Request for Information (RFI)

Establishment and Operation of the National Cybersecurity Academy of Jordan (NCAJ)

RFI Reference: NCAJ-RFI-2025-01
Issuing Body: National Cybersecurity Center (NCSC),
Hashemite Kingdom of Jordan
Release Date: July 27, 2025
Response Deadline: September 09, 2025.

Preamble

This Request for Information (RFI), along with the accompanying Proposed Business Model (BM), is issued solely for exploratory and informational purposes. The objective is to better understand the global and regional market landscape, identify potential solutions and delivery models, and collect feedback to refine the strategic direction for the establishment of the National Cybersecurity Academy of Jordan (NCAJ).

This RFI is not a Request for Proposal (RFP), nor should it be interpreted as an Expression of Interest (EOI). Responding to this RFI is entirely voluntary and does not imply any form of prequalification or future advantage. Furthermore, this RFI does not create any obligation, financial commitment, or contractual relationship on the part of the National Cybersecurity Center (NCSC) of Jordan or any Jordanian governmental entity.

The responses and insights gathered will serve exclusively to shape the development of a potential future RFP, planned for release in Q4 2025. All submissions will be treated as confidential and used only for internal planning and decision-making purposes.

Participants are encouraged to share their perspectives, proposed approaches, and potential alternatives to enhance the proposed business model and implementation strategy. However, participation in this RFI process will not influence or guarantee involvement in any subsequent procurement or partnership process.

Executive Summary

The National Cybersecurity Center (NCSC) of Jordan is issuing a Request for Information (RFI) to all qualified local and international training institutions, certification organizations, consortia, and educational entities to provide responses regarding the design, establishment, and functional capabilities of the National Cybersecurity Academy of Jordan (NCAJ). This ties directly to the overall objectives of Jordan's national digital transformation program, and the aim of positioning Jordan as a regional cybersecurity leader.

1. Purpose of the RFI:
   The National Cybersecurity Center (NCSC) of Jordan is inviting responses, feedback, and proposals from qualified local and global training organizations, certification bodies, consortia, and strategic education entities in the design, establishment, and operation of the National Cybersecurity Academy of Jordan (NCAJ). This RFI intends to:
   - Collect information about the executive bodies' capabilities, experience, and initial proposals.
   - Understand market interest to deliver on the NCAJ's objectives.
   - Collect feedback and alternative proposals to enhance, and ultimately improve the proposed business model.
   - Help develop a detailed Request for Proposal (RFP) that will be released in Q4 2025. The potential RFP, if released, will be in line with the Government Procurement By-law of Jordan.

   This RFI does not form a commitment to release an RFP or award any contract.

2. Background
   Jordan is establishing a national initiative for the NCAJ to become a premier regional hub for cybersecurity and AI-based cyber training, education, and innovation. A comprehensive business model has been developed to provide a roadmap for implementation of this initiative. The proposed model includes:
   - A dual-track training ecosystem of foundational and AI driven Cybersecurity.
   - A hybrid structure that includes non-profit and for-profit.
   - A national advisory board with governance from a global training organization and a leading Jordanian university managing the operations of the hub.

   A growth model with three phases:
   - Phase 1: Foundational cybersecurity training and integration of AI.
   - Phase 2: National hub-and-spoke model expansion.
   - Phase 3: International accreditation and knowledge transfer.

   This RFI document and the accompanying *"Proposed Business Model for the National Cybersecurity Academy of Jordan (NCAJ)"* should be read together as a single, integrated document to provide a complete understanding of the initiative.

3. RFI Objectives
   NCSC is interested in responses that:
   - Identify the responders' capability and experience in providing foundational and AI-driven cybersecurity education and certification at scale.
   - Propose a viable model to safely implement and sustain the NCAJ based on the business model provided.
   - Provide different governance/operational/business or technical models if felt to be a better option.

- Identify the risks, challenges and/or opportunities related to the proposed NCAJ framework.
- Identify the structure for long term partnership/sustainability, revenue sharing and governance.
- Identify potential global/regional partners, certifications or technologies the responder would use.

4. Instructions to Respondents

4.1 Eligibility

This RFI is open to:

- Individual local and international training/certification bodies.
- Consortiums involving training entities, institutions of higher education, and/or technology businesses.
- Organizations that can demonstrate expertise in cybersecurity education, certifications, and academic-level programming at scale.

4.2 Submission Format

Respondents should include:

- Cover Letter: A brief summary of professional interest and key contact information,
- Organizational Profile: The official name and legal structure of the organization, relevant past history, certifications, and relevant experience,
- Proposed Approach: A detailed response specifically related to Section 3 above,
- Alternative Solutions (Optional): If respondents are proposing alternatives to the model in this RFI, they should clearly state the alternatives along with rationale, comparative value, and implementation considerations,
- Annexes: (Optional) Brochures, case studies, white papers, testimonials etc.

4.3 Evaluation Criteria:

Taking the requirements, metrics and indicators listed in the appendices into consideration wherever possible, responses will be assessed against - but not limited to - the following criteria:

- Relevance and detail of relevant past experience in the delivery of foundational and AI-enabled cyber security education and certification at scale.
- The technical robustness and scale of the proposed implementation approach.
- The innovation and proposed value of the alternatives (if proposed).

- Risk mitigation strategies.
- Proven ability to create strong public-private-academic partnerships.

4.4 Submission Deadline:

Responses can be submitted via email at NCAJ@ncsc.jo and must be received no later than 09 September 2025. Late submissions will not be considered.

4.5 Confidentiality

Submissions will be treated as confidential and used only for the purpose of helping to shape the future RFP.

5 Next Steps

- The NCSC may follow up with clarification meetings or requests for additional information before the specified submission deadline.
- In Q4 of 2025, based on the information received, a formal RFP will be released.
- We expect to select a vendor and sign the contract in Q1-Q2 of 2026.

6 Contact Information

If you have any questions related to this RFI, please contact:
Email: NCAJ@ncsc.jo
Subject Line: RFI Inquiry – NCAJ-RFI-2025-01

If possible, please confirm the receipt of this RFI and your intention to respond no later than 09 September 2025. We look forward to your contribution to shape the future of cybersecurity in Jordan and the MENA region.

Appendices – National Cybersecurity Academy of Jordan

Appendix A – Evaluation Framework

Responses to the RFI will be assessed based on the following weighted criteria:

- Relevant experience in one or more domains of cybersecurity education and certifications (25%)
- Technical integrity and overall scalability of approach (30%)
- Value of the proposed innovation, and value of alternatives presented (15%)
- Risk mitigation strategies (10%)
- Aspects of public-private-academic partnerships where they may arise (20%)

Appendix B – Alignment with Global Frameworks

Alignment with globally recognized frameworks such as, but not limited to:

- NIST NICE Framework
- ISO/IEC 27001
- MITRE ATT&CK Framework
- ENISA for EU cybersecurity capacity building guidelines.

Appendix C – Governance Structure and Responsibilities

Governance Roles:

- NCSC: governance; Strategic Alignment; Funding Requests.
- Global Partner: Manage curriculum, provide trainers; certification authority.
- Local University: Daily administration; provisions of local trainers; provisions of service for learners.

Decision Making: A National Advisory Board will provide oversight for policy, partnerships and compliance.

Appendix D – Preliminary Risk Management

Risk Categories:

- Strategic: Poor partner performance, geopolitical restrictions
- Operational: System downtime, trainer turnover
- Financial: Funding delayed and not realizing expected ROI
- Cyber: Attacks on training services and customer data being leaked

Recovery strategies consist of staged rollout, standby trainers, legal contracts, and monitoring.

Appendix E – Training Quality Assurance

The following QA processes are recommended:

- Trainers need to hold advanced accreditation.
- Course should be rated through formative assessments and end learner feedback.
- Certification pass rates should be tracked and published on an annual basis.
- Content should be reviewed by industry every 12–18 months.

Appendix F – Financial Model Overview

Financial Estimates:

- Upfront funding
- Operational cost per year
- Funding sources: training, licensing, and public-private partnerships

A tiered pricing structure and international programs will assist in sustaining long-term operations.

Appendix G – Strategic Outcomes

Outputs linked to national goals, include:

- Reduction in the national cyber skills gap (from workforce monitoring surveys)
- Growth in the readiness index on GCI (Global Cybersecurity Index) and National Cyber Security Index (NCSI).
- Trained professionals are being called upon to join national CERTs.
- Increased growth in the number of locally developed cybersecurity solutions, including the emergence of cybersecurity startups.