Vendor Questions
I am inquiring about the Request for Information (RFI): Insider Threat Program Technical Solutions. Is this a new requirement or are there incumbents or related contracts currently providing similar services for the department? If so, could you provide the task order, contract number and vendor names?
Our product can be deployed on-premises and even when the customer asks for a cloud deployment, we can support that without moving any data (CUI/ITAR, etc.) outside the premises of their organization. While, in principle we can obtain a FedRAMP certification, it may be the case that our product does not necessarily need it. Also, if you deem that we should be eventually getting FedRAMP certification even for on-prem deployments, would it be a showstopper if we don't have FedRAMP certification at the time of submission?
Regarding the Request for Information for Insider Threat Program Technical Solutions, the SAM.gov posting lists two response due dates: the top of the notice lists January 7, 2025 while the body of the posting lists January 24, 2025. Please confirm that vendor responses are due on January 24, 2025.
I'm hoping to find out if the work outlined in the RFI is currently being performed under an incumbent contract or task order for the JMD, or if this is new work which may be procured if responses to the market research are favorable. If there is an incumbent, is it possible to learn the name of the current vendor and corresponding contract or task order number?
I am having issues with filling in the Technical Capabilities Matrix. On the first page, under 'describe each product…in 200 words of fewer' – there isn't a box to input text. On the next page (page 2), where it asks for deployment options, I can input text, however, it not only inputs the text on page 2, but also page 1 and 3. (See attached). Deleting text from page 2 or 3, removes it from the document entirely. Can you send me a new copy of that PDF, or would it be acceptable to create my own document to provide the required technical responses? Please advise.
As it relates to Case Management capabilities, could you please clarify if you are seeking a case management solution that will be 1) deployed as a standalone, 2) integrates with case management solutions, or 3) offers case assignment management capabilities with SOC tasks?
Please confirm if the Department of Justice requires responses to be submitted directly from the product vendor or systems integrators who will include all vendors associated with the solution.
Will the Department of Justice require a minimum set of technical capabilities or solely exploring all possible solution capabilities?
During the Industry Day presentations, will additional presenters be able to join virtually via conference call?

On the question “If yes, what level is the product FedRAMP certified (IL4-IL6)?” - Did you mean to say Low, Moderate, or High? It appears frameworks are being mixed as FedRAMP certifies low, moderate, and high and DoD as IL4-IL6.
On the question “If yes, what level is the product FedRAMP certified (IL4-IL6)?” - How should a vendor that is FedRAMP moderate certified answer as FedRAMP certification does not indicate IL4-IL6 designation.
We recommend changing the question “If yes, what level is the product FedRAMP certified (IL4-IL6)” to “If yes, what level is the product FedRAMP certified (low, moderate, or high)?”
Is this procurement for one office, or will we be presenting it to several different offices?
Is there a requirement to be IL4-6 certified?
Can vendors bring marketing materials to share with attendees?
Can vendors bring a banner and tablecloth to display their company name at the event?
What is the Government’s anticipated timeline for a potential solicitation release?
What is the current state of the program?
What technologies and infrastructure are currently being used?
Are there specific challenges that DOJ is facing to warrant the market research request?
Please confirm that the questions for this RFI are due on 1/7?2025, but the actual responses are due on 1/24/2025 per instructions on SAM
The instructions say to email our submission in one email with all of the forms attached; however, the police form is full of PII (SNN, place of birth, etc.) Is there a more secure way to get these to you? Can we SAFE them to you? Or can we password protect them?
The Vendor Information template has three fields at the bottom for us to indicate who will be attending, but they are grouped somehow in the background and when you change one, they all change. This does not allow 3 separate names. Is there a way to fix this? Or can we list our attendees in the body of our response email?

Instructions indicate that vendors should complete just one “Industry Day Vendor Information Template file per submission, no matter the number of products”. However, the form offers space to provide only one “Product Name” and associated “Type of Product”. If a vendor has more than one product, or a product with multiple capabilities (aka type of product) we are unable share this information in the Industry Day Vendor Information Template as it is currently formatted. Will the government clarify the instructions or provide an updated form to allow for multiple products and product types to be entered?
In the “Industry Day Vendor Information Template”, the “Years Vendor in Business” field is formatted for month and year, rather than a numeric value. Will the government confirm you want the month and year the company was founded and not actually the number of years in business?
There is a formatting issue with the “Industry Day Vendor Information Template”. We are to complete the names of personnel representing our company at the Industry Day in March. However, when a single name is entered into the form, all three fields are automatically completed with that same name. Will the government please provide a new form that allows for three unique names to be completed?
There is a formatting issue with the “Industry Day Technical Capabilities Matrix” file. We are to complete three text boxes as noted in a, b, and c below. However, these boxes are not formatted to allow for separate entries. When you enter text into any of these three fields, the text becomes the same across all three fields. Will the government please provide a new form that allows for three unique entries to the questions below? 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. 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.
Is this RFI response limited to vendors on the STARS III contract vehicle or is it open to all vendors?
Is the government seeking a service-oriented solution only to meet the Objectives outlined in the RFI, where the focus would be on the expertise and capabilities of the vendor to deliver ongoing support, consulting, or managed services?
Is the government seeking the procurement of products or technologies only to achieve the stated Objectives?

Is the government looking for an integrator who will collaborate with product teams to deliver a combination of tailored services, technology solutions, and system integration in order to achieve the Objectives described in the RFI?
The RFI on GSA eBuy and the RFI on SAM.gov have conflicting deadlines for the vendor questions, vendor submissions, and vendor registration response. Would the government please clarify the deadline for these items?
In the RFI, you make reference to a FedRAMP certification. Does that imply that the DOJ is looking solely for a SaaS offering? Will the DOJ sider on-premises solutions? Will the DOJ consider a hybrid approach of on-premises and SaaS solutions?
Will the DOJ utilize responses to this RFI to down select vendors for the industry day?
Can the DOJ define what they mean by “Data Integrator?”
Can the DOJ define what they mean by “AI Integrator?” Is that asking if the vendor solution can detect AI having been utilized in a threat? Or perhaps the vendor is utilizing AI that is integrated into the overall solution?
Can the DOJ define what they mean by “Image Analysis?” Would that be a capability to analyze image files (e.g., pictures) OR the capability to analyze forensic image file collections (e.g., EO1 files)?
If an endpoint solution is required or accepted as part of a larger solution, how many endpoints would need to be monitored for threats?
There was some confusion around dates as it appears some were updated/modified. I wanted to confirm that the deadline today is just for questions, and that the below timeline is accurate. CURRENT TIMELINE:RFI Issuance: December 18, 2024 Vendor Questions Due: January 7, 2025 Vendor Submissions Due: January 24, 2025 Vendor Registration Response by DOJ: February 14, 2025
Will the Industry Day include a formal presentation by the Government, or will it consist solely of individual vendor demonstrations of capabilities?
Who is the audience for the presentations (e.g., technical evaluators, program managers, senior leadership), so that we can tailor the level of detail in our presentation.
If a vendor has multiple related solutions that address different aspects of the Insider Threat Program, or a single solution addressing multiple program objectives, is it permissible to showcase these in a single presentation, or should they be separated?

Are there specific formatting or technical requirements for advance presentation submissions (e.g., file types, file size, resolution, compatibility)?
What is the preferred method for vendors to submit presentation materials in advance, given the restriction on USB drives?
Will the Government provide equipment to display submitted presentation materials, or should vendors plan to bring and use their own devices for presentations and demonstrations?
Considering the absence of Wi-Fi at the venue, are vendors permitted to use personal hotspots for internet connectivity during solution demonstrations, or should we prepare for a fully offline demonstration environment?
We encountered an issue while completing the Vendor Information Template. Specifically, the final three fields for participant names appear to be linked. When a name is entered into one field, the other fields automatically populate with the same name. Editing any of these fields updates all the others to match, making it impossible to enter unique names for multiple participants.
There is conflicting documentation concerning the timeline and due dates. The GSA eBuy posting and respective documentation states the deadline for an RFI response is January 7, while the SAM.gov announcement states that only questions are due January 7, and the response is due January 24. Can you verify the correct response deadline for this RFI?
Since no WiFi will be available at the Industry Day Event, is it a safe assumption that vendors cannot bring and use a WiFi hotspot for their technical presentation? If a WiFi hotspot is acceptable, will vendors be able to conduct a live product demonstration during their technical presentation?
Are there specific AI algorithms or models that are preferred?
Publicly Available Electronic Information - can we assume that social media of employees/contractors is fair game once a reasonable suspicion is identified? At what point can credit data (FCRA covered) be used in the investigation - either OSINT or subscription based data?
Data Loss Prevention - is there a DOJ standard tool for DLP or does it vary by component?
Are you looking at blockchain in terms of resource usage in mining, or cryptocurrency trading?

Do you plan to leverage zero trust for insider threat hunting?
Is this RFI for a specific DOJ Component or a DOJ-wide Insider Threat program?
Which group would be managing this Insider Threat tool?
Is there a specific use case / example regarding the Image Analysis Tool in association with Insider Threat?
Who will the audience be for the presentation (e.g., executives, insider threat analysts, administrators, etc.)?
Please provide a timeline for this RFI Process to Final Contract Decision, or when is the Target “Go Live” date for this Solution.
Has this project been funded and approved, if not what/when is the process for that approval?
Is this Insider Threat Project part of a larger solution set being considered by DOJ, ie… DLP?
What types of integrations will DOJ need for this ITM Solution? (Example- SIEM)
Does DOJ desire/require a consolidated view and management of all User Behavior analytics and Data Risk across the main pillars of exfiltration, Email, End Point, and Cloud?
Do you anticipate vendors and/or service providers will present a custom solution to DOJ for the Industry Day demo in March?
Does DOJ prefer a COTS solution? Custom Development solution? Low-code/no code platform solution? Multiple platform/product solution managed by a Service Provider?
Who are the Project Stakeholders and Sponsor groups?
Does DOJ anticipate selecting a single solution to deter, detect, and mitigate insider threats?

What type of Microsoft licensing would be available for the Insider Threat solution?
Would DOJ modify their Microsoft licensing agreement to support this effort, if warranted?
Do the Project Sponsors have a desired contract start date? delivery date?
What are the existing Insider Threat tools being deployed at DOJ?
What is the AI Strategy at DOJ?
What type of dashboards and tools exist for Project Sponsors to identify and analyze Insider Threats?
What are the current Case Management solutions leveraged by the DOJ Stakeholders for this Insider Threat initiate?
What is the current technology landscape at DOJ for the following capabilities (related or unrelated to Insider Threat monitoring): • 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
Does the DOJ have a developer team to build GIS based applications? Or does the DOJ look for out of the box ready to use applications?

Who will be trained? What material will be used for training? What location is the training at? Is training based on proposed products in the RFI or other 3rd party products?
What data files are used? Are images hosted on-prem or in the cloud? What is the level of the Image Analysist?
Can we get a list of what data will be used for integration? What is the DOJ's definition of integrating?
What specific AI use cases are you currently exploring or implementing within the Department of Justice?
What challenges have you faced in scaling AI technologies, particularly in law enforcement or case management applications?
How do you currently assess the ethical implications and bias in AI algorithms used within your organization?
What integration challenges exist with your existing technology stack when implementing AI?
Are there specific trends in AI that you are looking to leverage, such as Natural Language Processing (NLP) or machine learning for predictive analytics?
What is your preference in terms of the underlying AI technology stack (e.g., proprietary, open-source, hybrid)?
Are you open to leveraging open-source AI components, or do you prefer using commercial AI platforms?
Can you provide more details on the challenges faced during the integration of AI technologies within the DOJ's operations, particularly related to fraud detection or anomaly identification?
What are the key types of data you need to search and analyze (e.g., case files, legal documents, metadata)?
How do you currently manage large datasets and perform searches across multiple sources (internal, external, public)?
Are there pain points related to search performance, indexing, or accuracy that you are experiencing?

What are the trends you see in analytic search that could improve search speed and relevance in your environment?
Can you provide more details about the challenges the DOJ has encountered in the implementation and scaling of the Real-time Analytical Intelligence Database (RAID)?
What performance or operational issues have been identified with RAID, particularly regarding the handling of large-scale data and integration with tools like i2 Analyst's Notebook and GIS?
Are there any gaps in the RAID system's ability to support cross-case analysis, and how can these be addressed?
What are the main challenges you encounter in managing cases from start to finish (e.g., case tracking, document management, collaboration)?
How do you currently track case progress, deadlines, and key events across multiple stakeholders?
What existing systems are you using for case management, and what limitations are you facing with those systems?
Are you looking for enhanced reporting and analytics capabilities integrated with case management?
Given the delays and budget overruns with the Litigation Case Management System (LCMS), can you share the main reasons behind these challenges? Were they related to integration with existing systems, user adoption, or other factors?
How is the DOJ addressing the unification of case management across multiple divisions? Are there specific areas where collaboration is still lacking, and how can a solution improve this?
What data sources are you currently integrating, and what challenges do you face in combining data from various systems?
Do you have a centralized data warehouse or do you operate on a decentralized model for data storage?
What data formats and protocols are commonly used across your systems (e.g., structured, unstructured, APIs)?
How do you handle data quality, consistency, and transformation during integration?

Can you elaborate on the data governance standards and centralized data catalog you are implementing? How do you ensure compliance across different components of the DOJ?
What types of sensitive data are you most concerned about preventing from being leaked or mishandled?
What tools or policies do you currently use for DLP, and what gaps do you see in your current DLP capabilities?
How do you address challenges related to monitoring and protecting data across both cloud and on-premise environments?
Are there specific trends in DLP technology (e.g., cloud-native DLP, AI-powered DLP) that you are looking to explore?
Are you looking for AI tools to detect fraud, misconduct, or other specific activities?
How do you currently assess potential fraudulent activities or anomalous behavior within data?
Are you interested in real-time detection and monitoring, or batch processing of data?
What type of AI detectors (e.g., anomaly detection, pattern recognition) do you find most relevant to your mission?
What types of images are you analyzing (e.g., surveillance footage, crime scene photos, legal documents)?
What specific image recognition or classification tasks do you need assistance with?
How do you currently process and extract actionable information from large image datasets?
Are you exploring AI-powered tools for automated image analysis or pattern recognition?
How do you envision leveraging image analysis capabilities in the DOJ's current AI and data strategy? Are there any specific areas, such as investigative or case management, where image analysis is most needed?

What specific training requirements do you have for your staff, especially in terms of technology adoption and security awareness?
Are you interested in using AI to enhance the training process or automate aspects of it (e.g., AI-driven simulations, adaptive learning)?
What are the challenges you face in ensuring that training is consistent, up-to-date, and measurable across the department?
Do you require ongoing access to training materials, or are you looking for on-demand training resources?
How has the DOJ implemented the training and upskilling of the workforce to support AI adoption and data literacy? What challenges have you encountered in ensuring consistency and engagement across the department?
What specific user activities do you need to monitor to ensure compliance, security, and operational efficiency?
How do you currently track user activity across your systems, and where do you see gaps in monitoring capabilities?
Are you concerned with detecting insider threats or simply ensuring compliance with internal policies?
How do you currently handle alerting, reporting, and auditing of user activities?
Can open source tools be used to address some of these needs?
What types of user behaviors are critical for detecting risks such as fraud or data breaches?
How do you differentiate between normal user behavior and potential threats?
What challenges do you face in accurately identifying anomalous behavior across large user bases?
Are you looking for AI-driven analytics to improve the accuracy of threat detection based on user behavior?

Can open source tools be used to address some of these needs?
What types of publicly available data do you need to monitor or access (e.g., news, social media, legal databases)?
How do you currently gather and analyze this publicly available information for your operations?
Are you looking for automated tools to help in the collection and analysis of this information at scale?
What challenges do you face with data privacy and the ethical use of publicly available information?
How are you currently utilizing blockchain data, and what use cases do you find most critical (e.g., financial transactions, tracking assets)?
Are you experiencing challenges in analyzing blockchain data at scale or across different platforms?
What specific trends in blockchain analysis are you looking to leverage (e.g., fraud detection, forensics)?
Do you require real-time blockchain data analysis, or is batch processing acceptable?
Are there any emerging technologies you are particularly interested in exploring for enhancing your operations (e.g., IoT, edge computing, quantum computing)?
How do you typically evaluate and adopt innovative technologies, and what obstacles do you face in this process?
What role does automation play in your current workflows, and how are you looking to expand its use in the future?
Are there any specific areas in your current tech stack where you see room for breakthrough innovations that could improve efficiency or security?
Should the product be deployed on-premise or in the cloud?

Would the Department of Justice provide the provisioning of required server and network infrastructure, or would this be handled by the vendor?
What would be the approximate number of users and locations in scope for the deployment?
What is your preference regarding the hosting of Large Language Models (LLMs)? Are you considering on-premise deployment, or do you prefer publicly hosted LLM solutions?
How do you view the use of open-source components in your technology stack? Are you open to integrating open-source tools, or do you prefer proprietary solutions for key capabilities?
It's not clear who we should send the form to, and in addition, this form requires an SSN. It is not a good practice to send PII information over the general email process. Can you please advise?
two of the documents are not accepting data correctly (see screenshots below)..As noted below, when you enter data in one field, the fields below auto fill also. As such, please provide a revised version of those two documents …
Is there a cost for use of the table being provided for the event?
Is this a one-day event…or is it for multiple days?
Will an external presenter be able to able to participate in the presentation part of the event?

Since the Police Inquiry form requires SSN numbers to be provided, is there a process for submitting that document encrypted?

DOJ's Responses
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
FedRAMP is not required for a vendor to participate in this information gathering event.
The due date for questions has been updated to January 24, 2025, which is also the due date for vendor responses.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
Please find attached the updated Technical Capabilities Matrix.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
Vendor submissions should be made directly by the vendor who owns the product.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
Presenters can not join virtually via conference call. This is an in-person event only.

Please find attached the updated Technical Capabilities Matrix.
Please find attached the updated Technical Capabilities Matrix.
Please find attached the updated Technical Capabilities Matrix.
This is an information gathering event sponsored by DOJ. However, insider threat professionals from other government entities are permitted to attend.
FedRAMP is not required for a vendor to participate in this information gathering event.
Yes, a vendor may bring marketing materials to share with attendees.
Yes, a vendor may bring a banner and tablecloth to display its company name.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
The due date for questions has been updated to January 24, 2025, which is also the due date for vendor responses.
The Policy Inquiry Form can be password protected if the Social Security Number is included on the form.
Please find attached the updated Vendor Information Template.

If a vendor has multiple products, it should fill out a Technical Capabilities Matrix for each product.
Please find attached the updated Vendor Information Template.
Please find attached the updated Vendor Information Template.
Please find attached the updated Technical Capabilities Matrix.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored. Service-oriented solutions are out of scope for this event.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.

This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
The due date for questions has been updated to January 24, 2025, which is also the due date for vendor responses.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
The due date for questions has been updated to January 24, 2025, which is also the due date for vendor responses.
The Government will welcome the attendees and vendors.
The event is open to all Insider Threat Professionals.
The vendor has the option to provide a capabilities briefing for each technical product.

For vendor capabilities briefings, a Microsoft Office 365 Suite compatible product should be utilized. There is 50 Mb file size limit for email and the file should be attached as a zipped file when submitting to itp@usdoj.gov.
The only method to provide the vendor capability presentation is itp@usdoj.gov.
DOJ will load the presentations provided by the deadline to itp@usdoj.gov for the vendor capability presentations onto a government-furnished computer. Vendors should plan to use their devices for any presentation at their assigned table.
Vendors are permitted to use personal hotspots at their assigned tables but there is no guarantee of connectivity. However, for the capability presentation, the presentation must be provided in advance to the itp@usdoj.gov.
Please find attached the updated Vendor Information Template.
The due date for questions has been updated to January 24, 2025, which is also the due date for vendor responses.
Vendors are permitted to use personal hotspots at their assigned tables but there is no guarantee of connectivity. However, for the capability presentation, the presentation must be provided in advance to the itp@usdoj.gov.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.

This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
The event is open to all Insider Threat Professionals.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
The vendor has the option to provide a capabilities briefing for each technical product.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event sponsored by DOJ. However, insider threat professionals from other government entities are permitted to attend.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.

This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
DOJ's AI Strategy is in compliance with M--24-10 "Advancing Governance, Innovation , and Risk Management for Agency Us of Artificial Intelligence and M-24-18 "Advancing the Responsible Acquisition of Artificial Intelligence in Government."
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.

This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.

This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.

This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.

This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.

This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.

This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
This is an information gathering event, not a solicitation for proposals. All possible technical solution capabilities are being explored.
The Policy Inquiry Form **MUST** be password protected if the Social Security Number is included on the form. *****Please note that all Personally Identifiable Information (PII) transmitted will be received exclusively by the designated security group, ensuring confidentiality and adherence to applicable privacy and security regulations.*****
Please find attached the updated Vendor Information Template and the Technical Capabilities Matrix.
There is no registration fee for vendors or attendees for this event.
This is a one day event.
This is an in-person event only.
The Policy Inquiry Form can be password protected if the Social Security Number is included on the form.