment:** Each vendor will be provided a table and 2 chairs.
- **Presentations:** There will be an opportunity for each vendor to provide a capabilities overview (10 minutes to 30 minutes) in a separate conference room. Presentations **MUST** be electronically provided via an email to [itp@usdoj.gov](mailto:itp@usdoj.gov), in advance, as USB drives are not permitted. Timeslots will be determined based upon the number of vendors that timely register.
- **Technology:** Wi-Fi is not available, and removable media is not allowed onsite. There is no guarantee of connectivity if using a personal Wi-Fi enabled device.
- **Security:** Marketing materials are permitted but must go through walk-in security (no loading dock) during the setup time on the day of the event. Vendor representatives must submit the Police Check Inquiry Form and will also go through an x-ray security check point upon arrival.
- **Parking:** No onsite parking available. There are parking lots around the area ranging in price from \$12-\$25.
- **Photography:** No pictures allowed within the facility. This includes pictures taken by personal mobile devices.

## OBJECTIVES:

The primary objective of this RFI includes understanding vendor technical capabilities for insider threat deterrence, detection, and mitigation in the following categories:

- Artificial Intelligence
- Analytic Search Tool
- Case Management
- Data Integrator
- Data Loss Prevention
- Artificial Intelligence Detector
- Image Analysis Tool
- Training
- User Activity Monitoring
- User Behavior Analytics
- Publicly Available Electronic Information
- Block Chain Analysis
- Other/Innovation

## REQUESTED INFORMATION:

Interested vendors must provide the following via email to [itp@usdoj.gov](mailto:itp@usdoj.gov):

1. Vendor Information Template (only 1 per vendor, no matter the number of products): Overview of the vendor, years in business, cage code, and relevant experience with federal government agencies. Point of contact for follow-up. The product capabilities as mentioned in the above Objectives.
2. Technical Capabilities Matrix (1 per type of product):
  - a. Describe each type of product being presented in 200 words or fewer.
  - b. Outline the deployment process, including options for cloud, on-premises, and/or hybrid solutions. Describe the scalability of the solution and any limits on the number of users or data volume in 200 words or fewer.
  - c. Is the product FedRAMP certified or able to obtain the certification, and at what level (Impact Level 4 – Impact Level 6/ Low-High)?
  - d. If available, describe any unique capabilities or emerging technologies the solution includes such as behavioral risk analysis or predictive modeling for insider threat prevention in 200 words or fewer not mentioned above.
  - e. For example, if vendor has a single product that provides multiply capabilities, then there would be a separate Technical Capabilities Matrix completed for each capability of that product.
3. Police Check Inquiry Form: Each person (up to three persons) representing the vendor.

## VENDOR SUBMISSION INSTRUCTIONS:

Vendors should submit the Vendor Information, Technical Capabilities Matrix(s) and Police Inquiry Check Form(s) as a single response with multiple attachments per vendor electronically (email) in PDF format by January 30, 2025, to [ITP@usdoj.gov](mailto:ITP@usdoj.gov). Please password protect the Police Check Form(s).

All submissions should include "DOJ Insider Threat Program RFI Response for **VENDOR NAME**" in the subject line.

## CURRENT TIMELINE:

RFI Issuance: December 17, 2024

Vendor Questions Due: January 24, 2025

Vendor Submissions Due: January 30, 2025

Vendor Registration Response by DOJ: February 14, 2025

Vendor Capabilities Briefing Due: February 20, 2025

## DISCLAIMER:

This RFI is for informational purposes only. This is not a solicitation for proposals, and responses will not result in contract awards. DOJ reserves the right to use or not use any information provided in response to this RFI.

## QUESTIONS:

Please submit questions related to this RFI to [ITP@usdoj.gov](mailto:ITP@usdoj.gov) by January 24, 2025. All questions should include "DOJ Insider Threat Program RFI Question" in the subject line.