Questions received by 6/12/25 11:30am v2

RFI

Q: Could you clarify if this is a new requirement or if there is a contract in place? If so, could you please provide us with the contract number?

A: *The incumbent is Thundercat Technologies (NNG15SC92B-15JPSS24F00000686) for supplying licenses for Salesforce/Recon. The services have not yet been awarded. No award of DMS licenses has been issued. It is expected that this will be submitted as a Small Business set-aside.*

Q: What is the intent behind the multi-tenant requirement (4.4.1(a))?  Who would the tenants be in this case?  Generally, single tenant implementations are more secure and reliable since they have dedicated resources. They also simplify the requirements, eliminating requirements such as 4.4.3(b).

A: *Currently ATR will likely be the only tenant in the platform, but we want to leave an opportunity to structure such that if other components within DOJ would like to work in the system, it is structured at the outset to accommodate that for efficiency and scalability and that instance level security is available if needed.*

Q: What is behind the 1 petabyte requirement? Are you expecting to store a lot of HD video, since this is an immense amount of storage, even for that purpose.

A: *The Division has more than 1 petabyte of existing data related to its matters in various repositories which it would like to consolidate and store with a matter tracking application, so that Staff has a unified user experience.*

Q: Is the ATR expecting to have 1 PB of high performance storage or is this expected to be split among the tiers?  How much storage will be needed in the high performance space?

A: *The storage requirement does not require high-performance storage. It may also include data that is not accessed over 90 days and can be put into lower tier storage to save costs.*

Q: What are the DOJ Cloud platform requirements mentioned in 4.2.9(a)?

A: *The requirement refers to the ability of the platform to be functional at an enterprise level, meaning that all the functionality is scalable as the agency grows, that it meets performance requirements at an enterprise level and that it allows for integration with other enterprise level systems within ATR’s security boundaries, or outside its boundaries as permissible and required. See other requirements under Unified Platform, Integrations, Advanced Security, Scalability and Adaptability, and Compliance and Export Capabilities which are key components of an enterprise architecture.*

Q: Could you clarify the 4.2.2(a) requirement for a CRM/API integration platform?   Are you intending that the solution includes features of a CRM or that it integrates with CRMs that are hosted in FedRamp environments?

A: *Yes, ultimately the features of a CRM platform for workflow, automation and API integration are of high value to ATR. If another product that is not classified as a CRM but has native capabilities to manage workflows, add automation to routine business tasks and integrate multiple diverse platforms where relevant data is stored (i.e. Relativity, ServiceNow, CourtLinks, etc.) it will be considered.*

Q: Based upon requirements 4.4.7(a),  and 4.3.21(a), it looks like the USDOJ is looking to host their own solution in one of the major cloud providers. Is the organization open to a SaaS/PaaS solution where the solution vendor handles hosting responsibilities?

A: *Yes, a SaaS/PaaS provider is acceptable if the platform is FedRAMP-compliant and meets all FISMA and NIST security requirements.*

Q: RFI Reference. Page 5, Section F. Vendor Responses. Point 1. "Respondent must select either Yes (it meets), No (it does not meet), or N/A (the requirement does not apply to the Respondent’s solution(s) within the three defined categories." Please note that Appendix A excel does not have the "N /A" option.  Please confirm if the Department will provide a revised excel OR should we include a comment in "Column G", where "N / A" is applicable.

*A: Please disregard the requirement for N/A. That was removed from the spreadsheet. All categories apply.*

Q: Could you please elaborate on how we should approach the columns in Appendix A when considering features for the MVP? Specifically, should each column represent the complexity of implementing a particular feature, or should we focus on selecting specific features that we intend to include in the MVP? Any guidance on how to best represent our approach to the MVP in this appendix would be greatly appreciated.

Q: Appendix A refers to the features that come “out of the box” or through configuration in the vendor provided solution. Ultimately, ATR would like to see the majority of the features in Appendix A to be included in the MVP as out of the box, requiring minimal configuration. If 100% of the feature is straight out of the box with modest low-code configuration required, then it qualifies as “out of the box.”

*A:* *If you can offer at least 80% of the features in an MVP with moderate development or through integrations with another product, identify the product you can use to integrate with in your response and you can mark it as a moderate (i.e., more complex than low-code/no-code, but modest development LOE) configuration.*

*If more than 80% of the feature is missing without significant development and cannot be met through integration with another product, mark as a significant (i.e., majority of work involves complex development LOE) configuration.*

*With respect to the MVP, it is up to each vendor to decide which features of Appendix A will be included as part of its MVP implementation. Each vendor should identify which parts of Appendix A will be included with respect to its response to Question F.2 through F.4 of the RFI.*

Q: Would DOJ accept a response that demonstrates alignment with the Division’s modernization vision, while clarifying that our solution, Signulu, is not yet FedRAMP certified, but is being developed to be FedRAMP-High or Moderate compliant? We are also considering StateRAMP and developing Signulu to be StateRAMP-compliant to ensure broader applicability.

*A: Due to timing of the need, any vendor responding to the RFI must have achieved FedRAMP High or Moderate status prior to their submission.*

Q: Could DOJ clarify which specific artificial intelligence capabilities are most valuable for enhancing legal and evidence management workflows?

*A: ATR intends that AI capabilities may include: AI-powered document classification; pattern recognition across document sets stored within and across matters; historical outcome analysis on similar cases; predictive models to generate case timeline and budget projections; deadline tracking and priority analysis; workload balancing recommendations; performance metrics; and budget forecasting*

Q : Beyond general API integration, are there specific DOJ systems or platforms that Signulu must integrate with (e.g., PACER, Relativity, Microsoft 365, ServiceNow)? Are there preferred integration frameworks or security protocols DOJ requires?

*A: ATR specific integrations include ServiceNow, Relativity, Microsoft 365, Courtroom document portals such as Courtlinks, and Oracle. Integrations must be compliant with all NIST and FISMA standards.*

Q: Appendix A references the need to store up to 1 petabyte of matter-related data. Could DOJ clarify the expected access protocols, authentication mechanisms, and security controls for unlicensed users accessing this data?

*A: Unlicensed users would need access to a community portal which would be integrated with the zero-trust Department Identity Management Systems, such as Zscaler and/or Okta using SAML. All security controls must conform to NIST and FISMA standards relating to zero trust architectures.*

Q: Beyond the MVP deployment estimate, what is DOJ’s anticipated timeline for: Full system rollout, user onboarding and training, and optimization and performance benchmarking?

*A: ATR is looking for the vendor to provide their timeline to meet an MVP that they deem viable based on the requirements from Appendix A it intends to provide as part of an MVP.*

Q: Could DOJ clarify expectations regarding licensing models for the proposed solution? Specifically: Are there preferred licensing structures (e.g., named users, concurrent users, enterprise- wide)? Should the solution support tiered access levels (e.g., investigators, attorneys, analysts, external reviewers)?

*A: ATR defers to the vendor for how it structures licensing models. Price is an important consideration to ATR. ATR intends to have various user roles as part of its access groups, including those named above.*

Q: Does DOJ anticipate the need for data migration from existing legacy systems into the new LEMMS/DMS platform? If so: Could DOJ provide guidance on the volume and format of legacy data? Are there specific systems or repositories that must be integrated or sunset?

*A: Yes, Data migration will be a part of this effort. The collection of metadata and artifacts within these disparate repositories equals approximately 1PB of data. ATR intends to sunset all of its legacy systems to decrease costs. For purposes of knowledge management capture, it is important that the legacy information is preserved for future searching.*

## *Description of the Legacy Case Management System*

*The legacy collective Case Management System (CMS) is comprised of roughly 13 Oracle-based tracking systems, and 1 SQL-based tracking system that houses evidence and matter related information for our civil, criminal, FOIA and economics programs. In addition to these systems that track important metadata and artifacts related to an investigation, ATR also houses matter-related document artifacts in multiple document repositories (e.g. eRoom, iManage, network shares, OneDrive, Confluence, etc.). The purpose of these systems and repositories is to collect in an organized manner, all related content for an investigation to manage, track, report on, collaborate and retain through the lifecycle of a matter – from its origination to its conclusion and disposition.*

## *Case Management System & Data Content*

*CMS data is comprised of user created content such as emails, memoranda, images, official forms and records, spreadsheets and the like that could potentially include sensitive PII, as well as Grand Jury Sensitive material that should be treated with extra care.*

*CMS is segmented into two systems: The Case Management component (14 separate systems) and the Case-specific Document Repositories (more than 5 document management systems or network share repositories).*

### *Case Management Component*

*The Case Management component houses data relevant to merger, non-merger, criminal, FOIA and economic-based information used in the analysis of cases. This component allows authorized authenticated users to view and manipulate matter data, conduct logical analyses of datasets, upload files, and do limited searches on matters and documents. The applications are both web-based and on-premises applications. Some, but not all, systems interconnect. However, sharing information across systems is difficult, if not impossible. Most of these systems require manual data-entry and are not available or connect to the public to collect information.*

### *Case-specific Document Repositories*

*Some artifacts collected within the Case Management component are stored in Oracle-based repositories on premises and in Azure. Multiple other systems, such as iManage and the evidence tracking system store artifacts in SQL-based repositories on premises and in Azure. A third set of repositories are contained on Windows-based NetApp shares on premises and in Azure. The information is manually uploaded to the repositories by the end-users and is stored differently from section to section within ATR.*

Q: Does DOJ require vendors to provide auditability and transparency for AI-driven features, including explanations for AI decisions and bias mitigation strategies?

*A: Yes*

Q: Is DOJ expecting vendors to provide a sandbox environment for testing integrations, user training, or patch validation prior to production deployment?

*A:* *Yes*

Q: Are there any DOJ-specific requirements regarding data residency (e.g., U.S.-based data centers only) or compliance with NIST SP 800-53 and FIPS 140-3 standards?

*A: All data must reside within the United States and must be housed on Government-approved data centers. All NIST and FISMA standards must be met. DOJ data cannot be replicated or backed up to foreign sites.*