CRDF Global
Request for Proposal Questions & Answers
Released August 13, 2026

The following questions and answers are provided in response to inquiries submitted regarding the Request for Proposals, "Seeking a Research Security Subject Matter Expert (Product Manager) and a Software Developer for the Full Development of the Research Security Case Management Tool".

These questions and answers are provided for informational purposes only and do not modify, amend, or supersede the terms of the Request for Proposals. In the event of any inconsistency between this Q&A and the RFP, the RFP shall govern. Responses reflect CRDF Global's interpretation of the RFP requirements as of the date of release. Respondents are responsible for monitoring the official procurement platform for updates or additional clarifications.

Questions and Answers:

Q: The anticipated contract issuance date is September 30, while the alpha milestone is also listed for the end of September. Should bidders propose a revised alpha date based on the actual agreement execution date?
A: Yes. Bidders should propose milestone dates, including the alpha, relative to the agreement execution date rather than to fixed calendar dates. Contract issuance is anticipated within two to three weeks of the August 21 submission deadline, with September 30 as the outer bound. Should negotiations with the selected vendor take longer than anticipated, deliverable deadlines will be revised from the actual execution date to support successful implementation.

Q: Which operating systems must the baseline standalone application support?
A: At minimum, the baseline application must run on Windows. Support for Linux and macOS should be proposed as Optional Capabilities, alongside any other optional capabilities the bidder offers.

Q: Will a contractor selected for Task Two only be paired with a Task One product manager selected by CRDF Global?
A: Yes. The contractor selected for Task Two will be paired with the Product Manager selected for Task One, who will serve as the technical point of contact for the development team. The Product Manager will provide a wireframe, feedback, user stories and story points, and other relevant information to ensure the software is effective and efficient for its intended audience. In addition, the Product Manager and the development team will coordinate with the experts selected under RFP 1, Research Security Toolkit: Risk Assessment Guide, Program Starter Kit, and Model Template and Workflow Library (REQ26-0594), to ensure the products are logically consistent and mutually supportive.

Q: Will CRDF Global arrange and fund the independent data-architecture and security audit, or should the Task Two bidder include that service in its proposed team and cost?
A: CRDF Global will arrange and fund the independent security assessment, which could include penetration testing and a code audit, through a qualified third party engaged separately by CRDF. Task Two bidders should not include this assessment in their proposed team or cost, and should not perform it themselves. An independent assessment must be conducted by a party other than the developer of the software, and that separation of duties is intentional. Bidders are responsible for supporting the assessment and for delivering the standard development artifacts that make it possible. The following are required Task Two deliverables:

- A threat model identifying the anticipated attack vectors and the mitigations applied to each.
- An architecture and data-flow diagram showing the components of the tool and how information moves through it.
- Static application security testing (SAST) and dependency scan output from the development team's continuous integration pipeline.
- A written no-network-egress attestation for the local deployment mode, with the supporting test evidence.

Q: To support our technical approach, we intend to include a short prototype demonstration (a link to a demo video and, optionally, a downloadable Windows build). Is supplementary material of this kind acceptable?
A: Yes. Supplementary material of this kind is acceptable and encouraged. Demonstrative evidence of your technical approach is welcome, provided it accurately represents the proposed approach to the software, past performance on similar applications, or particular assets or skills offered by your development team.

Q: The RFP mentions the tool should "present as an application rather than a website." Would a packaged desktop application with an embedded web-based interface (instead of requiring users to open a browser manually) satisfy this requirement?
A: Yes, provided the final user experience meets the intent. A packaged desktop application with an embedded interface is acceptable so long as the end user never has to open a browser and never perceives the tool as a website. The final product should be packaged and presented so that users feel confident in its security and its lack of network access. This phrase in the RFP is intended to require intentional user-experience design that communicates the tool's air-gapped nature through the interface itself.

Q: For updates and patches, does the end customer expect a simple manual installer flow, or some other offline-friendly update method?
A: We are open to developer recommendations on the best method for updates and patches. The tool is intended to be hosted on a website alongside the full toolkit, where users download the

application. Whatever method is proposed, it should give even the least technical end user a simple process for applying updates and patches.

Q: Should the application include a standard installer and uninstaller (similar to typical Windows desktop software), or are there any specific installation or deployment expectations?
A: A standard installer and uninstaller, as is typical for Windows desktop software, is preferred. The application should feel familiar and comfortable to its intended end users.

Q: Does the application need to be completely self-contained, or is it acceptable for the installer to install required runtime components and dependencies (for example, .NET runtimes or database packages) if they are not already present on the machine?
A: The application must be packaged with all required runtime components and dependencies included. The installer should not rely on components already being present on the machine, and it should not download runtimes, database packages, or other dependencies during installation. The delivered package must be able to install and run on a machine with no internet connection, consistent with the tool's self-contained and air-gapped design. Within that constraint, the choice of technology and build approach is open to the developer. The baseline requirement is a self-contained package that installs and runs on Windows; support for macOS and Linux should be proposed as Optional Capabilities. Where a developer proposes macOS or Linux support, any runtime tied to a single operating system, such as .NET on Windows, should be shown to operate fully across the proposed platforms.

Q: Is the expectation that an institution can simply copy or move the application and its data to another machine, or should installation always be performed through the installer?
A: The preferred outcome is that an organization fully owns the application once it is downloaded. The ability to copy the application and its data from one machine to another would reinforce that ownership. However, if that approach proves technically complex or creates conflicts with privacy or data-ownership requirements, then local data ownership and non-transmission of data take priority over portability.

Q: Will CRDF also handle the language localization for the Case Management Tool user interface?
A: If multiple-language functionality is proposed by the developer and selected by CRDF Global, CRDF Global will arrange the translation of the interface to enable that functionality.

Q: The delivery schedule for the case management tool calls for a working prototype by end of September which might be very close to the contract issuance date? This schedule looks challenging especially as task one includes partnering with future users to gather/document requirements and priorities. Starting with an early prototype based on the RFP requirements and

then using it as a catalyst for prototype refinement may be an approach to meet aggressive timelines.
A: Contract issuance is anticipated within two to three weeks of the August 21 submission deadline, with September 30 as the outer bound. Should negotiations with the selected vendor take longer than anticipated, deliverable deadlines will be revised from the actual execution date to support successful implementation. Respondents are encouraged to provide revised deliverable schedules and structure based on their specific expertise and suggested format.

Q: The solicitation states that offerors may propose for Task One, for Task Two, or for both, and that CRDF Global anticipates one or more awards. Can CRDF Global confirm that a proposal for Task Two alone is fully responsive and will not be scored lower on that basis than a proposal covering both tasks?
A: CRDF Global can confirm that a vendor who submits a proposal for Task Two alone will be considered fully responsive and will not be scored lower than a proposal covering both tasks. CRDF Global seeks to find the best technical approach for both tasks, and vendor(s) who provide the best technical approach in line with the objectives and goals of the RFP will be selected.

Q: The Proposal Requirements section refers to a provided budget template. That template does not appear to be attached to the solicitation as posted. Can CRDF Global make it available, or confirm that the cost table reproduced in the solicitation body is the required structure?
A: CRDF Global can confirm that the cost table within the solicitation is the required structure.

Q: The page limit is stated as 10 pages per Task, excluding CVs and cost proposals. Does the Task Three narrative count against the Task Two page allowance, or is Task Three treated as its own section with its own allowance?
A: The Task Three narrative counts against the page allowance, interested vendors should be aware that task three is intended to provide costing for coordination, cooperation, and reporting. CRDF Global does not expect significant narrative surrounding Task Three activities.

Q: The cost table lists Task Three separately for the Product Manager and for the Software Developer. Should an offeror proposing only Task Two complete only the Software Developer line for Task Three and leave the Product Manager line blank?
A: Correct. A vendor submitting a proposal for only Task Two or only Task One should complete only the Software Developer line or Product Manager line respectively, while leaving the other line blank.

Q: If Task One and Task Two are awarded to different offerors, will CRDF Global convene a joint kickoff and maintain a single integrated schedule across both awards, or will each contractor manage to its own agreement?

A: If Task One and Task Two are awarded to different vendors, CRDF Global will convene a joint kickoff and maintain a single integrated schedule across both awards. The intent of the Task One Product Manager is to provide advice and guidance to software developers from the perspective of institutional stakeholders from within a Research Security Office, so that final software will be effective and efficient for its intended audience.

Q: The Timetable anticipates contract issuance by September 30, 2026. The Anticipated Performance Schedule places the prototype and alpha milestone, a first working build of the full tool, at the end of September 2026. Read together, the first build could fall due on or before the date the agreement is executed. Can CRDF Global confirm the intended execution date, or confirm that the milestone dates shift relative to actual execution?
A: Contract issuance is anticipated within two to three weeks of the August 21 submission deadline, with September 30 as the outer bound. Should negotiations with the selected vendor take longer than anticipated, deliverable deadlines will be revised from the actual execution date to support successful implementation.

Q: The requirements and design baseline is due within three weeks of execution and is led by Task One. If the two tasks are executed on different dates, does that three week clock run from the later of the two executions?
A: CRDF Global anticipates issuing both awards on the same timeline. However, should awards be issued on different timelines, each contract shall have its own deliverable schedule and due dates reflective of the scope and schedule necessary to achieve required deliverables.

Q: Is the end of November 2026 final delivery date fixed by the funding instrument, or does it move with the execution date?
A: The completion date of the project is fixed by the funding instrument.

Q: The period of performance ends December 31, 2026. Task Three depends in part on deliverables from the companion Research Security Toolkit RFP, REQ26-0594. If those components are delayed, is an extension of the period of performance available, or would the Task Three scope be reduced instead?
A: Should deliverables from the companion solicitation REQ26-0594 be delayed, vendors selected for REQ26-0595 will not be held accountable for that delay, Task Three scope would be reduced as necessary.

Q: Who holds final approval authority over the requirements specification and prioritized backlog: the Task One product manager, or CRDF Global?
A: CRDF Global, and its funder hold final approval authority over all deliverables, product specifications, and requirements.

Q: Will CRDF Global establish a documented change control process for requirements introduced after the baseline is approved, including a mechanism for adjusting schedule or cost where a change is material?
A: Requirements will be baselined at the Requirements and Design Baseline milestone. Any changes after that will require a written change request and joint review by CRDF Global and the Contractor. Material changes affecting scope, schedule, effort, or cost will require a contract modification before work proceeds. Non-material clarifications within the approved scope will be managed through normal project coordination.

Q: If Task One is not awarded, or is awarded materially later than Task Two, does Task Two proceed against requirements authored by CRDF Global, and on what schedule?
A: Should Task One go unawarded or materially later than the Task Two award, Task Two vendors will proceed against requirements authored by CRDF Global and on a schedule mutually agreed upon within the contract vehicle.

Q: Task One is to distinguish need-to-have from want-to-have capabilities. Will the need-to-have set, once baselined, be treated as the contracted scope for Task Two, with want-to-have items handled as separately priced additions?
A: This specific task for the Task One vendor is to determine if capabilities and features outlined within the Task Two requirements are needed by research security offices, or if they are nice to have features. For the purposes of this solicitation vendors interested in responding to Task Two should consider the required features within the RFP as need-to-have capabilities, and optional features as want-to-have capabilities.

Q: Release acceptance sign-off is a Task One deliverable and formal user acceptance testing is a Task Two activity. Where the product manager withholds sign-off on grounds of fit to research security practice rather than defect, how does CRDF Global expect that to be resolved?
A: The final software product is intended to serve research security practitioners across the globe. The purpose of the Task One Product Manager having release acceptance sign-off is to ensure that the product serves its intended purpose. However, should the final product meet criteria as outlined in the contract, and is not defective CRDF Global will coordinate a resolution between the two parties.

Q: Which operating systems must the installers target, and at which minimum versions? Windows, macOS, and Linux each carry distinct packaging, signing, and testing effort, and the cost proposal will reflect the set CRDF Global names.
A: At minimum, the baseline application must run on modern Windows OS to include at minimum Windows 10 and 11. Support for Linux and MacOS should be proposed as Optional Capabilities, alongside any other optional capabilities the bidder offers.

Q: Must the application install and run without administrator privileges, or is an administrator assisted installation acceptable? Many research institutions restrict standard user installation, and this materially affects the packaging approach.
A: An administrator assisted installation is acceptable.

Q: Is code signing required for the delivered installers, meaning Authenticode for Windows and Apple notarization for macOS? If so, will CRDF Global hold and provide the signing certificates, given that CRDF Global owns the resulting software, or should the offeror procure certificates and price them?
A: Yes, all delivered installers shall be signed. Offerors are expected to deliver a documented, reproduceable build and signing pipeline sufficient for CRDF Global to independently produce and sign the released product. Vendors shall provide unsigned products alongside signed products at each milestone.

Q: Is there any constraint on the underlying technology stack? The requirement that the tool install and launch without a command line and present as an application rather than a website is compatible with a bundled runtime, and we would like to confirm that a bundled runtime is acceptable.
A: The application must be packaged with all required runtime components and dependencies included. The installer should not rely on components already being present on the machine, and it should not download runtimes, database packages, or other dependencies during installation. The delivered package must be able to install and run on a machine with no internet connection, consistent with the tool's self-contained and air-gapped design. Within that constraint, the choice of technology and build approach is open to the developer. The baseline requirement is a self-contained package that installs and runs on Windows; support for macOS and Linux should be proposed as Optional Capabilities. Where a developer proposes macOS or Linux support, any runtime tied to a single operating system, such as .NET on Windows, should be shown to operate fully across the proposed platforms.

Q: What record volume should the tool be designed for at a single institution, both at initial adoption and over a multi-year retention period? This drives the storage and search design.
A: The tool should be designed to support up to several million case records in a single-institution deployment while maintaining responsive search and reporting. A practical planning envelope is a one-time import of up to roughly 25,000 records at initial adoption, to accommodate institutions migrating an existing backlog; a sustained intake at the high end of several thousand new case records per month; and full searchability of all records across a retention period of at least seven to ten years and potentially indefinite.

Q: Are there accessibility requirements for the application interface, such as Section 508 conformance or WCAG 2.1 AA? These are achievable but must be scoped and tested rather than assumed.
A: Yes. As a federally funded product, the application is expected to meet Section 508 and WCAG 2.1 AA conformance, and offerors should scope and price accessibility work accordingly rather than treating it as assumed. Offerors should include in their pricing a self-assessed Accessibility Conformance Report (ACR), delivered at final delivery, together with remediation of the gaps that assessment identifies. A third-party accessibility audit is not required and should not be priced. CRDF Global will verify accessibility independently. Bidders should describe their approach to accessibility testing within the technical approach, including the tools and methods used to produce the self-assessment.

Q: The tool stores its records in a single database file the institution owns outright. Is there an expectation that the file format be readable by common third-party tools, or is a documented schema with an export path sufficient?
A: Either approach is acceptable. Bidders may propose a database file in an open, standard format that is directly readable by common third-party tools, or a format specific to the application accompanied by documented schema and a reliable export path to standard formats. Whichever approach is proposed should be described and justified within the technical approach, including how it preserves the institution's ability to access and retain its own records over the long term, independent of continued support for the application, and how it accommodates encryption of records at rest should an institution require it.

Q: Task Two requires support for an independent data-architecture and security audit prior to any public release. Who engages and funds that audit, CRDF Global or the contractor? If the contractor, should it be priced within core scope or as a separate line?
A: CRDF Global will arrange and fund the independent security assessment, which could include penetration testing and a code audit, through a qualified third party engaged separately by CRDF. Task Two bidders should not include this assessment in their proposed team or cost, and should not perform it themselves. An independent assessment must be conducted by a party other than the developer of the software, and that separation of duties is intentional. Bidders are responsible for supporting the assessment and for delivering the standard development artifacts that make it possible. The following are required Task Two deliverables:

- A threat model identifying the anticipated attack vectors and the mitigations applied to each.
- An architecture and data-flow diagram showing the components of the tool and how information moves through it.
- Static application security testing (SAST) and dependency scan output from the development team's continuous integration pipeline.

- A written no-network-egress attestation for the local deployment mode, with the supporting test evidence.

Q: Where in the performance schedule is that audit expected to occur, and is remediation of audit findings expected to complete within the period of performance?
A: The audit is expected to be conducted at the start of December, following the completion of pilot feedback iteration and remediation of audit findings is expected to be completed within the period of performance.

Q: Given that the activity is supported by the Department of State Bureau of Arms Control and Nonproliferation, are any federal control baselines flowed down to the contractor, such as NIST SP 800-171 or CMMC?
A: No.

Q: Will the contractor be exposed to Controlled Unclassified Information, export controlled data, or personally identifiable information during pilot support or testing? The confidentiality provision is clear on treatment, and we are asking about classification so that handling controls can be scoped correctly.
A: No. The contractor will not be exposed to Controlled Unclassified Information (CUI), export controlled data during the pilot support or testing. The only personally identifiable information the contractor may be exposed to during pilot testing are the names and emails of pilot testers.

Q: Does the append-only audit trail require cryptographic tamper evidence, such as hash chaining or record signing, or is enforcement at the application and database layer sufficient for the intended use?
A: Cryptographic tamper evidence is required in the baseline. Hash chaining of audit records is sufficient for the intended use; full record signing with a key infrastructure is not required for the desktop runtime version. Each audit entry should incorporate a hash of the preceding entry, so that any alteration or deletion of a prior record is detectable on verification. The tool should provide a means for a user or reviewer to verify the integrity of the chain. Enforcement at the application and database layer remains expected, but is not sufficient on its own. The local database file is directly accessible to anyone with access to the machine, and application-layer controls do not detect modification made outside the application. Given that the audit trail is the basis for the tool's evidentiary value, tamper evidence should not depend solely on the application being the only path to the data. Bidders should describe their proposed approach to hash chaining, how the integrity check is exposed to the user, and how chain verification is preserved across the export, import, and update paths described elsewhere in this Q&A.

Q: Is there a requirement to encrypt the local database file at rest, and if so, how does CRDF Global envision key custody for an institution owned, locally deployed store?

A: There is no requirement to encrypt the local database file at rest. However, developers who seek to improve security features of the software can propose encryption at rest, with keys stored on the local machine of the user.

Q: Which languages, if any, must be delivered as complete translations at final delivery, and which are satisfied by multilingual readiness through externalized interface strings only?
A: Required languages have not yet been determined, however, CRDF Global expects the language set to include, but not necessarily be limited to, English, Spanish, French, Portuguese, Mandarin, Arabic, and Hindi. The required languages for externalized strings will be set with the selected contractor during contract negotiations.

Q: Who supplies translation content: CRDF Global, the Task One product manager, or the developer? If the developer, translation should be priced as a separate line since it is a linguistic rather than an engineering cost.
A: If multiple-language functionality is proposed by the developer and selected by CRDF Global, CRDF Global will arrange the translation of the interface to enable that functionality.

Q: Is right to left script support required, for example Arabic? This affects layout engineering and testing well beyond string externalization and should be confirmed before pricing.
A: If multiple-language functionality is proposed by developer and selected by CRDF Global, right to left script support will be expected to be included within that feature.

Q: The optional capabilities list includes changing language settings within the tool. Should this be understood as runtime language switching by the end user, distinct from the externalized string readiness already in core scope?
A: Yes, these are distinct. Externalized interface strings are required in core scope, so that the interface can be translated without modifying the code. Runtime language switching, meaning an in-application setting that allows an end user to change the interface language while the tool is running, is the optional capability and should be priced separately. Bidders should note that CRDF Global will arrange for the translation of interface text itself; the optional capability covers the functionality to select and apply a language, not the production of translations.

Q: How many pilot institutions does CRDF Global anticipate, and in which countries or regions are they located?
A: CRDF Global expects to pilot the software product with trusted partners across the globe who conduct research security functions within their institution. CRDF Global expects at minimum 10 pilot users, across Latin America, Africa, Europe, Central Asia, and Southeast Asia.

Q: Is any travel expected for pilot deployment, training, or the knowledge transfer session, or is remote support sufficient? If travel is expected, should it be priced within the proposal or handled as a reimbursable.
A: No travel is expected for pilot deployment, training, or the knowledge transfer session at this time remote support is expected to be sufficient.

Q: Who recruits pilot institutions and manages their participation and availability? A limited pilot deployment carries very different effort depending on whether the contractor is responsible for scheduling and follow through.
A: CRDF Global will be responsible for recruiting and managing pilot institution participation and availability.

Q: Will pilot institutions use real case records or synthetic test data? This determines the handling controls and the confidentiality posture required during the pilot window.
A: Pilot institutions will use synthetic test data to test limits, and capabilities of the beta tool as provided for the pilot test.

Q: Optional capabilities are to be priced separately. When proposals are compared on the Price and Cost factor, is the comparison made on core scope, or on the total including all proposed options? An offeror who prices options thoroughly should not be disadvantaged against one who omits them.
A: When proposals are evaluated on Price and Cost factors it will be solely on the core scope. Optional features are intended to provide possible options that could be added to the core scope should funding permit.

Q: Is there a budget range or ceiling for this procurement, whether for Task Two alone or across all tasks? Cost realism is a stated subfactor, and a range would let offerors calibrate scope rather than guess.
A: CRDF Global does not publish a fixed budget ceiling for this procurement. Offerors should price based on the scope of work, their proposed technical approach, and prevailing market rates for comparable expertise. Cost realism will be evaluated based on the alignment between proposed cost, level of effort, and the technical approach, not against an undisclosed internal ceiling.

Q: For the central client-server deployment mode with authentication, role based access control, and single sign on: does CRDF Global expect this delivered and accepted within the period of performance, or is it a candidate for the design-forward compatibility treatment the solicitation invites?
A: Should this feature be accomplishable within the stated period of performance closing December 31st, 2026 with all required steps (pilot, iteration, audit, etc.), the developer should

clearly note that within their proposal. However, if it is not this is a candidate for the design forward-compatibility treatment outlined in the solicitation.

Q: If the client-server option is exercised, which single sign on protocols must be supported, and would the hosted instance be operated by CRDF Global, by adopting institutions, or by the contractor?
A: The client-server mode is an Optional Capability and is not part of the baseline scope. Should it be exercised, the hosted instance would be operated by the adopting institution on its own infrastructure and within its own network. CRDF Global does not intend to host instances on behalf of institutions, and the contractor would not operate instances in production, consistent with the principle that an institution's case records remain entirely within that institution's control. Specific single sign on protocol requirements are not determined at this time. Should this optional capability be exercised, requirements will be defined in coordination with the selected Product Manager and developer, taking into account the identity infrastructure in use at adopting institutions. Bidders may describe the protocols and directory integrations their approach would support, but should not assume a fixed requirement set.

Q: Documented integration interfaces for a risk assessment framework and for grant and research management systems depend on components under REQ26-0594. If those specifications are unavailable during the build, should the interfaces be delivered as documented extension points against an assumed schema?
A: Yes. Where the specifications under REQ26-0594 are not available during the build period, the integration interfaces should be delivered as documented extension points built against a clearly stated assumed schema. Bidders should document the assumptions made, the data elements expected, and what would need to change once the specifications are finalized, so that a future effort can complete the connection without redesigning the tool. This is consistent with the RFP's treatment of full connectors as future scope beyond 2026. Where possible, the assumed schema should be informed by coordination between the Task One product manager and the experts selected under REQ26-0594, rather than developed in isolation.

Q: The Contractor Requirements ask for demonstrated ability to incorporate cost sharing, leverage existing resources, and provide in-kind contributions. Is cost share a scored element, and if so is it evaluated within the Price and Cost factor or elsewhere? Is there a target percentage?
A: Yes, cost share is a scored element. It is evaluated within the Price/Cost factor, alongside overall cost compared to market rates, cost realism, and price structure. There is no fixed target percentage, offerors are encouraged to propose cost-sharing, leveraged resources, or in-kind contributions where feasible, and these will be considered favorably as part of the overall cost evaluation, but proposals are not required to meet a specific cost-share threshold to be competitive.

Q: Deliverables must contain no network callbacks and the tool must run with no network egress, while Task Two also requires a documented approach to distributing updates and patches. Can CRDF Global confirm that update distribution is expected to be manual, meaning a downloadable signed installer, and that an in-application update checker would not be acceptable even on an opt-in basis?
A: Confirmed. Update distribution is expected to be manual. Updates and patches will be published as downloadable, signed installers on the website hosting the full toolkit, and applied by the user from that downloaded file. An in-application update checker is not acceptable, including on an opt-in basis. Any such check requires an outbound network call, which is inconsistent with the no network egress requirement and with the attestation and supporting test evidence required as a Task Two deliverable, and it would not function on an air-gapped machine regardless. A capability that is present but disabled by default does not satisfy this requirement; the delivered application should contain no outbound network functionality at all. Within that constraint, CRDF Global remains open to developer recommendations on how the manual update process is designed. The method proposed should give even the least technical end user a simple, reliable process for applying an update, including verification of installer signatures and preservation of existing case data and audit history across updates.

Q: The warranty runs 90 days from final acceptance. With final delivery at the end of November and closeout in December, that period extends past the December 31, 2026 end of the period of performance. How does CRDF Global intend to contract the warranty tail, and is any retainage held against it?
A: The 90-day warranty will begin once CRDF Global formally accepts the final deliverables. Before the end of the 90-day warranty period, CRDF Global and the Contractor may discuss and mutually agree on any extended warranty, if needed in the agreement award stage. Any agreed-upon extended warranty will remain in effect even after the contract's Period of Performance has ended. CRDF Global does not plan to extend the Period of Performance solely for the warranty period and does not intend to withhold any retainage for the warranty.

Q: The third-party intellectual property indemnification is stated without a cap. Will CRDF Global consider a limitation of liability proportionate to the contract value, or is the indemnity intended to be uncapped as drafted?
A: CRDF Global's position is that third-party IP indemnification is not capped, given that the deliverables are intended for CRDF Global's exclusive ownership and future redistribution to research security offices globally, and that offerors are contractually required to disclose all third-party and open-source components and their licensing terms in advance (per the Ownership, Source Code, and Licensing section). Offerors that comply fully with the component disclosure and licensing-compatibility requirements substantially limit their own exposure under this

clause. CRDF Global may, in its sole discretion, consider proposed limitations of liability on a case-by-case basis during contract negotiation with the selected offeror(s).

Q: Third party and open source components must be offered under permissive licenses compatible with CRDF Global ownership. Would CRDF Global consider weak copyleft licenses that impose obligations only on modification of the component itself, such as MPL 2.0 or LGPL, or should the bill of materials be restricted to permissive licenses only, such as MIT, BSD, and Apache 2.0?
A: CRDF Global will accept permissive licenses and file level weak copyleft where obligations attach only to the component itself and do not extend to CRDF developed code or restrict CRDF's redistribution rights. LGPL will be evaluated case by case if identified in the proposal bill of materials.

Q: Are proposals expected to include a signed statement accepting the Ownership, Source Code, and Licensing section, or is a written acknowledgment within the technical narrative sufficient?
A: A written acknowledgment of these terms is acceptable within the technical narrative. These terms are listed upfront to ensure that prospective vendors are aware of the required terms and conditions associated with this software development contract.

Q: Since local data ownership and non-transmission take priority, are there specific expectations for protecting locally stored case and risk-assessment data, such as encryption at rest, Windows user/account-based access controls, or alignment with organizational security policies?
A: Protection of locally stored case data is a priority, and bidders should address it across three areas. Encryption at rest is not mandated in the baseline, as institutions may rely on full-disk encryption managed by their own IT. However, given the sensitivity of the records the tool holds, bidders are encouraged to propose encryption at rest as a security enhancement. Where proposed, the technical approach should specify the key custody model, whether keys are derived from a user passphrase, held in the operating system's native credential store, or managed at the institution level, and should address key recovery, since loss of a key would render records unrecoverable against retention requirements. Proposals should also note any effect the chosen model has on the ability to move an institution's application and data between machines. For access control, the local deployment should rely on the operating system's existing user account and file permission model rather than introducing a parallel account system, so that access to the data store follows the permissions the institution already administers. Bidders should describe how the application and its data store are installed and permissioned so that the records are not readable by other user accounts on a shared machine. Where the client-server option is exercised, authentication and role-based access control apply as described in that optional capability. For alignment with organizational security policy, the tool should be deployable without requiring an institution to weaken or make exceptions to its existing endpoint, disk encryption, backup, or account management policies. Bidders should identify any assumptions their approach makes

about the host environment, such as required privileges at installation or runtime, so that institutions can evaluate the tool against their own security baselines.

Q: Is there a preference for how documents and other case attachments should be stored locally, for example, within the application's local data store, in an application-managed local data directory (e.g. in a local AppData folder), or in an organization's existing local file storage?
A: File and document attachments are an Optional Capability rather than part of the baseline scope. Where a bidder proposes this capability, CRDF Global does not have a fixed preference among the storage approaches described, and bidders should propose the method best suited to their technical approach and justify it. Any proposed method must meet the following expectations. Attachments must reside entirely within the institution's own control, with no transmission outside the institution and no dependency on any externally hosted storage service. Attachments must remain associated with their case records and must be captured by the same backup, export, and portability path as the records themselves, so that an institution can move or restore its complete repository, records and attachments together, without data loss. Access to stored attachments must follow the same access control model as the case data, so that files are not readable by other user accounts on a shared machine. Where an organization's existing local or network file storage is used, bidders should describe how the tool maintains the integrity of the link between a case and its files if those files are moved or altered outside the application, and how such a change is surfaced in the audit trail. Bidders should also address storage growth, including deduplication of identical files attached to multiple cases.

Q: Does CRDF expect the application to provide a dedicated backup and restore function for locally stored data, or would a user-accessible export/import mechanism be considered sufficient for backup/recovery purposes?
A: A user-accessible export and import mechanism is sufficient for backup and recovery purposes; a dedicated backup and restore function is an optional capability. This approach is also consistent with the institutional data ownership requirements outlined in the solicitation, as it allows an institution to move its complete repository between machines and retain its own records independent of continued support for the application.
Where this approach is proposed, the export must capture the complete repository, including all case records, their associated metadata, and the full audit trail, so that a restored instance is a faithful and complete reproduction of the original. Attachments, where that Optional Capability is exercised, must be included in the same export and import path. Bidders should describe how the export is verified for completeness and integrity, how an import handles a restore into an existing instance, and how restore events are themselves recorded in the audit trail, so that the auditability of the record is preserved across a recovery.

Q: We would like to retain joint ownership of the source code associated with delivering product for these two RFPs. Both Rizkly and CRDF would have ownership rights to the code. Can you please let us know if this is acceptable.
A: At this time, CRDF Global is not considering joint ownership of the source code. Our intent is for CRDF to own the final project deliverables, while the Contractor retains ownership of its pre-existing tools, methodologies, and other background intellectual property. This allows CRDF to use, maintain, and enhance the software over time, while protecting the Contractor's existing intellectual property rights.

Q: How many different parties and number of people from each would make up the group that we work with to refine requirements and perform acceptance testing?
A: CRDF Global expects to pilot the software product with trusted partners across the globe who conduct research security functions within their institution. CRDF Global expects at minimum 10 pilot users, across Latin America, Africa, Europe, Central Asia, and Southeast Asia.

Q: For the initial end of November delivery of the Model Template and Workflow Library, we would like to confirm that that this initial product only includes model templates based on English/US region/legal/institutional concepts. The product would provide functionality for users in other regions to populate with model templates specific to their operating environment.
A: The Model Template and Workflow Library delivered at the end of November by the vendors selected under REQ26-0594 will be delivered in English. However, the templates and models provided will be generalized rather than specific to U.S. legal or institutional concepts. The intent of the Library is to provide templated resources to research security practitioners globally, and users in other regions will be able to adapt and populate the Library with templates specific to their own operating environment. This standardization is intended to be complementary to the Case Management Tool. A standardized language and format should allow the Case Management Tool to natively capture fields and terms drawn from research security artifacts such as technology control plans and risk management plans.

Q: Are there any citizenship, residency, or work-location requirements for Task Two development personnel? Given that the tool processes no classified or controlled information and is intended for distribution to institutions globally, may portions of the development work be performed by non-US-based members of a proposing team?
A: CRDF Global does not currently require Task Two development personnel to be U.S. citizens or residents. However, all proposed personnel and work locations must comply with applicable U.S. laws and regulations, including 2 CFR § 200.300, U.S. sanctions regulations, and any applicable export control requirements (e.g., EAR or ITAR), as well as any restrictions included in the resulting award. CRDF Global reserves the right to review and approve the proposed staffing approach to ensure compliance with these requirements and the project's security and technical needs.

Q: The timetable anticipates contract issuance "by September 30, 2026," while the performance schedule sets the requirements and design baseline within three weeks of execution and the prototype/alpha at "end of September 2026." Could CRDF clarify how the milestone dates shift if award occurs in late September? Should offerors propose against the calendar dates as published, or against elapsed time from execution?
A: Award is anticipated within two to three weeks of the proposal submission deadline. Should negotiations with the selected vendor result in agreement execution beyond that period, the deliverable timeline will be adjusted to reflect the actual execution date. Offerors should propose against elapsed time from execution rather than against the published calendar dates. Respondents are encouraged to provide their own schedule and timeline within the proposal, reflecting their expertise and experience in software development. Note that the final product must be complete by the beginning of December 2026 to allow time for the independent security and data architecture assessment.

Q: Task Two builds to requirements defined with the Task One product manager, and CRDF may award the tasks separately or on different timelines. If Task One is awarded later than Task Two, awarded to a different offeror, or not awarded, how should a Task Two offeror plan the requirements baseline? Is a Task Two offeror permitted to propose an interim requirements approach to protect the schedule?
A: Where Task One is unawarded, or awarded materially later than Task Two, Task Two vendors will proceed against requirements authored by CRDF Global, on a schedule mutually agreed within the contract vehicle. Where Task One is awarded to a different offeror on a comparable timeline, the Task Two vendor should plan to build the requirements baseline jointly with that product manager, as outlined in the solicitation. CRDF Global will coordinate between the two awardees. Task Two vendors are permitted to propose interim requirements to protect the development timeline. As noted in the solicitation's scoring criteria, the proposed timeline and the ability to complete within the period of performance are important evaluation factors.

Q: The deliverables require "installers for the target operating systems." Which operating systems and versions must the baseline delivery support: Windows only, or also macOS and/or Linux? Is a single-platform baseline with additional platforms as an optional capability acceptable?
A: At minimum, the baseline application must run on Windows, and baseline support should cover modern Windows versions, to include Windows 10 and Windows 11. A single-platform baseline is acceptable. Support for macOS and Linux should be proposed as Optional Capabilities, alongside any other optional capabilities the bidder offers.

Q: How many interface languages must be populated in the baseline delivery, as distinct from multilingual readiness through externalized strings? Will CRDF supply translations, or is translation within the developer's scope?
A: Baseline delivery requires multilingual readiness through externalized interface strings rather than a live in-application language switcher, which remains an Optional Capability. The baseline should be built to accommodate an interface language set expected to include, but not necessarily be limited to, English, Spanish, French, Portuguese, Mandarin, Arabic, and Hindi. This list may change. Developers are expected to support both left-to-right and right-to-left rendering in the baseline product, so that the interface displays correctly in any of these languages once strings are supplied. CRDF Global will supply the translations for interface terms and text, based on the completed UX design; translation is not within the developer's scope.

Q: Is there a budget range or an expected level of effort for the Task Two core scope that offerors should plan against? This would help ensure cost realism across proposals.
A: CRDF Global does not publish a fixed budget ceiling for this procurement. Offerors should price based on the scope of work, their proposed technical approach, and prevailing market rates for comparable expertise. Cost realism will be evaluated based on the alignment between proposed cost, level of effort, and the technical approach, not against an undisclosed internal ceiling.

Q: Will pricing for optional capabilities be included in the price/cost evaluation alongside core scope, or evaluated separately? Are there optional items CRDF considers likely to be exercised, particularly the central client-server deployment mode, that offerors should plan architecture around from the start?
A: Evaluation will be based solely on the core scope. Optional capabilities will not be scored, on either price and cost or technical factors. This solicitation is for the baseline product, and the optional capabilities list is intended to invite developers to tell us what else they might be able to do with the tool beyond the baseline scope, as possibilities to be considered should funding permit. Vendors will be selected on their technical approach to the core requirements and their ability to deliver the core software product within the required timeline. Offerors should still price each optional capability separately, as noted in the cost proposal format, so that CRDF Global can evaluate whether to exercise any of them following award. Optional capabilities that could be added without extending the development timeline are the most likely to be exercised, subject to available funding.

Q: At what point in the schedule will the independent third-party security assessment occur, and against what standard or framework? If findings require architectural change rather than defect remediation, how will schedule and cost impacts be handled?
A: CRDF Global will arrange and fund the independent security assessment, which may include penetration testing and a code audit, through a qualified third party engaged separately by CRDF

Global. The assessment is expected to be conducted at the start of December, following completion of the pilot feedback iteration. The specific standard or framework against which the assessment will be conducted is not yet settled and will be confirmed prior to the assessment. In the interim, bidders should build to recognized secure development practices and describe the standards they follow in their technical approach. Remediation of findings is expected to be completed within the period of performance. Where findings are architectural rather than defect-level, developers will be expected to remediate at no additional cost to CRDF Global, as security-by-design is a required feature of the software product. Final deliverables are expected to be delivered by the close of the period of performance, fully remediated against all assessment findings.

Q: How many pilot institutions are anticipated, and what level of developer support is expected during the pilot — support hours, response expectations, and whether any onsite or travel participation is required?
A: CRDF Global expects to pilot the software product with trusted partners across the globe who conduct research security functions within their institutions. We anticipate a minimum of 10 pilot users, drawn from Latin America, Africa, Europe, Central Asia, and Southeast Asia. Pilot builds are expected to be functional and operable by pilot users, requiring limited developer input and support. Bidders should propose the level of support hours and response times they consider appropriate for a pilot of this size and geographic distribution. The intent of pilot testing is to gather user feedback from a population representative of the tool's likely end users. No travel is expected or required of developers during pilot testing, and where direct engagement with pilot users is needed, virtual feedback and support sessions will suffice.

Q: Does CRDF hold any existing prototype, wireframes, record schema, or draft requirements from prior work on the Case Management Tool that would be provided to the selected developer?
A: No prior development work on the Case Management Tool has been completed. The only existing artifact is a proof-of-concept prototype that roughly approximates the baseline tool with very limited functionality. This artifact can be provided to the selected developer on request following award. However, developers are being solicited to produce bespoke software built to the baseline requirements, with security as a primary design feature, rather than to extend or refine the existing prototype. The record structure described in the solicitation should be treated as indicative rather than final. Wireframes and detailed requirements will be developed with the Task One product manager following award.

Q: The contractor requirements reference willingness to incorporate cost-sharing, leveraged resources, and in-kind contributions. Is cost-sharing scored, and if so under which evaluation criterion? Is there an expected or minimum level?
A: Yes, cost share is a scored element. It is evaluated within the Price/Cost factor, alongside overall cost compared to market rates, cost realism, and price structure. There is no fixed target

percentage, offerors are encouraged to propose cost-sharing, leveraged resources, or in-kind contributions where feasible, and these will be considered favorably as part of the overall cost evaluation, but proposals are not required to meet a specific cost-share threshold to be competitive.

Q: For the baseline local deployment, should the tool support multiple named user accounts with role-based access on a single machine (for example, a shared research security office workstation with per-user audit attribution), or is a single operator per installation assumed?
A: For the baseline local deployment, either approach is acceptable. At minimum, a single-operator installation must maintain an auditable log of changes recording what was changed and when. A local deployment that supports multiple named user accounts with authentication and per-user audit attribution is preferred. At minimum, a single-operator installation must maintain an auditable log recording what was changed, when, and by whom, with the acting user identified at the point of entry where the deployment does not support authenticated accounts. However, priority is given to delivering the baseline tool within the expected timeline, and bidders should not pursue multi-user support at the expense of that schedule.

Q: If the optional client-server mode is exercised, what scale should we design for — approximately how many users per institution, and what level of concurrent use?
A: Should the optional client-server capability be selected, scale should be designed for a medium to large sized research institution. Total named users per institution should be assumed to be in the low hundreds, with concurrent use well below that figure. However, should this optional capability be selected, final requirements will be determined in coordination with both the selected Product Manager and the selected developer.

Q: Should the baseline architecture be forward-compatible with the optional client-server mode (one codebase supporting both deployment modes), or may the option be treated as a separately architected phase?
A: Ideally, the baseline architecture will be forward-compatible with the optional capabilities and intentionally designed to support future iterations and refinements of the tool. However, CRDF Global is open to developer recommendations, based on your expertise and experience, for how the tool and any optional features should be designed and incorporated. Forward-compatibility should not come at the expense of delivering the baseline product within the period of performance.

Q: For the optional single sign-on integration, are there identity providers already in use among the anticipated pilot institutions (e.g., Microsoft Entra ID, Okta, SAML/Shibboleth) that we should prioritize?
A: Specific identity provider requirements are not determined at this time. Single sign-on integration falls within the optional client-server capability, which is not part of the baseline

scope and may or may not be exercised. Pilot institutions are expected to span Latin America, Africa, Europe, Central Asia, and Southeast Asia, and the identity infrastructure in use across those institutions varies considerably. Should this optional capability be exercised, requirements would be defined in coordination with the selected Product Manager and developer, taking into account the infrastructure actually in use at adopting institutions at that time. Bidders may describe the identity providers and protocols their approach would accommodate but should not assume a fixed requirement set or prioritize any particular provider.

Q: Which target operating systems and minimum versions must the installers support, and is enterprise deployment tooling (e.g., MSI packages for SCCM/Intune) expected?
A: At minimum, the baseline application must run on Windows, and baseline support should cover modern Windows versions, to include Windows 10 and Windows 11. A single-platform baseline is acceptable. Support for macOS and Linux should be proposed as Optional Capabilities, alongside any other optional capabilities the bidder offers.

Q: Would an application shell built on web technologies (e.g., an Electron- or Tauri-packaged, fully offline desktop application) satisfy the requirement that the tool "presents to the user as an application rather than as a website," provided nothing runs in a user's browser?
A: Yes. An application shell built on web technologies, such as an Electron- or Tauri-packaged desktop application, satisfies the requirement provided nothing runs in the user's browser and the user experiences it as a self-contained application. The specific technology stack is open to developer recommendation based on your expertise and experience, so long as the final tool is fully functional and operational in a completely air-gapped environment, with no network calls and no need for network access.

Q: Is a single-file embedded database such as SQLite an acceptable implementation of "a single database file that the adopting institution owns outright," and are there encryption-at-rest requirements for that file?
A: Yes. A single-file embedded database such as SQLite is an acceptable implementation of the required database file. There is no encryption-at-rest requirement in the baseline. However, vendors are encouraged to propose security-by-design features that could be incorporated into the baseline tool to increase the security of the data and user confidence in it. Where encryption at rest is proposed, bidders should address key custody and recovery as described in the response to the earlier question on encryption of the local database file.

Q: Who conducts the independent data-architecture and security audit, against what framework or standard, and where in the performance schedule should we plan for audit and remediation time?
A: CRDF Global will engage a trusted independent third party to conduct the data-architecture and security assessment. The specific framework or standard against which the tool will be

assessed is an open question and will be decided and confirmed with the selected developer at a later date. The assessment is expected to take place at the beginning of December 2026, following pilot feedback and the tool iterations based on that feedback. Assessment and remediation time should therefore be placed after pilot testing in the developer's proposed performance schedule.

Q: Given the no-network-egress requirement, should the documented update-distribution approach assume fully offline delivery (e.g., signed installer packages distributed by the institution) rather than any in-application update mechanism?
A: Yes.

Q: Approximately how many pilot institutions are anticipated, and in which regions and languages?
A: CRDF Global expects to pilot the software product with trusted partners across the globe who conduct research security functions within their institutions. We anticipate a minimum of 10 pilot users, drawn from Latin America, Africa, Europe, Central Asia, and Southeast Asia. Pilot builds are expected to be functional and operable by pilot users, English language only functionality will be acceptable for pilot testing.

Q: Which interface languages must be delivered at final acceptance, versus supported through externalized strings for later translation?
A: The baseline requirement is multilingual readiness through externalized interface strings rather than a fixed set of languages loaded at final acceptance. All interface text must be externalized so that any language can be supplied and applied without modifying the code. The specific languages required at final acceptance will be confirmed at a later date. As of now, CRDF Global expects a minimum set of English, French, Spanish, Portuguese, Arabic, Mandarin, and Hindi. The baseline tool must support both left-to-right and right-to-left rendering, so that the interface displays correctly in any of these languages once the strings are supplied. CRDF Global will provide the translated text for all required languages, based on the completed UX design; translation is not within the developer's scope. Translations will be loaded as they become available, which is the reason the baseline requirement is readiness rather than a fixed set of delivered languages. Live in-application language switching remains an Optional Capability, as noted in the response to the earlier question on runtime language switching. In the baseline, the interface language is selected at installation or through configuration.

Q: Should optional capabilities be priced assuming exercise at award, and may an offeror include selected options (for example, exportable PDF case summaries) within the base delivery schedule where the incremental cost is low?
A: All optional capabilities should be priced separately from the baseline tool, and should not be assumed to be exercised at award. Offerors are encouraged to identify which optional capabilities

they consider feasible to incorporate and finalize alongside the final tool, and to note any that could be delivered within the base schedule at low incremental cost. Where an offeror proposes to include an optional capability within the base delivery schedule, that capability and its cost should still be identified separately in the cost proposal, so that CRDF Global retains the ability to exercise or decline it. Inclusion within the base schedule should not extend the delivery timeline for the baseline product.

Q: What is the total budget allocated for this RFP?
A: CRDF Global does not publish a fixed budget or ceiling for this procurement. Offerors should price based on the scope of work, their proposed technical approach, and prevailing market rates for comparable expertise. Cost realism will be evaluated based on the alignment between proposed cost, level of effort, and the technical approach —not against an undisclosed internal figure

Q: Must the contractor or key personnel be onshore, or can offshore resources be used?
A: There is no onshore requirement for the contractor or key personnel. Offshore resources may be used, provided all personnel and the offeror are eligible to receive a subaward from the U.S. Government — i.e., not sanctioned or debarred — and have the legal work eligibility for whatever jurisdiction they are performing from. This applies unless a specific requirement for work to be performed within the United States is identified for a particular task, in which case that would need to be confirmed separately.

Q: Is there any preference for local contractors?
A: No. CRDF Global does not give preference to local or US-based contractors in the evaluation of proposals. Offerors are evaluated on technical approach, past performance and qualifications, price, and — for REQ26-0595 — proposed timeline, regardless of the contractor's location, consistent with the response provided above regarding onshore/offshore personnel.

Q: Is there an incumbent contractor currently performing any part of this work?
A: No.

Q: Is there an existing prototype, software, source code, requirements document, or other work product that will be provided to the selected contractor?
A: The only existing artifact is a proof-of-concept prototype that roughly approximates the baseline tool with very limited functionality. This artifact can be provided to the selected developer on request following award. However, developers are being solicited to produce bespoke software built to the baseline requirements, with security as a primary design feature, rather than to extend or refine the existing prototype. Wireframes and detailed requirements will be developed with the Task One product manager following award.

Q: Are references mandatory for both Task One and Task Two?
A: Yes, references are required for both Task One and Task Two. In the context of this solicitation, references should point to examples of previous work the offeror has completed that demonstrate the technical capabilities proposed within the technical approach. Examples of completed work, such as prior projects or delivered software, are preferred. These may be supplemented by individuals who can attest to the successful completion of similar scopes of work, or by other evidence-based justification of technical skill.

Q: How many references are required for each task?
A: There is no set requirement for the number of references for either task. CRDF Global expects proposals to include sufficient evidence to demonstrate that the technical scope, as proposed, is achievable by the submitting vendor.

Q: Can relevant experience and references from previous employers/projects of proposed team members be included?
A: Yes. Proposals should include relevant experience and references for proposed team members, including work performed at previous employers or on prior projects, where it demonstrates the individual's qualifications and relevant expertise. This aligns with the Past Performance/Qualifications evaluation factor, which considers the relevant experience of personnel in addition to the offeror's own organizational past performance.

Q: The Timetable anticipates contract issuance "by September 30, 2026," while the Performance Schedule requires the Requirements and Design Baseline within 3 weeks of execution and the Prototype/Alpha build by the end of September 2026 — leaving little to no time between contract execution and the first milestones if the agreement is signed near September 30. Could you clarify whether the Performance Schedule assumes an earlier effective start (e.g., work beginning upon notice of award) or whether these milestone dates would be adjusted based on the actual execution date?
A: Milestone dates will be adjusted based on the actual execution date rather than held to the published calendar dates. The period of performance begins at contract execution, and work is not expected to begin prior to execution, including following notice of award.
Award is anticipated within two to three weeks of the proposal submission deadline, with September 30, 2026 as the outer bound. Should negotiations with the selected vendor result in execution beyond that period, the deliverable timeline will be adjusted to reflect the actual execution date. Offerors should therefore propose against elapsed time from execution rather than against the published calendar dates, and are encouraged to provide their own schedule and timeline reflecting their expertise and experience in software development. Where Task One and Task Two are executed on different dates, the three-week clock for the Requirements and Design Baseline runs from the later of the two execution dates, so that both the product manager and the development team are under contract before the milestone period begins. Note that the final

product must be complete by the beginning of December 2026 to allow time for the independent security and data architecture assessment, and that this end date is fixed by the assessment window.