USAID Critical Infrastructure Digitization and Resilience (CIDR)

Request For Proposals (RFP)

No. REQ-MKD-23-0001

Call for Proposals for GAP Analysis, Vulnerability Assessment, and implementing an Information Security Management System (ISMS) at the Ministry of Agriculture, Forestry, and Water Economy in North Macedonia

Issue Date: Friday, September 8, 2023

WARNING: Prospective Offerors who have received this document from a source other than the CIDR Project at DAI, 7600 Wisconsin Avenue, Bethesda, MD, 20814, should immediately contact **CIDR_Procurement@dai.com** and provide their name and mailing address in order that amendments to the RFP or other communications can be sent directly to them. Any prospective Offeror who fails to register their interest assumes complete responsibility in the event that they do not receive communications prior to the closing date.

DAI conducts business under the strictest ethical standards to assure fairness in competition, reasonable prices and successful performance or delivery of quality goods and equipment. DAI does not tolerate corruption, bribery, collusion or conflicts of interest. Any requests for payment or favors by DAI employees should be reported as soon as possible to ethics@dai.com or by visiting www.dai.ethicspoint.com. Further, any attempts by an offeror or subcontractor to offer inducements to a DAI employee to influence a decision will not be tolerated and will be grounds for disqualification, termination and possible debarment. See provision No. 9 for more details.

REQ-MKD-23-0001: Questions and Answers

The deadline for receipt of questions was 5:00pm EST on Friday, September 15, 2023. All questions received by the deadline are included below with answers in **blue**.

- Is the scope of ISMS only IT processes or all ministry processes including critical infrastructures?
  Answer: The scope is deliniated with the data collected and processed and the services offered by the Ministry. The main goal is to protect this data, especially personal, financial, and other confidential and sensitive data, as well as to protect the services offered by the Ministry. Internal services offered from the IT department are only part of the scope as other processess of the Ministry are also included within the scope. Some of the services are provided from the central location while others are provided through the branch offices.

- Will the 40 branches mentioned in the document be included in the scope of ISMS certification?
  Answer: In general yes, additional scoping and inclusion of particular branch office will depend on the provision of services of the Ministry through the branch office, and also on the uniformity of the branch office setup.

- Approximately, how many assets and asset types are in the scope of ISMS?
  Answer: Asset identification is part of the procured services. The expected range is up to 400 assets, with priority given to the core infrastructure, connection points for the branch offices with the central location, and the end-points.

- Do assets have priority or importance level? If so are they categorized accordingly?
  Answer: Priority and importance of the assets is based on the sensitivity of the data and in accordance with the CIA triade. The activities stated in the question are part of the scope and are to be performed by the provider in cooperation with representatives from the Ministry.

- Approximately what is the number of software used in the Ministry? (commercial and not-commercial)?
  Answer: The activities stated in the question are part of the scope of work.

- Are there any former penetration test reports that were conducted on the systems? If not, are assessments wanted to be relied on automated vulnerability scanners or penetration tests which also includes automated scanning?
  Answer: There is no penetration report that can be shared at this time. The requested testing as part of the vulnerability assessments will be used to provide risk analysis inputs on a technical level, and it should be delivered to the extent that there are no false results that would impact the analysis. The testing should include, for example, all misconfigurations. Automated tools used for the assessment activity will be allowed. In general, this task is not entirelly dependent on the automation and it is expected form the provider to include in certain cases manual checks in order to prove the accuracy of the findings, followed by detailed documented reports and data.

- Does the service recipient have report formats or can the analysis be on the service providers report format?
  Answer: The format of the reports should be based on the proven methodology as best practices and at minimum the reporting requirements must comply with ISO 27005. The exact format(s) shall be agreed on at the start of the activities.

- Can service recipient provide detailed role structures, asset importances, network topologies and currently used active device rules?
  Answer: The organizational chart and structure can be provided through the public sources of the Ministry, but at this stage, their data may be considered sensitive and/or confidential. The statements in the question should be part of the deliverables of the project; for example, asset importance network topology and defined rules for active devices.

- Would be possible to know how large is the environment is? Such as how many devices connected to the network?
  Answer: Up to 400 assets, with priority given to the core infrastructure, connection point for the branch offices with the central location, and the endpoints.

- What are the operating systems running at servers and clients at the Ministry of agriculture, forestry and water economy?
  (MoA)
  Answer: Mostly Windows and Linux, but the provider of the services should be well versed in assessing other OSs.

- Is there a specific Information Classification and Handling Policy that MoA would like us to follow for the Asset inventory and classification? Or should we create one?
  Answer: The information classification and handling policy should be based on IS 27001:2022 requirements. It should at least include information, software, hardware, servicesof all organization units within the Ministry. This falls under joint activity and agreement that the provider should establish with the Ministry.

- Does a review of the network diagrams included for the assessment of technical infrastructure?
  Answer: No

- What would be the scope of the vulnerability risk assessment?
  - Is it an internal vulnerability risk assessment that includes servers, end-points, and internal applications? or an external vulnerability risk assessment that provides for anything outside the firewall, public-facing web applications, open ports, etc.?

  Answer: External penetration testing is not part of this scope of work. The scope will include only the activities listed in the RFP.

- Would like to confirm if the pricing is $60,000.00 or $600,000.00?
  Answer: The budget ceiling is $60,000.00 USD (Sixty Thousand USD).