CRDF GLOBAL

Seeking Authorized Resellers and Integrators to Supply Cybersecurity Software Licenses, Implementation Services, and Training for Ukrainian Critical Institutions

Cybersecurity Improvement Grants (CySIG) – Lot 1: Apparatus of the Verkhovna Rada of Ukraine | Lot 2: NCSH «Okhmatdyt» | Lot 3: Office of the Prosecutor General of Ukraine

REQ26-0910 REQUEST FOR PROPOSAL

Deadline: November 19, 2026 at 23:59 Eastern Time

Summary:
CRDF Global, with support from the United States Department of State, implements the Cybersecurity Improvement Grants (CySIG) program, a competitive program that strengthens the cybersecurity and resilience of central governmental institutions and state-owned critical infrastructure enterprises of Ukraine. Under this program, CRDF Global seeks qualified vendors – authorized resellers, distributors, or integrators of the named cybersecurity solutions – to supply commercial cybersecurity software licenses and subscriptions and to deliver the associated training and implementation services to three Ukrainian beneficiary institutions. This solicitation is organized in three lots: Lot 1, the supply of Splunk Enterprise and Splunk Enterprise Security term licenses and official Splunk administration training for the Apparatus of the Verkhovna Rada of Ukraine; Lot 2, the supply of a Tenable Security Center license for up to 1,500 assets together with professional implementation and configuration services and administrator workshops for the State Non-Commercial Enterprise «National Children's Specialized Hospital «Okhmatdyt» (Ministry of Health of Ukraine) (NCSH «Okhmatdyt»); and Lot 3, the supply of a SentinelOne Singularity Platform subscription (AI SIEM and Singularity Complete EDR for 100 servers) together with deployment, onboarding, and knowledge-transfer services for the Office of the Prosecutor General of Ukraine. Offerors may propose for any one lot, any combination of lots, or all three lots.

Scope:
All three lots share a common structure: the supply of commercial cybersecurity software licensed to the beneficiary institution as end user, with manufacturer support for the full license term, combined with manufacturer-certified services that ensure the beneficiary's own staff can independently operate, maintain, and expand the platform after the grant period. Lot 1 supports the expansion of the Security Operations Center (SOC) of the Apparatus of the Verkhovna Rada of Ukraine with a Security Information and Event Management (SIEM) platform. Lot 2 supports the implementation of a centralized vulnerability management capability for the IT environment of NCSH «Okhmatdyt». Lot 3 supports the deployment of centralized security monitoring and endpoint detection and response for the critical services of the Office of the Prosecutor General of Ukraine.

For each lot, CRDF Global anticipates executing a three-party agreement among CRDF Global, the selected contractor, and the beneficiary institution. Licenses will be registered in the name of the beneficiary institution, services will be delivered to the beneficiary in Ukraine (on-site in Kyiv, remotely, or in a hybrid format as agreed with the beneficiary), and completion of each deliverable will be confirmed by an acceptance certificate signed by the beneficiary and approved by CRDF Global.

The three lots will be evaluated and awarded independently. CRDF Global reserves the right to award each lot to a different offeror, to award any combination of lots to a single offeror, or to make no award for any lot. Offerors proposing for more than one lot may offer a discount conditional on a combined award, provided it is stated separately and does not alter the per-lot pricing.

Period of Performance:
Agreement Execution Date through (anticipated six (6) months from execution). The term of the software licenses supplied under each lot is a deliverable in its own right and may extend beyond the period of performance. For Lots 1 and 2, the license or subscription term is twelve (12) months from delivery of license keys or entitlements to the beneficiary. For Lot 3, the subscription term is twelve (12) months from activation of the beneficiary's tenant.

Licensing, Delivery, and Compliance Terms:
The following provisions are conditions of performance and award, not preferences.

- **Authorized channel.** The offeror must be an authorized reseller, distributor, or partner of the manufacturer for each product offered and must provide a Manufacturer Authorization Letter or equivalent evidence of current partner status valid for sales to end users in Ukraine. Training courses must follow official manufacturer curriculum and be delivered by the manufacturer or by a manufacturer-authorized training partner.
- **Genuine licenses in the beneficiary's name.** All licenses must be genuine, new, not previously activated or transferred, procured through manufacturer-authorized channels, and registered in the name of the beneficiary institution as end user. Manufacturer support and updates must be included for the full license term.
- **License term and entitlement.** Offerors shall state for each license the license term, the entitlement metric (for example, daily data ingestion volume for Lot 1, number of assets for Lot 2, and daily ingestion volume and number of protected servers for Lot 3), the support level, and the event that starts the license term. The license term shall not begin before license keys or entitlements are delivered to the beneficiary.
- **Brand name or equal.** The products named in this RFP reflect requirements identified by the beneficiaries during the CySIG competition. Offerors may propose an equivalent product only if it meets every salient characteristic listed in the relevant lot and is confirmed by the beneficiary as compatible with its environment. The burden of demonstrating equivalence rests with the offeror.
- **Eligibility and compliance.** Because this activity is funded by the U.S. Government, offerors must not be suspended, debarred, or otherwise excluded from U.S. federal awards; must comply with applicable U.S. and Ukrainian sanctions and export control requirements; and must not provide covered telecommunications equipment or services as defined in Section 889 of the FY2019 National Defense Authorization Act (2 CFR 200.216), or any hardware, software, or services developed or provided by Kaspersky Lab or its affiliates.
- **Taxes, duties, and delivery.** The goods and services procured under this RFP are exempt from Value Added Tax (VAT). CRDF Global will provide the selected contractor with an official tax exemption letter confirming this status. All prices must therefore be quoted in U.S. dollars, exclusive of VAT, and must include all other duties, fees, delivery, and administrative costs. Offerors should state in their proposal any obstacle they foresee to applying the exemption. Prices must be firm and fixed in U.S. dollars for the duration of the resulting agreement and shall not be indexed to, or adjusted for, changes in the hryvnia exchange rate.
- **Confidentiality and system access.** Contractor personnel who access beneficiary systems, logs, network documentation, vulnerability data, patient information, or case-related information shall comply with the beneficiary's security rules, sign any non-disclosure undertakings the beneficiary

requires, use such information solely to perform the resulting agreement, and not retain, copy, or disclose it beyond what is necessary for that purpose.

- **Cloud hosting and data handling (Lot 3).** For any cloud-delivered service, the offeror shall state the hosting region of the beneficiary's tenant, the data retention and deletion terms, and the manufacturer's data-processing terms, and shall identify any use of beneficiary data by the manufacturer beyond delivery of the service. These arrangements must be confirmed as acceptable by the beneficiary before award .
- **Warranty and defect remediation.** For a period of [90] days following acceptance, the contractor shall remediate at no additional cost any defect in the delivered licenses or in the configuration it performed that prevents the solution from operating as specified.
- **Payment.** For each lot, CRDF Global will pay for licenses or subscriptions and for services separately, in each case following the signing of the corresponding acceptance certificate by the beneficiary and approval by CRDF Global, within [30] days of receipt of a correct invoice. No advance payment will be made.
- Goods and/or services under this RFP are procured using funds allocated exclusively for the implementation of an international technical assistance project registered in Ukraine in accordance with the procedure established by applicable legislation.

Lot 1: Apparatus of the Verkhovna Rada of Ukraine – Expansion of the Security Operations Center (Splunk SIEM)

Objective: Expand the Security Operations Center of the Apparatus of the Verkhovna Rada of Ukraine by supplying Splunk Enterprise and Splunk Enterprise Security twelve (12)-month term licenses (20 GB/day) with the Splunk Standard Success Plan, and by delivering official Splunk system and data administration training to designated SOC personnel. The platform will provide centralized, real-time log ingestion, correlation, alerting, and investigation, improve mean-time-to-detect and mean-time-to-respond, and support alignment with national cybersecurity requirements, NIST CSF 2.0 (Detect and Respond), CIS Controls v8,NIST CSF 2.0 (Detect and Respond), CIS Controls v8,ISO/IEC 27001, and NIS2-related obligations.

Required Items:

#	Item	Specification	Qty.
1	SE-T-LIC-ST Splunk Enterprise – Term License (with support)	Entitlement: 20 GB/day ingestion; term: twelve (12) months ; Standard Success Plan (manufacturer support) included for the full term	1
2	ES-T-LIC-ST Splunk Enterprise Security – Term License (with support)	Entitlement: 20 GB/day, matching Item 1 and co-termed with it; Standard Success Plan included for the full term	1
3	Splunk Enterprise System Administration (SESA) course	Official Splunk curriculum; one seat per participant	3
4	Splunk Enterprise Data Administration (SEDA) course	Official Splunk curriculum; one seat per participant	3

Salient Characteristics (for any proposed equivalent):

- Centralized SIEM platform deployable in the beneficiary's own environment, capable of real-time ingestion of at least 20 GB/day of logs and events from heterogeneous sources.
- Event correlation, alerting, investigation, and incident response workflow capabilities, with maintained security detection content.
- Manufacturer support equivalent to or better than the Splunk Standard Success Plan, and updates, for the full license term.
- Manufacturer-certified system administration and data administration training equivalent in content and duration to the courses listed above.

Example Activities include:

- Confirm license sizing, entitlement metric, and deployment architecture with the beneficiary before placing the order.
- Procure and deliver the licenses through manufacturer-authorized channels, registered to the Apparatus of the Verkhovna Rada of Ukraine as end user, and provide license keys, entitlement confirmation, and support portal access.
- Ensure the Splunk Enterprise Security license is sized to and co-termed with the Splunk Enterprise license.
- Enroll three (3) designated SOC personnel in each of the SESA and SEDA courses, coordinate course dates, format, and language with the beneficiary, and confirm attendance. All three participants can attend online in English; Ukrainian-language delivery is preferred where the manufacturer or its authorized training partner offers it.
- Obtain and deliver certificates of completion for each participant.

Optional Services (priced separately):

Deployment of the platform is expected to be carried out by the beneficiary's SOC team. The beneficiary will host the platform in its own environment, and its SOC team has prior hands-on experience with Splunk Enterprise Security. Offerors may propose, as a separately priced option, remote technical guidance during deployment (for example, architecture review, advice on data source onboarding, and review of the Enterprise Security configuration). CRDF Global may elect to exercise or decline this option.

Lot 1 Deliverables:

- License keys or entitlement certificates for Items 1 and 2 registered in the beneficiary's name, with manufacturer confirmation of support entitlement.
- Signed acceptance certificate for the delivered licenses.
- Training enrollment confirmation and certificates of completion for three (3) participants in each course (six (6) course seats in total).
- Delivery summary covering items supplied, entitlement (GB/day), license start and end dates, support plan and contacts, and renewal dates.

Lot 2: NCSH «Okhmatdyt» – Centralized Vulnerability Management and Scanning System (Tenable Security Center)

Objective: Establish a sustainable vulnerability management capability at NCSH «Okhmatdyt» by supplying a Tenable Security Center license sized for 1,500 assets (workstations, servers, and IP addresses supporting clinical and laboratory services), delivering professional implementation and configuration services, and conducting administrator workshops for the hospital's information security team. The platform

will enable continuous, automated vulnerability discovery, risk-based prioritization, and remediation tracking across the hospital's IT environment, protect sensitive pediatric health data, and support uninterrupted medical services.

Required Items:

#	Item	Specification	Qty.
1	Tenable Security Center Software License (1,500 Assets)	Sized for 1,500 assets (workstations, servers, and IP addresses supporting clinical and laboratory services); manufacturer: Tenable, Inc. (Columbia, Maryland, USA); license type and term: twelve (12)-month subscription; manufacturer support included for the full term	1
2	Implementation and Configuration Services	Deployment, integration, scan policy configuration, initial baseline scan, and at least two (2) administrator workshops of not less than three (3) hours each for up to five (5) of the hospital's system administrators, delivered online or on-site, in Ukrainian, as described below	1

Salient Characteristics (for any proposed equivalent):

- On-premises vulnerability management platform licensed for at least 1,500 assets, covering workstations, servers, and IP addresses supporting clinical and laboratory services, and deployable in the beneficiary's own environment.
- Active and credentialed vulnerability scanning, risk-based prioritization, dashboards and reporting, and remediation tracking.
- Role-based access control and scan configuration that can be restricted to protect sensitive clinical systems and medical devices.
- Manufacturer support and updates for the full license term.

Example Activities include:

- Hold a kickoff and pre-deployment assessment with the hospital's information security team covering network segments, asset inventory, scan windows compatible with clinical operations, medical and laboratory devices to be excluded from active scanning or scanned only in agreed windows, service accounts for credentialed scanning, and the update method (online or offline)
- Procure and deliver the license through manufacturer-authorized channels, registered to the hospital as end user.
- Specify the server or virtual machine resources required for the platform, to be provided by the beneficiary. The hospital has confirmed that it will provide these resources within its existing virtualized server infrastructure; no additional hardware is required.
- Install and configure Tenable Security Center and the scanning components included in the license within the hospital's environment.
- Integrate the platform with existing infrastructure as agreed with the beneficiary (directory authentication, email notifications).
- Establish scanning policies, scan zones and schedules, and credentialed scanning, with safe-scanning settings that avoid disruption to clinical systems and medical devices.

- Configure dashboards, reports, risk-based prioritization, and remediation tracking workflows, and complete an initial baseline scan.
- Conduct at least two (2) hands-on administrator workshops of not less than three (3) hours each, for up to five (5) participants, covering platform administration, asset and scan management, scan policy tuning, reporting and dashboards, and remediation tracking, so that the hospital's team can independently operate and maintain the system.

Optional Services (priced separately):
Offerors may propose, as a separately priced option, post-implementation remote support for a defined period (for example, [3] months) covering tuning, scan policy adjustments, and operator questions. CRDF Global may elect to exercise or decline this option.

Lot 2 Deliverables:

- License key or entitlement certificate registered in the beneficiary's name, stating the license type, start and end dates , and asset count, with manufacturer confirmation of support entitlement.
- Implementation plan agreed with the beneficiary before deployment begins.
- Installed and configured platform with a completed initial baseline scan and summary of results.
- As-built configuration documentation (architecture, scan policies, schedules, integration settings, and administration procedures), excluding credentials and secrets.
- Administrator workshop agenda, training materials, and attendance records for at least two (2) workshops, in Ukrainian.
- Signed acceptance certificates for the license and for the implementation services.

Lot 3: Office of the Prosecutor General of Ukraine – Centralized Security Monitoring and Endpoint Detection and Response (SentinelOne Singularity AI SIEM and EDR)

Objective: Strengthen centralized security monitoring and incident response at the Office of the Prosecutor General of Ukraine by supplying a SentinelOne Singularity Platform subscription – Singularity AI SIEM with an ingestion tier of approximately 35 GB per day and Singularity Complete Cloud Workload Security (EPP+EDR) for 100 servers with 90-day EDR data retention hosting the institution’s critical services – and by delivering deployment, onboarding, integration, acceptance testing, and knowledge-transfer services. The platform will provide centralized correlation of security telemetry, AI-driven detection, autonomous prevention and response, and retention of security telemetry to support investigations and incident reporting obligations, including CERT-UA notification requirements, protecting the confidentiality, integrity, and availability of sensitive investigative and prosecutorial information and services.

Beneficiary environment: The in-scope servers are virtual machines running supported versions of Red Hat Enterprise Linux and Windows Server. Detailed information on the server estate, log sources, and network connectivity will be shared with the selected offeror at kickoff, under the confidentiality terms of this RFP.

Required Items:

#	Item	Specification	Qty.
1	SentinelOne Singularity Platform – Platform Access (reference SKU PF-PLT-FF-A1)	Access to the Singularity Platform, including initial data ingest; tenant provisioned for the beneficiary; manufacturer: SentinelOne, Inc. (Mountain View, California, USA); term: twelve (12) months from activation	1
2	SentinelOne Singularity AI SIEM, 90-day retention – per daily average GB (reference SKU S1-AISIEM90-GB-A1)	35 GB daily average ingestion; 90-day retention; unlimited queries; Hyperautomation actions, Purple AI queries, and detection rules as included in the manufacturer SKU at this ingestion tier; co-termed with Item 1	35
3	SentinelOne Singularity Complete Cloud Workload Security – per server (reference SKU S1-CMPAI-CW-A1)	EPP + EDR for servers, including NGAV, Rogues/IoT discovery, firewall control, device control, remote shell, Deep Visibility, STAR custom detection rules, annual Purple AI query entitlement, and Standard Support; co-termed with Item 1	100
4	SentinelOne 90-Day Data Retention Extension – per endpoint (reference SKU PM-RT90-ND-A1)	Extends EDR hunting and investigation telemetry retention from 14 to 90 days for the 100 servers in Item 3; co-termed with Item 1	100
5	Deployment and Onboarding Services (one-time)	Tenant provisioning, log-source onboarding, EDR agent deployment, integration, acceptance testing, documentation, and at least one (1) knowledge-transfer workshop of not less than three (3) hours for up to five (5) members of the institution's IT security team, delivered online or on-site, in Ukrainian, as described below	1

Salient Characteristics (for any proposed equivalent):

- Unified platform combining cloud-delivered SIEM and endpoint detection and response under a single management console, with native correlation of endpoint telemetry and third-party log sources.
- SIEM ingestion of at least 35 GB/day from heterogeneous sources (firewalls, identity/Active Directory, DNS, network devices, servers, and applications), with AI-assisted detection, correlation, alerting, and investigation, and retention of at least 90 days.
- Server endpoint protection (EPP + EDR) for at least 100 servers with autonomous prevention, detection, and response, including ransomware rollback where supported by the server operating system, and EDR telemetry retention of at least 90 days.
- Role-based access control and a tenant hosting region and data-handling terms acceptable to the beneficiary.
- Manufacturer support and updates for the full subscription term.

Example Activities include:

- Hold a kickoff and pre-deployment assessment with the institution's IT security team to confirm in-scope servers, log sources, ingestion sizing, maintenance windows, and tenant hosting region and data-handling arrangements.
- Procure and activate the subscription through manufacturer-authorized channels, registered to the Office of the Prosecutor General of Ukraine as end user, and provide tenant access and entitlement confirmation.
- Onboard the identified critical log sources (server operating system logs, including identity/Active Directory; perimeter and application security devices such as firewalls; the email gateway; and EDR telemetry) to the AI SIEM for centralized correlation and detection.
- Deploy Singularity Complete Cloud Workload Security agents on the 100 in-scope servers in phases, within agreed maintenance windows and with a rollback plan, so that critical services are not disrupted; configure prevention and response policies.
- Integrate the platform with agreed systems and configure detection use cases, alerting and notification procedures, and dashboards.
- Conduct functional and acceptance testing with the beneficiary.
- Document alert-handling procedures and incident response runbooks aligned with the beneficiary's existing policies.
- Conduct at least one (1) hands-on knowledge-transfer workshop of not less than three (3) hours, for up to five (5) participants, covering platform administration, monitoring, and incident handling, and transition the solution into operational use so that the institution's team can independently operate it.

Optional Services (priced separately):

Offerors may propose, as separately priced options, (a) post-implementation remote support for a defined period (for example, [3] months) covering detection tuning, policy adjustments, and operator questions; and (b) a twelve (12) month renewal of the subscriptions in Items 1–4 at the same entitlement. CRDF Global may elect to exercise or decline either option.

Lot 3 Deliverables:

- Subscription entitlement confirmation registered in the beneficiary's name, stating the SKUs and quantities delivered, the term start and end dates, support entitlement, and tenant hosting region.
- Implementation plan agreed with the beneficiary before deployment begins.
- Operational AI SIEM with the agreed log sources onboarded, and EDR agents deployed on the 100 in-scope servers.
- Acceptance test results.
- Baseline metrics report at go-live (server agent coverage, onboarded log sources, and initial detection and response times), used to measure project results.
- As-built configuration documentation, detection use cases, alert-handling procedures, and incident response runbooks, in Ukrainian, excluding credentials and secrets.
- Knowledge-transfer workshop agenda, training materials, and attendance records, in Ukrainian.
- Signed acceptance certificates for the subscription and for the deployment services.

Coordination and Reporting with CRDF Global (All Lots)

Objective: Coordinate with CRDF Global and the beneficiary institution throughout the period of performance and document completion of each lot.

Example Activities include:

- Hold a kickoff meeting with CRDF Global and the beneficiary within [10] business days of agreement execution.
- Provide brief progress updates to CRDF Global every two weeks and promptly report any risks to schedule or scope.
- Communicate with beneficiaries in Ukrainian and with CRDF Global in English; provide beneficiary-facing documentation in Ukrainian and reports to CRDF Global in English.
- Prepare a final completion report within seven (7) business days of final acceptance.

Coordination Deliverables:

- Kickoff meeting minutes.
- Bi-weekly progress updates.
- Final completion report with all signed acceptance certificates attached.

Anticipated Performance Schedule:

Milestone	Deliverables	Expected Delivery Date
Kickoff and sizing confirmation	Kickoff with each beneficiary; confirmed license sizing and configuration (all lots)	Within 2 weeks of execution
License delivery	License keys or entitlements registered to each beneficiary (all lots)	Within [4] weeks of execution
Training (Lot 1)	SESA and SEDA completed by three participants each; certificates of completion	Within [3] months of execution
Implementation (Lot 2)	Installed and configured platform, baseline scan, documentation, administrator workshops	Within [3] months of execution
Deployment (Lot 3)	Subscription activated; agreed log sources onboarded to AI SIEM; EDR agents deployed on 100 servers; acceptance testing; documentation; knowledge-transfer workshops	Within [3] months of execution; knowledge transfer and final acceptance may move to within [6] months if war-related circumstances cause delays
Acceptance and closeout	Signed acceptance certificates; final completion report	Within [6] months of execution

Contractor Requirements:

Lot 1 (Apparatus of the Verkhovna Rada of Ukraine – Splunk):

- Current authorized Splunk partner or reseller status with the ability to transact licenses for end users in Ukraine.
- Ability to procure official Splunk Education courses directly or through an authorized training partner.

- Experience supplying SIEM licensing and related services to government or critical infrastructure clients.

Lot 2 (NCSH «Okhmatdyt» – Tenable):

- Current authorized Tenable partner or reseller status with the ability to transact licenses for end users in Ukraine.
- Engineers holding Tenable manufacturer certification or documented equivalent experience implementing Tenable Security Center.
- Demonstrated experience implementing vulnerability management platforms, ideally in healthcare or critical infrastructure environments.
- Ability to deliver services on-site in Kyiv, online, or in a hybrid format, in Ukrainian.

Lot 3 (Office of the Prosecutor General of Ukraine – SentinelOne):

- Current authorized SentinelOne partner or reseller status with the ability to transact subscriptions for end users in Ukraine.
- Engineers holding SentinelOne manufacturer certification or documented equivalent experience deploying Singularity AI SIEM and EDR.
- Demonstrated experience deploying SIEM and endpoint detection and response solutions for government, law enforcement, or critical infrastructure clients.
- Ability to deliver services on-site in Kyiv, online, or in a hybrid format, in Ukrainian.

All Lots:

- Registered legal entity eligible to contract under U.S. Government-funded awards, per the Licensing, Delivery, and Compliance Terms.
- Willingness to enter a three-party agreement with CRDF Global and the beneficiary institution.
- Willingness to accommodate reasonable changes or adjustments to delivery as directed by CRDF Global or the beneficiary.
- Demonstrated ability and willingness to incorporate cost-sharing, leverage existing resources, and provide in-kind contributions where possible to maximize project impact and efficiency.

Proposal Requirements:
Each proposal must include:

Technical Proposal

- A clear statement of which lot or lots the offeror is proposing (Lot 1, Lot 2, Lot 3, or any combination).
- For each lot, a description of the products and services offered, including exact manufacturer part numbers (SKUs) and quantities, license entitlement metric, license term, support level, and a point-by-point compliance statement against the Required Items and Salient Characteristics.
- Delivery approach and schedule: for Lot 1, training format, dates, and language; for Lot 2, implementation methodology, including safeguards for clinical systems and medical devices, and the administrator workshop plan (agenda, format, duration, and number of participants); for Lot 3, deployment methodology, including the log-source onboarding plan, phased EDR agent rollout with safeguards for production servers, the proposed tenant hosting region, confirmation that the offered agents support current Red Hat Enterprise Linux and Windows Server versions, and the knowledge-transfer workshop plan (agenda, format, duration, and number of participants).

- Manufacturer Authorization Letter or equivalent evidence of authorized partner status for each product offered.
- CVs and manufacturer certifications of proposed personnel (required for Lots 2 and 3).
- List of recent, relevant experience with at least [two (2)] references, with past performance clearly included.
- **10-page limit per lot, excluding CVs, authorization letters, and cost proposals**

Written Acceptance of Terms

- Written acknowledgment and acceptance of the Licensing, Delivery, and Compliance Terms and of the three-party agreement structure, together with a self-certification that the offeror is not excluded from U.S. federal awards and complies with the Section 889, Kaspersky, and sanctions requirements. A proposal that does not accept these terms may be found non-responsive.

Cost Proposal in USD

- **NOTE:** Offerors are required to submit their cost proposal using the format below or a template following the same structure. Prices must be submitted in a separate table for each beneficiary institution, with one price for every line item listed, quoted in U.S. dollars exclusive of VAT (see the tax exemption provision above), and valid for at least [90] days from the submission deadline. Optional services and any combined-award discount must be listed separately. Offerors may add rows to show cost-sharing, leveraged resources, or in-kind contributions; all additions should be clearly labeled.

Cost proposal as formatted below (complete the table for each lot proposed):

Lot 1 – Apparatus of the Verkhovna Rada of Ukraine

#	Item Description	Qty.	Unit Price (USD)	Total (USD)
1	SE-T-LIC-ST Splunk Enterprise – Term License with Standard Success Plan; 20 GB/day; term: 12 months	1		
2	ES-T-LIC-ST Splunk Enterprise Security – Term License with Standard Success Plan; 20 GB/day; co-termed with Item 1	1		
3	Course: Splunk Enterprise System Administration (SESA) – price per seat	3		
4	Course: Splunk Enterprise Data Administration (SEDA) – price per seat	3		
	Total Lot 1 (USD)			
	Optional (not part of Total Lot 1): Remote technical guidance during deployment			

Lot 2 – State Non-Commercial Enterprise «National Children's Specialized Hospital «Okhmatdyt»

#	Item Description	Qty.	Unit Price (USD)	Total (USD)
1	Tenable Security Center Software License (1,500 Assets); license type and term: twelve (12)-month subscription	1		

#	Item Description	Qty.	Unit Price (USD)	Total (USD)
2	Implementation and Configuration Services (including baseline scan and at least two (2) administrator workshops)	1		
	Total Lot 2 (USD)			
	Optional (not part of Total Lot 2): Post-implementation remote support			

Lot 3 – Office of the Prosecutor General of Ukraine

#	Item Description	Qty.	Unit Price (USD)	Total (USD)
1	SentinelOne Singularity Platform access, including initial data ingest; 12 months from activation	1		
2	SentinelOne Singularity AI SIEM, 90-day retention; 12 months (unit price per daily average GB)	35		
3	SentinelOne Singularity Complete Cloud Workload Security (EPP + EDR); 12 months (unit price per server)	100		
4	SentinelOne 90-Day Data Retention Extension; 12 months (unit price per endpoint)	100		
5	Deployment and Onboarding Services, one-time (including integration, acceptance testing, documentation, and knowledge-transfer workshop)	1		
	Total Lot 3 (USD)			
	Optional (not part of Total Lot 3): Post-implementation remote support			
	Optional (not part of Total Lot 3): Twelve (12) month renewal of Items 1–4 at the same entitlement			

Offerors proposing for more than one lot may state a discount conditional on a combined award in a separate line below the lot tables. Each lot's total must be stated without that discount.

Contractor Selection Criteria:

Each lot will be evaluated and awarded separately using the lowest price technically acceptable (LPTA) method. CRDF Global will first determine whether each proposal is technically acceptable for each lot proposed, applying the pass/fail criteria below. A proposal that fails any applicable criterion will be rated unacceptable for that lot and will not be considered further for that lot. Among the technically acceptable proposals for a lot, CRDF Global will award to the offeror with the lowest total evaluated price for that lot, provided the price is determined to be fair, reasonable, and realistic. CRDF Global reserves the right

to accept or reject any and all proposals, to request clarifications from offerors, and to negotiate the terms of any subsequent agreement at its own discretion.

Basis of Award:

Technical proposals will not be scored or ranked, and no additional credit will be given for exceeding the minimum requirements. The total evaluated price for each lot is the Total Lot price stated in the offeror's cost proposal; optional services and any discount conditional on a combined award are not included in the evaluated price. Where the same offeror is selected for more than one lot, CRDF Global may apply any combined-award discount that offeror has stated. If two or more technically acceptable proposals for a lot have the same total evaluated price, CRDF Global will award to the offeror proposing the earliest delivery of the lot. CRDF Global retains full discretion to contract for all, some, or none of the items and optional services included in any proposal submitted under this RFP, and to award the lots to the same or to different offerors.

Technical Acceptability Criteria:

Each criterion below is rated Acceptable or Unacceptable for each lot proposed. A proposal must be rated Acceptable on every criterion that applies to the lot to be eligible for award. Evaluation will be based on the documents submitted with the proposal; CRDF Global may, but is not obliged to, request clarification of minor omissions.

Criterion	Applies to	Requirement for an Acceptable rating
1.Manufacturer authorization	All lots	Manufacturer Authorization Letter or equivalent evidence of current authorized partner status, valid for sales to end users in Ukraine, for each product offered.
2. Compliant products and quantities	All lots	Exact manufacturer part numbers (SKUs), quantities, entitlements, and terms matching the Required Items for the lot, or a proposed equivalent that meets every Salient Characteristic and is confirmed by the beneficiary as compatible with its environment.
3. Manufacturer support	All lots	Manufacturer support and updates included for the full license or subscription term.
4. Training	Lot 1	Official Splunk SESA and SEDA courses, three (3) seats each, delivered by Splunk or a Splunk-authorized training partner.
5.Implementation and workshops	Lots 2 and 3	Implementation or deployment methodology covering the Example Activities for the lot, and administrator or knowledge-transfer workshops meeting the stated minimum number, duration, and participants, delivered in Ukrainian.

Criterion	Applies to	Requirement for an Acceptable rating
6. Qualified personnel	Lots 2 and 3	CVs showing manufacturer certification or documented equivalent experience for the engineers who will perform the implementation or deployment.
7. Cloud hosting and data handling	Lot 3	Proposed tenant hosting region, data retention and deletion terms, and manufacturer data-processing terms stated in the proposal, and agent support confirmed for current Red Hat Enterprise Linux and Windows Server versions.
8. Relevant experience	All lots	At least [two (2)] references for comparable supply of licenses or related services, with past performance clearly included.
9. Schedule	All lots	Proposed delivery schedule within the period of performance and consistent with the Anticipated Performance Schedule.
10. Terms and eligibility	All lots	Written acceptance of the Licensing, Delivery, and Compliance Terms and of the three-party agreement structure, and self-certification of eligibility and compliance with the Section 889, Kaspersky, and sanctions requirements.
11. Complete price	All lots	A price for every line item in the lot's cost table, in U.S. dollars exclusive of VAT, firm and fixed, and valid for at least [90] days from the submission deadline.

Timetable:
The procurement process is intended to follow the timeline below.

Activity	Date
Request for Proposal (RFP) Issued	October 20, 2026
Deadline for Questions and Answers	October 27, 2026
RFP Questions and Answers Released	October 29, 2026
Proposal Submission Deadline	November 19, 2026
Anticipated Contract Issuance	By December 15, 2026

Questions and Answers:
Interested parties may submit questions regarding this RFP to Yana Zarakhovska, yzarakhovska@crdfglobal.org . Questions will be accepted through 23:59 Eastern Time on October 27, 2026 and will be addressed as received. Following the close of the Q&A period, a consolidated Q&A document containing questions received and the corresponding responses will be posted alongside the RFP on the CRDF Global website.

Submission:
Proposals should be submitted to Yana Zarakhovska, yzarakhovska@crdfglobal.org no later than **23:59 Eastern Time on November 19, 2026**, with the lot number(s) stated in the email subject line. Proposals should be submitted as electronic documents in PDF, Word, or Excel format.

Background:
CRDF Global is an independent nonprofit organization founded in 1995 in response to the collapse of the Soviet Union and the threat of large-scale proliferation of weapons technology from the region. With support authorized by the Nunn-Lugar Act of 1991 and the Freedom Support Act of 1992, as well private foundation contributions, CRDF Global embarked on bolstering the global scientific community and fostering alternatives to weapons research.

In the past 30 years, our work has expanded to address ever-changing global concerns, but our commitment to ensuring the success of our partners remains the same. We are a leading provider of flexible logistical support, program design and management, and strategic capacity building programs in the areas of higher education, CBRNE security and nonproliferation, border security, cybersecurity, global health, technology entrepreneurship, and international professional exchanges.

With offices in Arlington, VA; Amman, Jordan; Kyiv, Ukraine; Manila, Philippines; Almaty, Kazakhstan; and Warsaw, Poland; CRDF Global's global staff and networks of local community and government stakeholders deliver programs tailored to specific regions that advance U.S. security interests in over 120 countries across the globe.

Vision Statement:
Our world, healthy, safe, and sustainable.

Mission Statement:
Safety, security, and sustainability through science, innovation, and collaboration.

Values:
We do the right thing.
We care about each other and the people we work with.
We work together to deliver excellence

CRDF Global provides equal opportunities to all qualified individuals without regard to age, race, color, religion, sex, sexual orientation, gender identity, national origin, protected veteran status, or disability. We are committed to fostering a respectful, collaborative, and supportive work environment where all individuals can contribute and thrive. We recognize and uphold the inherent value and dignity of every person, and we strive to maintain a workplace that honors a wide range of backgrounds, perspectives, and experiences.

More information is available at www.crdfglobal.org.

Solicitation Terms & Conditions:

Right to Select Suppliers. CRDF Global reserves the right to negotiate with and select all qualified suppliers at its own discretion and is not obligated to inform suppliers of the methods used in the selection process. CRDF Global reserves
the right to dismiss any and/or all suppliers from the bid process and reject any and/or all proposals.

Obligation. This RFP does not bind nor obligate CRDF Global in any way. CRDF Global makes no representation, either expressed or implied, that it will accept or approve in whole or in part any proposal submitted in response to this RFP. CRDF Global may reward, in whole or in part, the proposal at its sole discretion.

Notification. CRDF Global will notify bidders following completion of the evaluation process, as to whether or not bidders have been awarded the contract. The only information regarding the status of the evaluation of proposals that will be provided to any inquiring bidder shall be whether or not the inquiring bidder has been awarded the contract. CRDF Global may, at its sole discretion, inform any inquiring bidder of the reason(s) as to why it was not awarded the contract.

Binding Period. Following the due date of submission of this Proposal, the pricing included in this RFP shall be binding upon the supplier for the duration of the contract.

Hold Harmless. By submitting a response to the RFP, bidder agrees that CRDF Global has sole discretion to select any and/or all suppliers. During or following the conclusion of this process, bidders waive their rights to damages whatsoever attributable to the selection process, materials provided, supplier selection, or any communication associated with the RFP process and supplier selection.

Transfer to Final Contract. The terms and conditions of the RFP, including the specifications and the completed proposal, will become at CRDF Global's sole discretion, part of the final contract (the "Agreement") between CRDF Global and the selected bidder. In the event that responses to the terms and conditions will materially impair a bidder's ability to respond to the RFP, bidder should notify CRDF Global in writing of the impairment. If bidder fails to object to any condition(s) incorporated herein, it shall mean that bidder agrees with, and will comply with the conditions set forth herein.

Exceptions. Any exceptions to the terms and conditions or any additions, which bidder may wish to include in the RFP, should be made in writing and included in the form of an addendum to the applicable Section in the RFP.

CRDF Global Proprietary Information. Supplier agrees that all non-public information contained in this document and communicated verbally in reference to this RFP by CRDF Global shall be received for the sole discretion and purpose of enabling the supplier to submit an accurate response to this RFP. The information contained in this RFP and disclosed during the course of negotiations and communications are proprietary in nature and under no circumstances to be disclosed to a third party without prior written consent from CRDF Global.

Supplier Proprietary Information. Information contained in the response to this RFP will be considered proprietary in nature if marked "confidential" or "proprietary". Such marked documents will not be disclosed to third parties outside CRDF Global with the exception of retained consultants under contractual confidentiality agreements.