CRDF GLOBAL
REQUEST FOR PROPOSAL

Civilian Research and Development Foundation (CRDF) GLOBAL
REQUEST FOR PROPOSAL (RFP)

RFP-08-UA-2025

Experts in Cybersecurity, Digital Resilience and/or

Critical Infrastructure Protection

Submission Deadline: 31 Jul 2025, 6 pm Kyiv time

1 Introduction & Intent

CRDF Global is expanding our Cybersecurity and Digital Resilience (CS/DR) global technical services delivery team. This Request for Proposal (RFP) is one of our primary mechanisms for expanding our highly qualified and professional CS/DR Team specifically for our needs in Afro-Eurasia, with an initial focus on Europe and Northern Africa.

This RFP will result in a negotiated General Services Contract (hereafter “GSC”) with selected Vendors and SME(s) to be referred to as Partners. While the GSC is not a guarantee of work, GSC Partners can be engaged by CRDF Global staff with an abbreviated selection process. This allows CRDF Global to leverage Partners for strategic initiatives, proposal submissions, and programmatic responses to urgent timelines. Each Partner GSC will be structured to allow CRDF Global Agreement Officer(s) to issue Task Orders (TOs) to the Partner upon successful negotiation of scope and budget. The specific duration of the GSC can be negotiated following selection but is expected to be between 3 – 5 years. Further, each GSC establishes baseline pricing.

2 Cybersecurity and Digital Resilience (CS/DR) Services & Skills Sought

CRDF is seeking to build a cadre of companies and Subject Matter Experts (SMEs) who possess proven CS/DR capabilities and experience with whom we can build relationships to complement and supplement our teams. We are interested in those who offer the unique perspectives of the European/Eurasian regions and countries, an understanding of country and regional cultures, languages, governmental and legal structures (especially as it relates to cybersecurity), and the organic capabilities and capacities of the country and region being supported.

2.2 CS/DR Needs as Defined by the Systems Engineering Phase

Our opportunities address national as well as critical national Infrastructure (CNI) domain specific CS/DR needs. They span the entire program lifecycle, programmatically and technically. We may be responsible for the entire program – from inception through operations and sustainment – or we may be inserted into any phase, at any point. We develop our concepts, and align our internal capabilities, to the Systems Engineering Phases. We will draw upon these phases to describe and specify our requirements within each Task Order.

Phase	Definition
Concept & Architecture	Define mission/business needs, risk posture, and high-level cybersecurity and digital resilience requirements. This phase identifies stakeholders, use cases, threats, and initial system architecture aligned with mission objectives.
Solution Development	Translate conceptual architecture into detailed system and security designs.

Phase	Definition
& Detailed Design	Select security technologies, define secure data flows, and incorporate principles like Zero Trust, defense-in-depth, and resilience-by-design.
Implementation	Develop or acquire system components with integrated cybersecurity capabilities. Conduct secure coding, system hardening, and configuration in accordance with cybersecurity baselines and compliance frameworks.
Integration, Configuration & Test (IC&T)	Integrate subsystems and verify secure interoperability. Conduct security testing (e.g., penetration testing, red team assessments) and configure systems to meet cybersecurity policies and authorization requirements.
Operations & Monitoring	Deploy and operate the system within a secure environment. Continuously monitor for threats, vulnerabilities, and anomalies using SIEM, SOAR, and logging infrastructure, ensuring effective incident response.
Sustainment & Continuous Improvement	Maintain and enhance cybersecurity posture over time. Apply updates, patching, threat intelligence, vulnerability management, and lessons learned to ensure ongoing system resilience.
Procurement & Supply Chain Risk Management (SCRM)	Ensure secure sourcing, acquisition, and lifecycle management of systems and components. Integrate cybersecurity into contract requirements, vet vendors, and mitigate supply chain risks across dependencies.

2.3 Needs as Defined by Positional CS/DR Roles & Responsibilities

What follows is a broad set of positional roles and responsibilities that offer the respondent a clear idea of the type of efforts the CRDF CS/DR Team supports and our performance expectations of any Partner who joins us.

- **Solutions Architect:** The Solutions Architect is responsible for designing end-to-end cybersecurity and digital resilience solutions that align with organizational goals, ensuring the architecture integrates security controls, compliance requirements, and resilience strategies across systems and environments.
- **Systems Engineer:** The Systems Engineer leads the technical design, integration, and lifecycle management of secure systems, applying engineering principles to ensure cybersecurity and resilience are embedded in the system architecture, components, and operations from concept to decommission.
- **Engineer:** The Engineer implements, configures, and supports security technologies and controls, translating design specifications into functional system components that uphold integrity, availability, and confidentiality in dynamic operating environments.
- **Curriculum Developer:** The Curriculum Developer designs, develops, and updates training content and learning paths tailored to cybersecurity and resilience objectives, ensuring alignment with current threats, technologies, standards, and organizational skill gaps.
- **Trainer:** The Trainer delivers cybersecurity and digital resilience education and skills training to various

audiences, using practical methods to build technical competencies, awareness, and readiness for evolving threats and security practices.

- **Data Scientist:** The Data Scientist applies advanced analytics, machine learning, and statistical modeling to detect threats, optimize cybersecurity operations, and predict risks, supporting proactive digital resilience strategies with data-driven insights.
- **Data Modeler:** The Data Modeler designs logical and physical data models that support cybersecurity analytics, monitoring, and decision-making, ensuring data structures are optimized for security, consistency, integration, and analytical performance.
- **Data Analyst:** The Data Analyst collects, processes, and interprets cybersecurity-related data to generate actionable insights, identify anomalies, support incident response, and inform risk-based decision-making in support of organizational resilience.
- **OSINT Analyst**: The Cybersecurity OSINT Analyst is responsible for identifying, collecting, analyzing, and reporting on publicly available data sources to detect threats, vulnerabilities, and adversary activities relevant to an organization's digital assets. This role supports cybersecurity risk assessment, threat intelligence, incident response, and strategic decision-making. The analyst integrates findings across the systems engineering lifecycle to inform secure architecture design, proactive defense, and resilience strategies.

Appendices A, B and C, are shared to provide an increased understanding of the technical services sought and map the roles and responsibilities to each SE phase. They include exemplar activities, tasks and deliverables by role, and by SE phase.

- **Annex A – CS/DR Position Roles & Responsibilities** to Systems Engineering Phases with associated Activities, Tasks and Deliverables
- **Annex B – Systems Engineering Phases** to CS/DR Positions with associated Activities, Tasks and Deliverable
- **Annex C – CS/DR Labor Category** (LCAT) position descriptions with associated roles, responsibilities, experience and credentialling requirements

2.4 Support for CS/DR Currency, Capability & Capacity Building

CRDF also offers a variety of programs that support cybersecurity awareness, currency, system/operations hardening and advanced threat protection activities. These activities may include other requirements, such as secure event spaces, publishing, website presence, and media/communications campaigns and will be identified and defined within each TO. Activities include, but are not limited to;

- Vulnerability Disclosure Programs (VDP)
- Cyber Security Improvement Grants (CySigs)
- Cyber Range installation, operations and sustainment including scenario development & infrastructure upgrades
- Workshops and TTXs, in an on-line, in person, and hybrid format
  - OSINT Workshops
  - End-Point Hardening (Cyber Hygiene)
  - CTF/Hackathons/IRD

3 Contract for Services:

Following selection, CRDF Global will negotiate a General Services Contract (hereafter "GSC") with the selected SME(s).

While the GSC is not a guarantee of any work, the selected SME(s) on a GSC can be engaged by CRDF Global staff with an abbreviated selection process. This allows CRDF Global to potentially leverage the partnership with the SME for strategic initiatives, proposal submissions, and programmatic responses to urgent timelines. The GSC will be structured to allow CRDF Global Agreement Officer(s) to issue Task Orders upon successful negotiation of scope and budget.

The specific duration of the GSC can be negotiated following selection but is expected to be between 3 – 5 years.

The GSC would seek to negotiate and lock in elements of pricing and cost that are agreeable to both parties.

3.2 GSC Selection Requirements and Criteria:

The selection will be based on CRDF Global's evaluation of the Contractor's ability to meet CRDF Global's requirements described below, as well as factors such as competitive pricing, quality of proposal, past performance, and other intangible factors. CRDF Global reserves the right to accept or reject any and all proposals, and to negotiate terms of any subsequent agreements at its own discretion.

3.2.1 General Requirements:

- Proven experience
  - Conducting research/feasibility studies and development cybersecurity, information security or critical infrastructure protection fields in Afro-Eurasia. Experience in the Post- Soviet countries, USA and Europe in general are preferred.
  - Architecting, designing, implementing, integrating, testing, operating, modernizing and sustaining cybersecurity capabilities, especially in support of critical national infrastructure domains
  - Conducting CS/DR themed seminars/event/competitions/workshops.
  - Collaborating with government entities, private sector and civil society actors.
  - Working in donor-funded projects, especially for the U.S. government or multilateral institutions.
- Strong writing and speaking skills in English and the Task Order's designated country is required. There may be circumstances where translation services can be provided in support of niche needs.
- Excellent knowledge of Afro-Eurasian CS/DR challenges and environment especially as it relates to CNI in general, and then for the TO's country-region focus and/or domain of interest.

3.2.2 Selection Criteria

CRDF seeks to optimize the balance between cost, quality, and other performance-based criteria and will be awarded based on Best Value. We will use a multifactor system composed of four primary weighted factors:

- Technical Expertise – 35%: The bidder's technical capabilities and experience in delivering similar projects with an ability to be agile and innovative.
- Program Management – 15%: The bidder's ability to effectively integrate into the management team, methods and approach to include innovating, scheduling, budgeting, analyzing and reporting, collaborating, communicating and their ability to proactively identify and mitigate risk and exploit opportunity
- Past Performance – 20%: he bidder's track record of successful project completion and adherence to contract requirements.
- Cost – 30%: The overall cost of the project, including life-cycle costs.

These factors will be refined, if/as needed, with each Task Order.

3.3 Proposal Requirements

3.3.1 Each proposal must include:

- Statement of Interest and Technical Capabilities
  - Detailed description of the services offered in correlation with the RFP Subject Matter Expertise detailed under Scope and Tasks
  - List of recent experiences/samples working with the US Government and/or CRDF Global programming
  - Resumes (no more than 2 pages) of key contact(s)/project lead(s)
- Cost proposal (recommended, but optional)
  - Description of the pricing and cost factors (e.g. hourly rates (preferably), fixed-cost pricing on standard services, etc.), that the SME would be willing to negotiate under the General Services Contract.
- Completion & online submission of CRDF Global's Contractor Data Form: https://crdfglobal.formstack.com/forms/contractor_data_form

3.3.2 RFP Timetable:

CRDF Global reserves the right to make changes to the RFP Timetable without providing explicit notification ahead of time.

[July 03, 2025]:	RFP Posted & Live
[July 15, 2025]:	RFP Questions Due
[July 22, 2025]:	RFP Questions & Answers Released
[July 31, 2025]:	RFP Submission Due

3.3.3 Proposal Submission:

Proposals must be submitted as electronic documents in PDF, Word or Excel format. Proposals should be submitted to ofomin@crdfglobal.org & procurement@crdfglobal.org no later than: 31 July 2025, 6 pm Kyiv time. CRDF Global reserves the right to disqualify any proposal submitted after the submission deadline.
The subject line of the email must read:

RFP-08-UA-2025 _Proposal_Name of a submitter

3.3.4 Background:

Founded in 1995, CRDF Global is an independent nonprofit organization that promotes international scientific and technical collaboration through grants, technical resources, training, and services. Based in Arlington, Virginia with offices in the Eurasia and MENA regions, CRDF Global works with more than 40 countries in the Middle East, North Africa, Eurasia, and Asia. We specialize in bringing isolated scientific communities into the scientific mainstream through a variety of science engagement and capacity-building programs. CRDF Global encourages science cooperation between countries where official relations are strained.

More information is available at www.crdfglobal.org.

3.4 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, the 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 a bidder fails to object to any condition(s) incorporated herein, it shall mean that the bidder agrees with and will comply with the conditions set forth herein.
- **Exceptions.** Any exceptions to the terms and conditions or any additions, which the 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.

ANNEX A –

CRDF Cybersecurity & Digital Resilience Positions aligned to System Engineering Phases

Role	Systems Engineering Phase	Responsibilities	Activities	Tasks
Curriculum Developer	**Concept & Architecture**	Design training outlines that support emerging system security needs.	Identify key learning objectives from architecture outcomes.	Draft course modules on threat modeling and risk analysis.
	Solution Development & Detailed Design	Develop training content aligned with system design and secure coding practices.	Integrate SSDLC, DevSecOps, and ZTA principles into curriculum.	Design interactive lessons and assessments.
	Implementation	Update training content based on system deployment and configuration.	Incorporate real deployment scenarios.	Revise labs and procedures.
	Integration, Configuration & Test	Develop hands-on labs that simulate real-world attack and defense.	Use results from test events to enhance learning.	Incorporate red team scenarios into curriculum.
	Operations & Monitoring	Maintain training based on observed operations.	Gather feedback from analysts and engineers.	Update materials to reflect new threats.
	Sustainment & Continuous Improvement	Update learning content to reflect lessons learned.	Gather feedback, review incident data.	Refresh modules and assessments.
	Procurement & Supply Chain Risk Management	Develop training on supply chain risks and secure procurement.	Collaborate with SCRM teams.	Draft modules on supplier risk.
Data Analyst	**Concept & Architecture**	Support data requirements analysis to understand mission-driven data needs.	Gather metadata and work with SMEs on expected data behaviors.	Document data definitions and dependencies.
	Solution Development & Detailed Design	Support development of dashboards and data views for system monitoring.	Map data flows to KPIs and risk metrics.	Design visualizations, prepare user guides.
	Implementation	Monitor initial data behavior, flag anomalies.	Analyze logs, user behavior.	Create reports, suggest adjustments.
	Integration, Configuration & Test	Analyze test data for trends and weaknesses.	Run post-test analytics, correlate findings.	Generate dashboards of system behavior under attack.
	Operations & Monitoring	Analyze operational data for patterns and risk.	Develop KPIs for threat and risk.	Generate weekly reports, identify outliers.
	Sustainment & Continuous Improvement	Generate insights to improve defenses and resilience.	Analyze long-term trends.	Correlate incidents with system changes.
	Procurement & Supply Chain Risk Management	Monitor procurement data for suspicious patterns.	Review supplier transactions.	Generate compliance reports.
Data Modeler	**Concept & Architecture**	Define logical data architecture aligned with security and resilience.	Work with architects to map critical data flows.	Develop entity-relationship diagrams and data flow diagrams.
	Solution Development & Detailed Design	Design robust data schemas supporting security, privacy, and analytics.	Create logical and physical data models, enforce classification rules.	Document model assumptions, validate with use cases.
	Implementation	Implement data structures in operational databases.	Work with DBAs to enforce design.	Build tables, validate against data sources.
	Integration, Configuration & Test	Ensure test datasets support validation of models and data pipelines.	Simulate data breaches, verify data tagging.	Create synthetic data, align with test goals.
	Operations & Monitoring	Optimize models for system performance under load.	Monitor query performance, adjust structures.	Tune database indexes.
	Sustainment & Continuous Improvement	Maintain scalable and secure data design.	Support data lifecycle management.	Archive and reorganize data flows.
	Procurement & Supply Chain Risk Management	Design data flows to track supplier lineage and risk.	Model supplier metadata.	Map supplier relationships.
Data Scientist	**Concept & Architecture**	Model potential data-driven threat scenarios and anomaly detection baselines.	Conduct exploratory data analysis on anticipated data types.	Create prototype analytics use cases.
	Solution Development & Detailed Design	Develop and test security analytics models using system design inputs.	Build detection models, simulate adversarial behavior.	Select algorithms, test with sample data.
	Implementation	Validate models with operational data post-deployment.	Test in staging environments.	Run anomaly detection, tune parameters.
	Integration, Configuration & Test	Verify analytic models using test data under varied threat conditions.	Apply red/blue data to detection models.	Score model accuracy, adjust for false positives.
	Operations & Monitoring	Continuously improve models using live data.	Monitor for model drift, retrain models.	Apply real-time anomaly scoring.
	Sustainment & Continuous Improvement	Refine models with new data and attack techniques.	Incorporate emerging threats.	Retrain models.
	Procurement & Supply Chain Risk Management	Build models to detect supply chain anomalies.	Analyze sourcing and logistics data.	Develop risk scoring models.

Role	Systems Engineering Phase	Responsibilities	Activities	Tasks
Engineer	**Concept & Architecture**	Support engineering analysis of security needs and risk.	Participate in technical workshops and architecture sessions.	Assist in threat modeling and requirements gathering.
	Solution Development & Detailed Design	Design secure subsystems, select components, and evaluate vulnerabilities.	Code secure modules, use threat libraries, apply encryption.	Conduct code analysis, design secure communication protocols.
	Implementation	Deploy and configure components securely, test installations.	Apply hardened settings, enable logging.	Script installs, test modules in sandbox.
	Integration, Configuration & Test	Perform component integration, test secure interactions.	Run red/blue team scenarios, tune detection mechanisms.	Configure test environments, patch vulnerabilities.
	Operations & Monitoring	Respond to alerts, monitor logs, and remediate issues.	Tune detection rules, escalate threats.	Run scripts, respond to anomalies.
	Sustainment & Continuous Improvement	Continuously improve component security.	Patch vulnerabilities, improve scripts.	Conduct mini-assessments.
	Procurement & Supply Chain Risk Management	Test supplier components for vulnerabilities.	Perform static analysis, firmware checks.	Write supplier validation test plans.
Solutions Architect	**Concept & Architecture**	Define high-level cybersecurity architecture and resilience concepts aligned with mission objectives.	Conduct threat modeling, perform BIA, and draft CONOPS.	Develop architecture decision matrix, lead security posture definition.
	Solution Development & Detailed Design	Define detailed security design incorporating Zero Trust, SSDLC, and layered defense.	Design secure system and data flows, select technologies.	Develop solution blueprints, participate in design reviews.
	Implementation	Ensure implementation aligns with security architecture and policy.	Provide oversight to engineers, verify integration plans.	Approve architecture deviations, resolve security conflicts.
	Integration, Configuration & Test	Oversee validation of architecture via integration testing and red team exercises.	Review test plans, ensure traceability to design.	Support cyber range scenarios, approve test coverage.
	Operations & Monitoring	Ensure operational security posture adheres to architectural intent.	Review ongoing security telemetry and design drift.	Conduct regular architecture reviews.
	Sustainment & Continuous Improvement	Evolve system architecture in response to changing threats and tech.	Review incident data, plan architecture upgrades.	Propose architectural improvements.
	Procurement & Supply Chain Risk Management	Define secure procurement requirements and architecture criteria.	Evaluate third-party architecture risk.	Write architecture-based procurement specs.
Systems Engineer	**Concept & Architecture**	Translate mission needs into preliminary security requirements and system concepts.	Analyze system requirements, support CONOPS development.	Perform gap analysis, assist in risk assessment.
	Solution Development & Detailed Design	Develop and validate security requirements and system interfaces.	Model system interactions, align with SSDLC practices.	Create security requirement traceability, support vendor selection.
	Implementation	Lead secure deployment of components and systems.	Coordinate configurations, validate dependencies.	Verify software builds, manage technical documentation.
	Integration, Configuration & Test	Coordinate system-level testing, validate interfaces and security posture.	Manage vulnerability scanning, penetration testing.	Conduct functional security tests, support A&A process.
	Operations & Monitoring	Monitor and manage secure system operations and logging.	Oversee SIEM operations, manage configuration baselines.	Automate patching, verify endpoint configurations.
	Sustainment & Continuous Improvement	Apply updates and upgrades without disrupting operations.	Manage lifecycle of controls and configurations.	Validate updates, rollback if needed.
	Procurement & Supply Chain Risk Management	Assess supplier compliance with cybersecurity controls.	Conduct security evaluations, audits.	Coordinate SCRM assessments.
Trainer	**Concept & Architecture**	Advise on initial training needs aligned to early system security posture.	Coordinate with architects and engineers to scope knowledge gaps.	Recommend pre-design training programs.
	Solution Development & Detailed Design	Deliver instruction on security architecture and SSDLC principles.	Prepare technical labs, conduct live demonstrations.	Facilitate workshops, assess trainee understanding.
	Implementation	Train operations teams on secure implementation practices.	Deliver hands-on configuration training.	Oversee labs, administer tests.
	Integration, Configuration & Test	Facilitate technical test training for operators and response teams.	Conduct live integration test exercises.	Simulate attacks, lead response drills.
	Operations & Monitoring	Train staff on monitoring tools and incident response.	Lead drills, monitor tool proficiency.	Administer simulations, evaluate readiness.
	Sustainment & Continuous Improvement	Provide recurring training on new tools, techniques.	Train on new versions and threat types.	Prepare quick-reference guides.
	Procurement & Supply Chain Risk Management	Deliver training on secure procurement and supplier vetting.	Simulate supplier risk scenarios.	Facilitate interactive training.

Role	Systems Engineering Phase	Responsibilities	Activities	Tasks
OSINT Analyst	**Concept & Architecture**	▪ Identify emerging threats and geopolitical risks ▪ Support risk modeling and mission needs assessment	▪ Collect strategic threat intelligence ▪ Map threat actors and TTPs ▪ Conduct deep/dark web reconnaissance	▪ Create OSINT-based threat landscape reports ▪ Feed data into threat models and CONOPS ▪ Support BIA with contextual indicators
	Solution Development & Detailed Design	▪ Supply threat intelligence for secure system design ▪ Prioritize security controls based on OSINT	▪ Perform vulnerability intelligence gathering ▪ Correlate threats to design weaknesses	▪ Deliver design-phase intel briefs ▪ Annotate architecture with probable threats ▪ Contribute to adversary emulation
	Implementation	▪ Monitor for signs of supply chain or data leakage ▪ Report campaigns targeting implementations	▪ Track chatter from threat groups ▪ Scan code repositories and forums for leaks	▪ Generate OSINT alerts ▪ Collaborate with DevSecOps
	Integration, Configuration & Test	▪ Provide intel for cyber range scenarios ▪ Validate configurations against attacks	▪ Monitor for exploits of CVEs or misconfigs ▪ Inject threat actor behavior into testing	▪ Author threat scenarios ▪ Debrief teams with intel findings
	Operations & Monitoring	▪ Provide continuous monitoring ▪ Correlate events with OSINT indicators	▪ Aggregate data from social media, forums, paste sites ▪ Perform attribution analysis	▪ Issue intel bulletins ▪ Flag IOCs to SOC/IR teams
	Sustainment & Continuous Improvement	▪ Re-assess threat environment ▪ Update risk and resilience profiles	▪ Monitor threat actor behavior ▪ Perform recurring OSINT scans	▪ Deliver quarterly threat reports ▪ Update threat models
	Procurement & Supply Chain Risk Management	▪ Assess third-party cyber posture ▪ Monitor public exposure of suppliers	▪ Search for vendor leaks and security incidents ▪ Analyze geopolitical supply risks	▪ Produce supply chain threat assessments ▪ Inform procurement decisions

ANNEX B –

Systems Engineering Phases with mapped CRDF Cybersecurity & Digital Resilience Positions

Systems Engineering Phase	Role	Responsibilities	Activities	Tasks
Concept & Architecture	**Solutions Architect**	Define high-level cybersecurity architecture and resilience concepts aligned with mission objectives.	Conduct threat modeling, perform BIA, and draft CONOPS.	Develop architecture decision matrix, lead security posture definition.
	Systems Engineer	Translate mission needs into preliminary security requirements and system concepts.	Analyze system requirements, support CONOPS development.	Perform gap analysis, assist in risk assessment.
	Engineer	Support engineering analysis of security needs and risk.	Participate in technical workshops and architecture sessions.	Assist in threat modeling and requirements gathering.
	Curriculum Developer	Design training outlines that support emerging system security needs.	Identify key learning objectives from architecture outcomes.	Draft course modules on threat modeling and risk analysis.
	Trainer	Advise on initial training needs aligned to early system security posture.	Coordinate with architects and engineers to scope knowledge gaps.	Recommend pre-design training programs.
	Data Scientist	Model potential data-driven threat scenarios and anomaly detection baselines.	Conduct exploratory data analysis on anticipated data types.	Create prototype analytics use cases.
	Data Modeler	Define logical data architecture aligned with security and resilience.	Work with architects to map critical data flows.	Develop entity-relationship diagrams and data flow diagrams.
	Data Analyst	Support data requirements analysis to understand mission-driven data needs.	Gather metadata and work with SMEs on expected data behaviors.	Document data definitions and dependencies.
	OSINT Analyst	Inform initial risk posture and high-level architecture design; Identify emerging threats and geopolitical risks; Support risk modeling and mission needs assessment	- Collect strategic threat intelligence; Map threat actors and TTPs; Conduct deep/dark web reconnaissance	Create OSINT-based threat landscape reports; Feed data into threat models and CONOPS; Support BIA with contextual indicators
Solution Development & Detailed Design	**Solutions Architect**	Define detailed security design incorporating Zero Trust, SSDLC, and layered defense.	Design secure system and data flows, select technologies.	Develop solution blueprints, participate in design reviews.
	Systems Engineer	Develop and validate security requirements and system interfaces.	Model system interactions, align with SSDLC practices.	Create security requirement traceability, support vendor selection.
	Engineer	Design secure subsystems, select components, and evaluate vulnerabilities.	Code secure modules, use threat libraries, apply encryption.	Conduct code analysis, design secure communication protocols.
	Curriculum Developer	Develop training content aligned with system design and secure coding practices.	Integrate SSDLC, DevSecOps, and ZTA principles into curriculum.	Design interactive lessons and assessments.
	Trainer	Deliver instruction on security architecture and SSDLC principles.	Prepare technical labs, conduct live demonstrations.	Facilitate workshops, assess trainee understanding.
	Data Scientist	Develop and test security analytics models using system design inputs.	Build detection models, simulate adversarial behavior.	Select algorithms, test with sample data.
	Data Modeler	Design robust data schemas supporting security, privacy, and analytics.	Create logical and physical data models, enforce classification rules.	Document model assumptions, validate with use cases.
	Data Analyst	Support development of dashboards and data views for system monitoring.	Map data flows to KPIs and risk metrics.	Design visualizations, prepare user guides.
	OSINT Analyst	Align design with real-world threat vectors and adversarial tactics; Supply threat intelligence for secure system design; Prioritize security controls based on OSINT	Perform vulnerability intelligence gathering; Correlate threats to design weaknesses	Deliver design-phase intel briefs; Annotate architecture with probable threats; Contribute to adversary emulation

Systems Engineering Phase	Role	Responsibilities	Activities	Tasks
Implementation	**Solutions Architect**	Ensure implementation aligns with security architecture and policy.	Provide oversight to engineers, verify integration plans.	Approve architecture deviations, resolve security conflicts.
	Systems Engineer	Lead secure deployment of components and systems.	Coordinate configurations, validate dependencies.	Verify software builds, manage technical documentation.
	Engineer	Deploy and configure components securely, test installations.	Apply hardened settings, enable logging.	Script installs, test modules in sandbox.
	Curriculum Developer	Update training content based on system deployment and configuration.	Incorporate real deployment scenarios.	Revise labs and procedures.
	Trainer	Train operations teams on secure implementation practices.	Deliver hands-on configuration training.	Oversee labs, administer tests.
	Data Scientist	Validate models with operational data post-deployment.	Test in staging environments.	Run anomaly detection, tune parameters.
	Data Modeler	Implement data structures in operational databases.	Work with DBAs to enforce design.	Build tables, validate against data sources.
	Data Analyst	Monitor initial data behavior, flag anomalies.	Analyze logs, user behavior.	Create reports, suggest adjustments.
	OSINT Analyst	Detect early indicators of compromise or risks during implementation; Monitor for signs of supply chain or data leakage; Report campaigns targeting implementations	Track chatter from threat groups; Scan code repositories and forums for leaks	Generate OSINT alerts; Collaborate with DevSecOps
Integration, Configuration & Test	**Solutions Architect**	Oversee validation of architecture via integration testing and red team exercises.	Review test plans, ensure traceability to design.	Support cyber range scenarios, approve test coverage.
	Systems Engineer	Coordinate system-level testing, validate interfaces and security posture.	Manage vulnerability scanning, penetration testing.	Conduct functional security tests, support A&A process.
	Engineer	Perform component integration, test secure interactions.	Run red/blue team scenarios, tune detection mechanisms.	Configure test environments, patch vulnerabilities.
	Curriculum Developer	Develop hands-on labs that simulate real-world attack and defense.	Use results from test events to enhance learning.	Incorporate red team scenarios into curriculum.
	Trainer	Facilitate technical test training for operators and response teams.	Conduct live integration test exercises.	Simulate attacks, lead response drills.
	Data Scientist	Verify analytic models using test data under varied threat conditions.	Apply red/blue data to detection models.	Score model accuracy, adjust for false positives.
	Data Modeler	Ensure test datasets support validation of models and data pipelines.	Simulate data breaches, verify data tagging.	Create synthetic data, align with test goals.
	Data Analyst	Analyze test data for trends and weaknesses.	Run post-test analytics, correlate findings.	Generate dashboards of system behavior under attack.
	OSINT Analyst	Support adversary emulation and red team exercises; Provide intel for cyber range scenarios; Validate configurations against attacks	Monitor for exploits of CVEs or misconfigs; Inject threat actor behavior into testing	Author threat scenarios; Debrief teams with intel findings
Operations & Monitoring	**Solutions Architect**	Ensure operational security posture adheres to architectural intent.	Review ongoing security telemetry and design drift.	Conduct regular architecture reviews.
	Systems Engineer	Monitor and manage secure system operations and logging.	Oversee SIEM operations, manage configuration baselines.	Automate patching, verify endpoint configurations.
	Engineer	Respond to alerts, monitor logs, and remediate issues.	Tune detection rules, escalate threats.	Run scripts, respond to anomalies.
	Curriculum Developer	Maintain training based on observed operations.	Gather feedback from analysts and engineers.	Update materials to reflect new threats.
	Trainer	Train staff on monitoring tools and incident response.	Lead drills, monitor tool proficiency.	Administer simulations, evaluate readiness.
	Data Scientist	Continuously improve models using live data.	Monitor for model drift, retrain models.	Apply real-time anomaly scoring.
	Data Modeler	Optimize models for system performance under load.	Monitor query performance, adjust structures.	Tune database indexes.
	Data Analyst	Analyze operational data for patterns and risk.	Develop KPIs for threat and risk.	Generate weekly reports, identify outliers.
	OSINT Analyst	Enable proactive defense and threat hunting; Provide continuous monitoring; Correlate events with OSINT indicators	Aggregate data from social media, forums, paste sites; Perform attribution analysis	Issue intel bulletins; Flag IOCs to SOC/IR teams

Systems Engineering Phase	Role	Responsibilities	Activities	Tasks
Sustainment & Continuous Improvement	**Solutions Architect**	Evolve system architecture in response to changing threats and tech.	Review incident data, plan architecture upgrades.	Propose architectural improvements.
	Systems Engineer	Apply updates and upgrades without disrupting operations.	Manage lifecycle of controls and configurations.	Validate updates, rollback if needed.
	Engineer	Continuously improve component security.	Patch vulnerabilities, improve scripts.	Conduct mini-assessments.
	Curriculum Developer	Update learning content to reflect lessons learned.	Gather feedback, review incident data.	Refresh modules and assessments.
	Trainer	Provide recurring training on new tools, techniques.	Train on new versions and threat types.	Prepare quick-reference guides.
	Data Scientist	Refine models with new data and attack techniques.	Incorporate emerging threats.	Retrain models.
	Data Modeler	Maintain scalable and secure data design.	Support data lifecycle management.	Archive and reorganize data flows.
	Data Analyst	Generate insights to improve defenses and resilience.	Analyze long-term trends.	Correlate incidents with system changes.
	OSINT Analyst	Assess evolving threats to deployed systems; Re-assess threat environment; Update risk and resilience profiles	Monitor threat actor behavior; Perform recurring OSINT scans	Deliver quarterly threat reports; Update threat models
Procurement & Supply Chain Risk Management	**Solutions Architect**	Define secure procurement requirements and architecture criteria.	Evaluate third-party architecture risk.	Write architecture-based procurement specs.
	Systems Engineer	Assess supplier compliance with cybersecurity controls.	Conduct security evaluations, audits.	Coordinate SCRM assessments.
	Engineer	Test supplier components for vulnerabilities.	Perform static analysis, firmware checks.	Write supplier validation test plans.
	Curriculum Developer	Develop training on supply chain risks and secure procurement.	Collaborate with SCRM teams.	Draft modules on supplier risk.
	Trainer	Deliver training on secure procurement and supplier vetting.	Simulate supplier risk scenarios.	Facilitate interactive training.
	Data Scientist	Build models to detect supply chain anomalies.	Analyze sourcing and logistics data.	Develop risk scoring models.
	Data Modeler	Design data flows to track supplier lineage and risk.	Model supplier metadata.	Map supplier relationships.
	Data Analyst	Monitor procurement data for suspicious patterns.	Review supplier transactions.	Generate compliance reports.
	OSINT Analyst	Evaluate vendor and supply chain threats; Assess third-party cyber posture; Monitor public exposure of suppliers	Search for vendor leaks and security incidents; Analyze geopolitical supply risks	Produce supply chain threat assessments; Inform procurement decisions

ANNEX C –

CRDF Labor Category (LCAT) Position Descriptions (PDs) with associated roles, responsibilities, experience and credentialling requirements

Job Family	Role	Responsibilities	NIST Requirements	ENISA Requirements	Activities	Tasks	Deliverables	Experience Requirements	Certification Requirements
Cyber Risk Management	Cyber Risk Analyst	Performs risk assessments and mitigation planning.	SP 800-30; RMF Step 3-5	ENISA Risk Management Guide	Risk identification, analysis, mitigation	Conduct assessments, document risks, track mitigation plans	Risk assessment reports, risk registers, mitigation plans	3-5 years in risk management, governance, or compliance roles	CRISC, CISSP, or FAIR
Cyber Risk Management	Third-Party Risk Analyst	Evaluates and manages cybersecurity risks posed by external vendors and partners.	SP 800-161; SP 800-37	ENISA Supply Chain Security Guide	Vendor risk assessments, contract reviews, continuous monitoring	Perform third-party assessments, document findings, track remediation	Vendor risk reports, risk register updates, mitigation follow-ups	3+ years in vendor management, procurement, or cyber risk analysis	CISA, CRISC, or Vendor Risk Management certs
Cybersecurity Architecture	Security Solutions Architect	Designs secure systems and architectures.	SP 800-160; SP 800-53 SA family	ENISA Secure Architecture Guidelines	Security design reviews, threat modeling, system architecture	Develop security blueprints, assess architecture, define controls	Security architecture diagrams, threat models, security control designs	8+ years in cybersecurity architecture or enterprise architecture	CISSP-ISSAP, SABSA, or AWS Certified Security – Specialty
Cybersecurity Architecture	Cloud Security Architect	Designs and implements secure cloud-based architectures and services.	SP 800-210; SP 800-144	ENISA Cloud Security for SMEs	Cloud architecture review, control implementation, vendor risk assessment	Define cloud security controls, assess provider risk, design secure cloud environments	Cloud security plans, provider risk assessments, architecture diagrams	5+ years in cloud engineering or security design	CCSP, AWS/Azure/GCP Security Certs
Cybersecurity Engineering	Cybersecurity Engineer	Implements and maintains security technologies and systems.	SP 800-160; SP 800-53	ENISA Security Controls Implementation Guide	System hardening, tool deployment, configuration management	Install and configure security tools, automate security checks, patch systems	System configurations, security baselines, implementation reports	▪ Mid-Range: 4+ years in system security implementation or network engineering ▪ Senior: 7+ years	CISSP, CompTIA Security+, GSEC
Cybersecurity Governance	Cybersecurity Policy Analyst	Develops and maintains cybersecurity policies, standards, and guidelines.	SP 800-53 PM family; RMF Step 1-2	ENISA Guidelines on Security Policy	Policy development, compliance reviews, stakeholder engagement	Draft policies, conduct policy gap analysis, update documentation	Cybersecurity policy documents, policy gap analysis reports, compliance matrices	3-5 years in policy or governance roles; knowledge of regulatory frameworks (e.g., NIST, ISO)	CISSP, CISM, or CGEIT
Cybersecurity Governance	Cybersecurity Compliance Manager	Oversees adherence to cybersecurity policies, standards, and regulatory requirements.	SP 800-53; SP 800-171	ENISA Compliance Monitoring Guidelines	Compliance audits, reporting, remediation planning	Conduct control assessments, compile compliance evidence, manage corrective action plans	Audit reports, compliance dashboards, corrective action tracking logs	5+ years in compliance or audit roles in regulated industries	CISA, CISM, or ISO 27001 Lead Auditor
Cybersecurity Training & Awareness	Cybersecurity Training Specialist	Develops and delivers cybersecurity training programs.	NICE Framework; NIST SP 800-50	ENISA Cybersecurity Skills Framework	Curriculum design, training delivery, assessment	Create training content, conduct sessions, evaluate effectiveness	Training materials, attendance logs, evaluation reports	2+ years in cybersecurity education or instructional design	CompTIA CTT+, SANS SEC401
Cybersecurity Training & Awareness	Security Awareness Program Manager	Leads the organization's cybersecurity awareness and culture initiatives.	SP 800-50; NICE Framework	ENISA Cyber Awareness Campaign Guide	Awareness campaigns, phishing simulations, behavioral analytics	Plan campaigns, run simulations, analyze training outcomes	Campaign schedules, simulation results, awareness reports	3-5 years running awareness programs or corporate communications	CISSP, SANS Security Awareness Professional
Security Operations	Security Operations Center (SOC) Analyst	Monitors security events and responds to incidents.	SP 800-61; SP 800-137	ENISA CSIRT Services Framework	Alert monitoring, threat analysis, incident response	Analyze logs, escalate threats, document incidents	Incident reports, threat analysis reports, SOC dashboards	3+ years in security operations or incident response roles	CompTIA Security+, CySA+, or GCIA
Security Operations	Threat Intelligence Analyst	Analyzes threat data to identify adversary behaviors and indicators of compromise.	SP 800-150; NIST Cyber Threat Intelligence	ENISA Threat Landscape Reports	Threat analysis, IOC tracking, intelligence sharing	Correlate threat data, produce intel reports, brief stakeholders	Threat intelligence reports, IOC databases, briefings	3+ years in threat intel or cyber defense analysis	GCTI, CEH, or Threat Intelligence Analyst certs

Job Family	Role	Responsibilities	NIST Requirements	ENISA Requirements	Activities	Tasks	Deliverables	Experience Requirements	Certification Requirements
Cybersecurity Intelligence & Threat Analysis	OSINT Analyst	Conduct open-source research to detect cyber threats, disinformation, and criminal activity; Support threat modeling, situational awareness, and decision-making; Collaborate with CTI, SOC, and IR teams; Monitor social media, forums, paste sites, surface/deep/dark web for emerging risks; Correlate data with threat intelligence frameworks.	▪ NIST SP 800-61 Rev. 2 – Incident Handling Guide ▪ NIST SP 800-53 Rev. 5 – Controls: AU-6, IR-4, RA-5, SI-4 ▪ NIST SP 800-150 – Guide to Cyber Threat Information Sharing ▪ NIST SP 800-160 Vol. 1 – Threat analysis in system security engineering ▪ RMF Tasks: RM-1 through RM-3	▪ ENISA Threat Landscape (ETL) – OSINT as part of strategic and operational threat intelligence ▪ ENISA Cybersecurity Skills Framework: Role: “Threat Intelligence Analyst”, Work Group 2.4 ▪ ENISA Guidelines on Threat Intelligence Sharing and Situational Awareness	▪ Monitor OSINT platforms for emerging cyber threats ▪ Perform threat actor and campaign profiling ▪ Extract IOCs and behavioral patterns ▪ Maintain awareness of geopolitical events impacting cyber risk ▪ Use automation tools and AI for data aggregation and analysis	▪ Curate intelligence feeds from open sources ▪ Tag, classify, and enrich findings with contextual metadata ▪ Write threat briefings and situational reports ▪ Support red/blue team operations with environmental reconnaissance ▪ Escalate validated threats to IR and SOC teams ▪ Monitor OSINT platforms for emerging cyber threats ▪ Perform threat actor and campaign profiling ▪ Extract IOCs and behavioral patterns ▪ Maintain awareness of geopolitical events impacting cyber risk ▪ Use automation tools and AI for data aggregation and analysis	▪ Daily/Weekly Threat Intelligence Reports ▪ OSINT Enrichment Profiles ▪ Threat Actor Dossiers ▪ Risk Indicators Dashboard ▪ IOC/IOA Watchlists ▪ Strategic Briefings for Executives or Risk Committees	▪ Entry-Level: 0–2 years of experience in intelligence analysis, cybersecurity, or geopolitics ▪ Mid-Level: 3–5 years in OSINT, CTI, or cyber defense roles ▪ Senior: 6+ years with expertise in adversary behavior analysis, geopolitical risk, and SIGINT/OSINT fusion	▪ ENISA Threat Landscape (ETL) – OSINT as part of strategic and operational threat intelligence ▪ ENISA Cybersecurity Skills Framework: Role: “Threat Intelligence Analyst”, Work Group 2.4 ▪ ENISA Guidelines on Threat Intelligence Sharing and Situational Awareness