AMENDMENT #2: Activity No. 2025-21004A: Technical Assistance: Bulgaria Public Administration Cybersecurity

POC: Mary Larocco, USTDA, 1101 Wilson Boulevard, Suite 1100, Arlington, VA 22209-3901, Tel: (703) 875-4357, Fax: (703) 775-4037, Email: RFP@ustda.gov.

Please note that the Request for Proposals (RFP) for the Technical Assistance for the Bulgaria: Public Administration Cybersecurity is amended, as follows:

Questions, Answers and Clarifications: This amendment consists of clarifying questions and answers submitted by potential Offerors regarding the RFP packet. Responses to submitted questions are attached.

Question #1:

Our company would like to reconfirm its understanding of the Nationality, Source, and Origin clause in Annex II of the Grant Agreement. Could USTDA please confirm whether up to 30% of the total budget may be allocated exclusively to:

· Bulgarian citizens

· Individuals who are residents of or lawfully authorized to work in Bulgaria

· Bulgarian subcontractors

Additionally, is our understanding correct that Bulgarian entities are the only non-US entities that may be subcontracted or recruited under this provision and no other regional, non-US entities/experts will be accepted?

A1: This is correct. Up to 30% of the grant funds may be allocated to a subcontractor entity or entities that are registered to do business in Bulgaria.

Either the prime Contractor or a Bulgarian subcontractor engaged on this activity can utilize up to 30% of the grant funds for labor from: (i) Bulgarian citizens, (ii) a permanent resident of Bulgaria, or (iii) any other person lawfully authorized to work in Bulgaria. Citizens of another country or a regional bloc (i.e., the EU) who are

legally permitted to work in Bulgaria would be permissible, so long as they comply with all applicable employment laws.

Question #2:

We note that no page limits have been specified for the proposal sections. To promote consistency and comparability across submissions, could you please confirm whether you would be willing to introduce page limits? We propose the following maximum limits per section (using a readable font, size 10 pt):

· Firm Background Information: 1 page

· Organizational Structure, Management Plan, and Key Personnel: 10 pages

· Technical Approach and Work Plan: 10 pages

· Experience and Qualifications: 6 pages

In addition, we propose that supporting materials such as CVs and detailed work plan tables (if using Excel schedules) be submitted as annexes and not count towards the above page limits.

A2: The grantee confirms that no page limits will be applied to the proposal sections, except for the Executive Summary, which should be limited to no more than five (5) pages. For all other documentation offerors are free to structure their responses as they deem appropriate and provide as much detail as they consider necessary to adequately address the requirements of the procurement.

Question #3

What is the anticipated duration of the programme?

A3: The anticipated duration of the Technical Assistance is approximately twelve months or one year.

Question #4:

Is direct engagement with at least 15 U.S. suppliers expected to include formal interviews or simply documented outreach?

A4: The Offerors are intended to provide a robust understanding of the market, relationships, and ability to assess supplier capabilities.

To this end, both direct interviews/consultations and documented outreach activities are expected to be undertaken. The number of interviews and suppliers to be interviewed is going to be defined during execution.

Question #5:

Could you please confirm whether the 12 tasks outlined in the Terms of Reference are expected to be delivered sequentially, or whether bidders are encouraged to propose an appropriate sequencing and structuring of these tasks within technical approach?

A5: Unless otherwise specified in the Terms of Reference, USTDA defers to the Grantee and the selected Contractor to jointly determine the appropriate sequencing of task performances. Any bidder that intends to perform tasks out of sequence from those listed in the Terms of Reference could specify as such in its submission to assist the Grantee's evaluation thereof, but this is not required.

Question #6:

Which institutions have formally committed to participating in the activity?

A6: For the purposes of this assignment, Offerors should consider the Ministry of Innovation and Digital Transformation (MIDT) and Information Services JSC (IS JSC) as the primary organizations within the scope of the assessment and stakeholder engagement activities.

Question #7:

Amendment No. 1 revised Task 2 to reference the "review and further development" of NCS documentation. Could USTDA and/or the Grantee please confirm what existing NCS documentation, policy frameworks, architectural artifacts, draft strategies, standards, or related materials MIDT or IS JSC currently has in place that the Contractor would be expected to review and build upon?

A7: The Contractor will be expected to review and build upon the documentation currently available from MIDT. The documentation to be provided will include, at a minimum:

1. System Architecture
2. High-Level Design (HLD)
3. Low-Level Design (LLD)
4. SOC (Security Operations Center) Processes

These materials are intended to provide the foundational information necessary for understanding the current environment. Additional relevant documentation may be shared during project implementation if deemed necessary and available.

Question #8:

Task 6 requires the Contractor to model at least three SOC growth scenarios, with assumptions that may include log data ingestion rates, endpoints monitored, staffing levels, incident volumes, and technology scaling requirements. Will JSC provide current baseline data for these metrics, or is the Contractor expected to develop baseline assumptions independently based on interviews, available documentation, and industry benchmarks?

A8: The Contractor is expected to possess the necessary qualifications, knowledge, and experience to develop appropriate baseline assumptions for the SOC growth scenarios. Accordingly, Offerors should not assume that specific baseline data for metrics such as log data ingestion rates, endpoints monitored, staffing levels, incident volumes, or technology scaling requirements will be provided.

As part of the assignment, the Contractor is expected to assess the current environment, gather and validate relevant information through stakeholder engagement and review of available documentation, and apply professional judgment and industry best practices to establish the assumptions required for the analysis.

The proposed SOC growth scenarios should clearly state the underlying assumptions and demonstrate the methodology used to derive them.

Question #9-#10:

The RFP and Terms of Reference refer to the exclusion of law enforcement, national security, and intelligence agencies from the project scope, based on the jurisdictional boundaries of the former Ministry of Electronic Governance. In May 2026, the Ministry of Electronic Governance merged with the Ministry of Innovation and

Growth to form the Ministry of Innovation and Digital Transformation, which is now designated as the joint beneficiary of this Technical Assistance. Could USTDA and the Grantee please confirm:

#9. Whether MIDT's current ministerial mandate and jurisdictional scope are identical to the former MEG's mandate with respect to cybersecurity oversight authority, specifically confirming whether law enforcement, national security, military, and intelligence agencies remain excluded from the NCS scope and SOC migration roadmap; and

#10. Whether the definition of "Covered Entities" under the Cybersecurity Act, as referenced in the Terms of Reference, includes any entities under the jurisdiction of the Ministry of Interior, Ministry of Defense, State Agency for National Security, or any other law enforcement, military, or intelligence body.

If any such entities are potentially in scope, clarification would be helpful before proposal submission, as this may materially affect the technical approach, access requirements, personnel qualifications, clearance considerations, and the overall risk profile of the engagement.

A9: The grantee confirms that, for the purposes of this Technical Assistance, the scope and jurisdictional boundaries applicable to the former Ministry of Electronic Governance continue to apply. Accordingly, law enforcement, national security, military, and intelligence agencies remain outside the scope of the NCS initiative and the SOC roadmap to be developed under this assignment.

Therefore, Offerors should assume that the project scope is limited to the civilian public-sector entities falling within the relevant mandate of the Ministry of Innovation and Digital Transformation and should not include law enforcement, national security, military, or intelligence organizations in their analyses, assessments, recommendations, or roadmap development activities.

A10: See A9

Question #11:

To inform the proposed approach for the NCS Architecture under Task 2.1, the NISM Compliance Plan under Task 2.2, and the SOC Roadmap under Task 6, could USTDA

and/or the Grantee provide an approximate count of Covered Entities currently subject to OMRNIS requirements? Could USTDA and/or the Grantee also indicate how many of those entities are currently expected to migrate SOC operations or managed cybersecurity services to Information Services JSC under the proposed NCS?

A11: At present, there are approximately 100 Covered Entities subject to the applicable OMRNIS requirements.

For planning purposes under the proposed NCS, it is currently anticipated that approximately 30 entities will migrate their SOC operations.

These figures should be considered indicative and are provided to assist Offerors in developing their technical approach for the NCS Architecture (Task 2.1), the NISM Compliance Plan (Task 2.2), and the SOC Roadmap (Task 6). Offerors are expected to apply their professional judgment and propose a scalable approach that can accommodate potential changes in the number of participating entities over time.

Question #12:

Task 5 requires a comprehensive assessment of IS JSC's current SOC operating model, including governance, staffing, processes, technology platforms, incident response playbooks, service lines, SLAs, pricing, and performance metrics. Will IS JSC make available to the selected Contractor direct access to SOC personnel for interviews and access to relevant operational documentation, including system configurations, service agreements, playbooks, metrics, and related materials necessary to complete the assessment? If access to certain information will be restricted, could USTDA and/or the Grantee identify those limitations so Offerors can account for them in the proposed methodology?

A12: The Ministry of Innovation and Digital Transformation (MIDT) and Information Services JSC (IS JSC) will facilitate access to relevant personnel and documentation to the extent necessary and appropriate for the execution of the assignment. However, Offerors should not assume that specific operational metrics, detailed system configurations, service agreements, playbooks, or other internal SOC artifacts will be made available in a predefined format or with a guaranteed level of completeness.

The Contractor is expected to possess the necessary knowledge, qualifications, and experience to assess the current SOC environment and develop findings and

recommendations based on available information, stakeholder discussions, SOC personnel interviews, and industry best practices.

Accordingly, Offerors should propose a methodology that is sufficiently flexible to accommodate varying levels of information availability. The assessment should rely on the Contractor's professional expertise to evaluate the current operating model and identify any information gaps that may need to be addressed during the course of the engagement.

Any access limitations resulting from confidentiality, security, or operational considerations will be communicated to the selected Contractor as appropriate; however, no specific restrictions have been identified at this stage.

Question #13:

The RFP references PRIDST funding available to Bulgarian government agencies for cybersecurity investments. Beyond PRIDST, are there any ongoing EU-funded, TAIEX, Twinning, NATO, World Bank, or other internationally funded technical assistance programs currently advising MIDT, IS JSC, or related Bulgarian public-sector entities on cybersecurity governance, SOC operations, NIS2 implementation, or NCS development? If so, will the selected Contractor be expected to coordinate with those programs, and will relevant documentation be made available?

A13: The Ministry of Innovation and Digital Transformation (MIDT) and Information Services JSC (IS JSC) are not aware of any ongoing EU-funded, TAIEX, Twinning, NATO, World Bank, or other internationally funded technical assistance programs currently advising MIDT, IS JSC, or related Bulgarian public-sector entities on cybersecurity governance, SOC operations, NIS2 implementation, or NCS development that are relevant to the scope of this assignment.

Accordingly, no specific requirements for coordination with other technical assistance programs are envisaged under this project. Offerors should therefore prepare their proposals on the assumption that the selected Contractor will not be required to coordinate with parallel externally funded initiatives.

As no such programs have been identified in relation to this assignment, no associated documentation is expected to be made available. Should any relevant initiatives

emerge during the project, any necessary coordination arrangements will be communicated to the selected Contractor as appropriate.

Question #14:

For past performance references involving national government clients, public-sector cybersecurity projects, or sensitive cybersecurity engagements where confidentiality, national security restrictions, or non-disclosure agreements limit disclosure of client contact information or contract details, will USTDA and the Grantee accept a generalized description of scope, deliverables, outcomes, and client type instead of full client-identifying information? If not, what minimum information is required to satisfy the reference requirements in Section 3.5?

A14: For the purposes of demonstrating relevant experience, Offerors may provide references that include a generalized description of the project scope, deliverables, outcomes, and client type where confidentiality obligations, national security restrictions, or non-disclosure agreements limit the disclosure of client-identifying information or specific contract details.

The primary objective of the past performance requirement is to enable the evaluation of the Offeror's experience and capabilities in delivering assignments of comparable scope and complexity. In this regard, references should provide sufficient information to demonstrate the relevance of the work performed, particularly in areas such as cybersecurity strategy, Security Operations Center (SOC) development and optimization, cyber-defense maturity assessments, maturity frameworks for cyber-defense centers, and the development, enhancement, or upgrade of NCS capabilities.

At a minimum, Offerors should provide:

- A description of the client type (e.g., national government agency, public-sector entity, critical infrastructure operator, etc.);
- The project's objectives and scope;
- Key deliverables and services provided;
- The timeframe of the engagement;
- The outcomes achieved; and
- The Offeror's role and responsibilities.

Where client-identifying information cannot be disclosed, Offerors should clearly indicate that such information is subject to confidentiality restrictions.

Question #15:

The RFP requires letters of commitment from proposed key personnel confirming their availability. Does this requirement apply only to individuals designated as key personnel in the organizational structure and management plan, or does it apply to all named personnel included in the proposal, including supporting SMEs and subcontractor personnel?

A15: The requirement for letters of commitment applies only to personnel identified as Key Personnel in the proposed organizational structure and management plan.

Question #16:

Could USTDA and/or the Grantee provide the anticipated project start date, expected duration, and target completion date for the Technical Assistance, assuming timely award and contract execution?

A16: The grantee and USTDA are not able to provide a specific start date. The RFP is scheduled to close on August 3, 2026, and then the grantee will begin their review process. Please see more information about the USTDA competed granted process linked below on the USTDA document center webpage.

https://s3-us-gov-west-1.amazonaws.com/cg-654ebf73-8576-4082-ba73-dd1f1a7fe8dc/uploads/Competed-Process-Flow-Chart-Presentation_final-2.pdf

Question #17:

Could USTDA and/or the Grantee clarify whether any tasks are expected to require in-person work in Bulgaria, including the kickoff meeting, stakeholder interviews, SOC assessment activities, workshop, or final presentation? If in-person work is expected, please identify the specific tasks or meetings for which on-site presence is required or preferred.

A17: Certain project activities are expected to be conducted **in person in Bulgaria**. Specifically, on-site participation is expected for the following key events:

- **Project Kick-off Meeting**
- **Workshop(s) with relevant stakeholders**
- **Final Presentation of findings and recommendations**

For all other activities, including stakeholder interviews, assessment work, analysis, and the preparation of deliverables, Offerors may propose the approach they consider most effective, including a combination of remote and in-person engagement as appropriate.

Question #18:

Given that the Technical Assistance may require review of SOC documentation, cybersecurity policies, incident response materials, system metrics, or other operational information, could USTDA and/or the Grantee clarify whether any data-handling, remote-access, hosting, confidentiality, GDPR, or Bulgarian public-sector information-security restrictions are expected to apply to the Contractor's work? In particular, will any reviewed data or documentation be required to remain within Bulgaria or the European Union?

A18: All applicable information security, confidentiality, data protection, and public-sector information-handling requirements are expected to apply to the Contractor's work throughout the execution of the assignment.

Offerors should assume that access to and handling of documentation, operational information, cybersecurity-related materials, and other project data will be subject to relevant legal, regulatory, and organizational restrictions, including applicable GDPR requirements and information security policies.

The Contractor will be expected to implement appropriate safeguards for the protection, storage, transmission, and processing of any information obtained during the engagement and to comply with any specific security requirements communicated by the Grantee or relevant authorities.

Offerors should therefore propose a methodology that can operate within a controlled and security-conscious environment. Any detailed requirements regarding data access, remote connectivity, information handling, confidentiality obligations, or location-based restrictions on data storage and processing will be communicated to the selected Contractor as applicable during project implementation.

Question #19:

Could USTDA provide any additional formatting or length preferences for the technical proposal?

A19: There is not a technical proposal length requirement. Regarding the formatting requirements please carefully review Section 3: PROPOSAL FORMAT AND CONTENT.

Question #20:

Beyond the five weighted evaluation criteria outlined in Section 4 of the RFP, how should Offerors prioritize the depth and structure of their technical narratives to most effectively demonstrate relevant qualifications, and what additional guidance can USTDA provide on the relative importance of specific sub-elements within each criterion?

A20: Beyond the five weighted evaluation criteria set forth in Section 4 of the RFP, no additional weighting or prioritization will be applied to specific sub-elements within those criteria.

Offerors are encouraged to use their professional judgment in structuring their technical proposals and in determining the level of detail necessary to demonstrate their qualifications, experience, and proposed approach. There is **no page limit** for proposal submissions, and Offerors are free to provide any information and supporting documentation they believe is relevant to substantiate their expertise, past performance, technical capabilities, methodology, and project team qualifications.

The evaluation will be based on the extent to which the proposal clearly demonstrates the Offeror's ability to successfully perform the required services in accordance with the published evaluation criteria. Accordingly, Offerors are encouraged to provide sufficiently detailed narratives and supporting evidence that highlight relevant experience, expertise, and the practical applicability of their proposed approach to the objectives of the assignment.

Offerors may include additional materials, references, case studies, methodologies, certifications, or other documentation they consider helpful in demonstrating their qualifications and experience.

Question #21:

Would USTDA consider the use of third-country personnel for advisory or analytical support from regional subject matter experts? And can this additional personnel be included in the 30% local requirement?

Given the relevance of regional cybersecurity governance models and the potential value of incorporating lessons learned and leading practices from nations that have undergone similar national cybersecurity system implementations.

A21: Up to 30% of the grant funds may be allocated to a subcontractor entity or entities that are registered to do business in Bulgaria.

The prime Contractor and/or Bulgarian subcontractor(s) engaged on this activity can utilize up to 30% of the grant funds for labor from: (i) Bulgarian citizens, (ii) a permanent resident of Bulgaria, or (iii) any other person lawfully authorized to work in Bulgaria. Citizens of another country or a regional bloc (i.e., the EU) who are legally permitted to work in Bulgaria would be permissible, so long as they comply with all applicable employment laws.

Personnel who are not U.S. or Bulgarian citizens, are not U.S. or Bulgarian permanent residents, or are not lawfully authorized to work in the U.S. or in Bulgaria would be impermissible.

Question #22:

Referring to Appendix 3.10, pg 27, what, if any, target countries does USTDA contemplate for this activity?

A22: There is not a “Target country” is this particular Technical Assistance.

Question #23:

Referring to Annex 1, pg 33, would USTDA provide further guidance on the process for task modifications and indicate who will provide written approval?

A:23 All proposed amendments or other proposed modifications to the Tasks in the Terms of Reference must be jointly agreed upon by the Grantee and Contractor in

writing and signed by both parties, but they only become effective if expressly approved in writing by USTDA's Office of General Counsel.

As financier of the activity, USTDA would typically be involved in any preliminary discussions between a Grantee and Contractor if the parties identify a potential need to modify a task or tasks. This allows each of the Grantee, the Contractor, and USTDA to fully understand any potential ramifications to the work schedule, and whether such changes are permissible under USTDA's Mandatory Contract Clauses and within the budget

Question #24:

What level of detail does USTDA expect in the NCS architecture (e.g., conceptual framework vs. implementation-ready technical design)? Would USTDA be able to provide any additional definition of expected design depth or granularity?

A24: USTDA and the Grantee expect the NCS Architecture to go beyond a high-level conceptual framework and provide an implementation-ready technical design that can serve as a practical foundation for deployment and operationalization of the NCS.

The proposed architecture should include sufficient technical depth and granularity to support decision-making, planning, procurement, implementation, and future operations. In particular, the architecture is expected to identify the key functional and technical components, their relationships and interfaces, governance considerations, and the target operating model required to achieve the objectives of the NCS.

In addition, the architecture should include clear recommendations for future growth and scalability, addressing how the NCS can accommodate an increasing number of participating entities, evolving cybersecurity requirements, growing data volumes, additional services, and future technology enhancements.

Offerors are encouraged to propose a level of design that demonstrates a clear path from the current state to implementation, while ensuring that the architecture remains adaptable, scalable, and aligned with long-term national cybersecurity objectives.

Question #25:

To what extent do the Reference Task Values provided in Appendix 4 reflect direct project expenses such as international and in-country travel, lodging, and incidental

costs associated with in-person activities including the Kickoff Meeting, National Cybersecurity System Workshop, and Final Presentation, and how should Offerors account for these costs in planning their technical approach and level of effort? Is there an expectation for non-host country personnel to be in country for an extended period?

A25: Appendix Four provides an estimated value for each task. Offerors can use this as an example, but it is not binding.

Question #26:

Could USTDA please provide additional guidance on which international frameworks such as NIS2, ISO 27001, and NIST CSF should be prioritized for this activity?

A26: NIS2, ISO 27001, and NIST CSF, SOC CMM

Question #27:

Could USTDA please clarify the level of access, upon award, the offeror will have to relevant documentation and information from the Ministry of Innovation and Digital Transformation (MIDT) and Information Services JSC, and how will that access and information take place?

A27: Upon award, the Contractor will be provided with access to relevant documentation and information from the Ministry of Innovation and Digital Transformation (MIDT) and Information Services JSC to the extent necessary for the performance of the assignment.

Offerors should not assume that specific operational metrics, datasets, or other detailed quantitative information will be provided. The Contractor is expected to apply its professional expertise, knowledge, and experience to assess the current environment based on the information made available, stakeholder engagements and industry best practices.

28. Would USTDA provide guidance regarding the language requirements for all formal deliverables, interim work products, workshop materials, and presentations outlined across the twelve tasks in the Terms of Reference, and to what extent should Offerors anticipate the need to provide Bulgarian-language versions of key deliverables?

A28: All formal deliverables, interim work products, workshop materials, presentations, and other outputs produced under this assignment are expected to be provided in English.

Question #29:

Would USTDA provide guidance on what administrative support and documentation will be provided to the selected offeror to facilitate tax exemption on eligible expenditures incurred in the host country during performance of the Activity, and what process should the offeror anticipate for obtaining any necessary tax exemption letters, certifications, or other official instruments required by Bulgarian authorities to ensure full compliance with local provisions?

A29: USTDA will not provide specific guidance, administrative support, or documentation for managing the Offeror's tax obligations. The selected Contractor is solely responsible for understanding, managing, and complying with all applicable tax laws, regulations, and procedures in the host country, including determining the applicability of any tax exemptions and obtaining any required tax exemption letters, certifications, permits, or other official documentation from the relevant authorities.

Question #30

While preparing our proposal for the referenced RFP, we identified a few key experts who need to be reallocated to this project. They will require a couple of weeks to wrap up their current assignments. Could the Government/Grantee please consider extending the proposal due date by two weeks?

A30: The proposal due date has been extended until August 3, 2026.

Question #31

What is the desired end state for IS as the default national SOC provider?

Specifically, should the contractor assume IS will provide centralized monitoring, incident response, advisory support, procurement support, compliance oversight, or some combination of these functions?

A31: For the purposes of this assignment, Offerors should assume that Information Services JSC (IS JSC) is envisioned as the default national SOC service provider under the NCS framework.

The desired end state is for IS JSC to provide a comprehensive set of centralized cybersecurity services to participating entities. These functions are expected to include a combination of:

- Centralized security monitoring and detection capabilities
- Incident response and coordination support
- Cybersecurity advisory and expert services
- Support for the acquisition and deployment of cybersecurity capabilities and services
- Compliance monitoring and oversight support related to applicable cybersecurity requirements
- Shared SOC and managed cybersecurity services for participating entities

A key objective of the assignment is to assess and define the most appropriate target operating model, governance structure, service portfolio, and implementation roadmap to support this vision. Accordingly, Offerors should consider a broad service delivery model that enables IS JSC to provide scalable, efficient, and sustainable cybersecurity services while supporting the long-term objectives of the NCS.

Question #32:

Following award, what current-state documentation, operational data, facility access, and stakeholder engagement opportunities will be made available to support the current-state assessment and roadmap development activities?

A32: Upon award, the Contractor will be provided with access to relevant documentation and information from the Ministry of Innovation and Digital Transformation (MIDT) and Information Services JSC to the extent necessary for the performance of the assignment.

Offerors should not assume that specific operational metrics, datasets, or other detailed quantitative information will be provided. The Contractor is expected to apply its professional expertise, knowledge, and experience to assess the current

environment based on the information made available, stakeholder engagements and industry best practices.

Question #33:

What level of detail is expected for the Financing Plan and Cybersecurity Procurement Oversight Plan deliverables? Should the contractor provide high-level planning assumptions, multi-year budget estimates, procurement sequencing recommendations, or implementation-ready investment and acquisition recommendations?

A33: The Financing Plan and Cybersecurity Procurement Oversight Plan should be developed at an implementation-ready level of detail rather than as high-level planning documents. The contractor is expected to provide comprehensive and actionable recommendations that can directly support decision-making, budgeting, and execution activities.

Question #34:

Would participation in this technical assistance activity create any organizational conflict-of-interest restrictions regarding future implementation, procurement, or follow-on cybersecurity activities that may result from this study?

A34: Based on the current understanding of this assignment, participation in this Technical Assistance activity is not expected to create any organizational conflict-of-interest restrictions with respect to future implementation, procurement, or follow-on cybersecurity activities that may result from the study.

Accordingly, Offerors may assume that involvement in the preparation of the assessment, recommendations, architecture, roadmap, and related deliverables under this assignment will not, in itself, preclude them from participating in future opportunities that may arise from the project's outcomes.

Nevertheless, Offerors remain responsible for complying with any applicable conflict-of-interest requirements set forth in the RFP, Grant Agreement, or other relevant procurement regulations and policies. At this time, no specific conflict-of-interest restrictions are anticipated as a result of participation in this Technical Assistance activity.

Question #35

Which government ministries, agencies, and other entities should be considered in scope for assessment and stakeholder engagement under this assignment? The RFP references multiple organizations, including MEG, MIDT, IS, DANS, MoD, and MoI, but does not clearly establish the intended scope of stakeholder engagement.

A35: For the purposes of this Technical Assistance, Offerors should consider the Ministry of Innovation and Digital Transformation (MIDT) and Information Services JSC (IS JSC) as the primary organizations within the scope of the assessment and stakeholder engagement activities.

While other government entities may be referenced in the background materials or may be consulted as appropriate during the course of the assignment, Offerors should base their proposed methodology and stakeholder engagement approach on engagement with MIDT and IS JSC.

Accordingly, Offerors should not assume that organizations such as DANS, the Ministry of Defence (MoD), the Ministry of Interior (MoI), or other national security, military, intelligence, or law enforcement bodies are within the scope of the assessment unless otherwise specifically directed during project implementation.