GOBIERNO DE PUERTO RICO
PUERTO RICO INNOVATION AND TECHNOLOGY SERVICE

Questions and Answers (Q&A) for Service Contract Opportunity Notice PRITS-2023-006

For Comprehensive On-Demand Cybersecurity Support: Virtual CISO (vCISO) Services for Enhanced Government Cyber Resilience

Table of Contents

1. Introduction 1

2. Questions 1

Scope 1

General 1

Legal Affairs 2

Timeline, Reporting, and Performance Metrics 3

Certifications and other requirements 4

Services 5

Technical 5

Out-of-Scope Questions 6

1. Introduction

The Puerto Rico Innovation and Technology Service (PRITS) Office has created this question-and-answer (Q&A) document to address inquiries and provide clarification for those interested in submitting proposals for comprehensive vCISO services for enhanced government cyber resilience. This document promotes transparency, fairness, and a clear understanding of the requirements and expectations associated with these projects. The following section presents the received questions and their corresponding responses, categorized by relevant topics for easy reference and comprehension.

2. Questions

Scope

1. What is the scope of the vCISO services in terms of the number of agencies, municipalities, and other entities?

   In direct alignment with PRITS, the Selected Proponent(s), if any, will be strategically allocated across various government entities and/or municipalities, depending on the proponents' demonstrated capacity and capabilities. This dynamic allocation process will ensure that resources are optimally utilized, enhancing the overall effectiveness of cybersecurity efforts and ensuring that the government benefits from the expertise and resources needed to meet specific goals and objectives.

2. Can you provide more specific details of the functions and roles of the vCISO?

   The vCISOs will assisting and supporting the internal CISO with the cybersecurity strategy, and further strengthening the overall information security posture. Their functions encompass the collaboration on developing comprehensive cybersecurity policies and procedures, assisting in assessments and risk mitigation, facilitating the management of security incidents and responses, ensuring compliance with industry regulations and standards, providing strategic guidance and insights on technology and infrastructure, and fostering a culture of cybersecurity awareness among staff. The vCISOs' role is multifaceted, combining technical expertise with strategic guidance to safeguard critical assets, sensitive data, and the government's resilience against evolving cyber threats.

General

1. Are there plans to move forward the proposal submission deadline, considering the short time frame between the publication of the responses and the current proposal deadline?

   SCON PRITS-2023-006 complies with the minimum open period for receiving proposals. Currently, there is no anticipation of extending the submission period for proposals.

2. When will responses to these questions be provided?

   As stated on the SCON's cover page and section 1.1, responses will be published on September 21st, 2023.

3. How will the responses be provided? Will all questions and answers be shared among all Proponents?

As per Section 1.2.2 of the SCON, the responses will be published on the PRITS website (www.prits.pr.gov), ensuring that all Proponents can access them.

4. What is the deadline (time of the day) on Sept 25, 2023, to submit the proposal? (e.g., 11:59 PM AST, 5:00 PM AST, etc.)

   Proponents may submit proposals until 11:59 PM AST.

5. How would I get confirmation of receipt of the proposal since submission is via email and not a secure web portal?

   An email will be sent to confirm that we have received your submission.

6. If the proposal must be mailed via post or personally delivered, could you provide an address and more explicit instructions on the delivery?

   As outlined in Section 2.2 of the SCON, proposals must be submitted electronically to procurement@prits.pr.gov before the specified deadline. In cases where email attachments exceed size limits, physical copies may be considered. If submitting by mail, proposals must reach PRITS by the established deadline. For in-person and mail submissions, please use PRITS' address:

   360 Calle Ángel Buonomo
   Sector Tres Monjitas
   San Juan PR 00918

7. What are PRITS default invoicing and payment terms?

   As per the contract agreement, contractors must submit invoices once a month for services performed, and allowable reimbursable costs (if any) incurred before the invoice date. Invoices should be prepared based on the cost proposal submitted and negotiated with PRITS.

   PRITS shall make monthly payments, based on invoices received, for actual services satisfactorily performed, and for authorized reimbursable costs incurred, as outlined in the contract agreement. PRITS will pay the contractor no later than 30 days after receiving a compliant invoice.

8. What internal human resources will be available for this project?

   vCISOs will work closely with PRITS' internal CISO, the Security Operations Center (SOC), the Chief Innovation and Information Officer (CIIO), the Chief Technology Officer (CTO), Chief Information Officers of government entities and municipalities, PRITS internal staff, and other key stakeholders, as determined by assigned tasks.

Legal Affairs

1. Are Service Level Agreements going to be required?

   A Service Level Agreement might be requested depending on the specific tasks and scope of the vCISO services.

2. Is this an annual or multiannual contract? Do we need to quote two years or one, as the SCON mentions?

   The contract may be extended up to two years. Proponents shall include services for two years in their proposals; however, they must provide a cost breakdown for both one and two years, respectively.

3. Can you provide the complete schedule, including dates, the entire process, covering contract award, contract formalization, and the contract's start date? Section 3.3 mentions that any modifications to the schedule due to this request will be included in the timeline. However, there is no information in the SCON defining the full schedule and timelines.

   The contract award will take place after PRITS conducts a thorough evaluation of all submitted proposals. Section 3.3 specifies that if PRITS requires additional information from qualified proponents during the evaluation process, the selection committee may request it. Once a proponent is selected, the legal division will contact them. Contract formalization will occur only after all necessary documents have been received, and all legally required processes have been completed. PRITS retains the authority to manage the full schedule and other internal government-related processes.

4. Is PRITS Fiscal year aligned with the Calendar year? If not, what is PRITS Fiscal year first month?

   As a government agency, PRITS follows the government's fiscal year, which start on July 1st.

Timeline, Reporting, and Performance Metrics

1. How will the project success will be measured? Will you be using existing metrics and Key Performance Indicators (KPIs), or will new ones need to be designed?

   KPIs are included as part of the Cybersecurity Plan. These performance metrics have been designed to align with our cybersecurity objectives and ensure the effectiveness of our security measures. While the initial set of KPIs is in place, our approach remains flexible and adaptive. As we progress in our cybersecurity initiatives, adjustments to these KPIs may be required to address evolving threats and vulnerabilities. These modifications will be overseen and managed by our internal Chief Information Security Officer (CISO).

2. Are there any key milestones or deadlines for this period?

   The milestones and deadlines are initially defined within the Cybersecurity Plan. However, these timelines may be subject to adjustments based on evolving government needs and at the discretion of the internal CISO. Detailed information regarding any changes or updates to these milestones will be communicated to the Selected Proponents.

3. How frequently and in what format should progress updates be submitted?

   Progress updates may be requested on a weekly, bi-weekly, or monthly basis, depending on the project's complexity, tasks assigned, and government needs. These reports shall include a comprehensive overview of key milestones achieved, any identified cybersecurity risks, mitigation actions or updates on compliance with relevant standards or regulations, and recommendations to further improvements. The frequency and content of these updates will be determined by the internal CISO and tailored to ensure PRITS remains well informed on the overall state of cybersecurity and make informed decisions.

Certifications and other requirements

1. Are there any other specific regulatory requirements or standards, such as ISO 27001, HIPAA, PCI, NIST, or GDPR, or similar that your organization is obligated to comply with?

   The specific regulatory requirements and standards can vary across government entities and their required operations. As the services provided may have a government-wide impact, each entity may have its own unique compliance needs and obligations. Therefore, it is essential for vCISOs to be flexible and adaptable in addressing these diverse requirements as they work with different government entities.

2. Regarding the request to submit certifications, are there particular certifications that are required?

   We anticipate that Proponents will provide certifications pertinent to the cybersecurity services outlined in the SCON. These certifications will serve as a demonstration of their expertise and qualifications in delivering the required services effectively.

3. Is the expectation for the vCISO to work full-time throughout the engagement, or will the daily hours be determined based on the specific goals and tasks assigned to the vCISO?

   The tasks to be assigned to vCISOs will depend on their qualifications, capabilities, and the specific goals and assigned tasks. However, the nature of these tasks may evolve and change over the course of the performance period. The specific hours and workload will be tailored to the government needs and aligned with the dynamic cybersecurity landscape and PRITS' objectives, ensuring that vCISOs can provide comprehensive and responsive support as required.

4. Is it acceptable to submit a proposal that includes a group or pool of multiple vCISOs? Can the vCISO leverage other resources in its Company/organization to assist in delivering the expected outcomes under the vCISO guidance and direction?

   Both individual vCISOs and companies or groups of vCISOs are eligible to submit proposals in response to the SCON. While it is possible for the vCISO to leverage additional resources within their organization, it is important to note that the extent of such resource utilization may be subject to limitations upon the specific tasks assigned. The emphasis of this SCON lies in the expertise that the vCISO can contribute to each government entity and/or municipality. If additional resources are considered for utilization, the proposal must include their qualifications. Additionally, all resources, will be subject to the same terms and agreements, including NDAs, among other contractual obligations.

5. Do you expect a block of hours to be allocated for all services and deliverables collectively, or is it expected that time estimates will be provided for each specific objective and/or task?

   Proponents are strongly encouraged to incorporate a flexible pricing option that encompasses both options, a block of hours and per-task or per-objective. This approach allows for versatility to adapt to dynamic government needs, ensuring services align to requirements and timelines.

Services

1. Could you clarify the service expectations, including whether the primary work location, the mode of service delivery (remote, on-site, hybrid) and the frequency to travel to multiple locations, if applicable?

   vCISOs are expected to provide their services both virtually, and on-site, including at PRITS facilities, other governmental entities/agencies, and/or municipalities. The specific mode of service delivery will depend on the tasks assigned. The frequency of travel and the allocation of remote or on-site work will vary according to task requirements, government needs, and PRITS' criteria.

2. What is the minimum and maximum number of daily, weekly, and monthly work hours?

   The expected minimum and maximum work hours can vary depending on the nature and urgency of the tasks assigned to the vCISO.

Technical

1. Which cloud service providers and services does your organization use?

   Government entities and PRITS rely on a diverse array of cloud service providers and services to meet their operational needs. It is essential for vCISOs to be well-versed in working with these cloud environments. The expectation is that vCISOs will bring forth their qualifications and expertise to seamlessly collaborate with PRITS, agencies and municipalities, ensuring the secure and efficient management and security controls of these cloud environments.

2. Regarding the strategy, could you please specify which national benchmark should it be aligned to?

   The strategies must align with the comprehensive Cybersecurity Plan in place, and they should comply with supplementary directives and requirements established by PRITS.

3. The RFP outlines a scope of services and deliverables, such as cybersecurity reporting, phishing simulation exercises, cybersecurity awareness and training, and tiered incident management and response planning. Could you please clarify whether PRITS already has the necessary platforms and applications in place to support the delivery of these services, or if the awarded entity is expected to provide the corresponding solutions in addition to the specified deliverables?

   PRITS currently has multiple platforms and applications in place to facilitate the services mentioned in this SCON. However, it is highly encouraged and expected of vCISOs to provide feedback and suggestions regarding any tools or processes that may require improvement or can best align with the strategies of the Cybersecurity Plan.

4. Can you validate the accuracy of the following assumptions:
   a. PRITS will provide essential hardware (laptop) and associated software for the vCISO's role.
   b. Any necessary subscriptions (SaaS) required to fulfill the duties obligations outlined in this SCON will be covered.
   c. Access to the systems and information necessary to performing the responsibilities outlined in this SCON will be granted.
   d. PRITS will cover the expenses associated with the above.

PRITS will supply the essential tools, software, access, and permissions, as needed to fulfill the assigned tasks following the specified requirements. Nevertheless, it is expected that the vCISO will possess the minimum equipment, connectivity, and software for various responsibilities, including collaborating on governance documents, participating in meetings, submitting reports, and engaging with stakeholders, among other duties. PRITS will not cover or reimburse any additional costs incurred by the vCISO for these tools, software, and access.

5. How many employees/emails will be impacted with the phishing simulation? And how often the exercises will be done?

   The number of employees/emails impacted by the phishing simulations will be contingent upon the number of government entities/municipalities assigned to the vCISO. The frequency of these simulations will be determined by the prevailing risk profile and the ever-changing threat landscape, with the final decision made by PRITS.

6. How many historical incidents will be analyzed?

   The number historical incidents available for examination by the vCISO cannot be determined precisely since it will evolve over the performance period. This variability is due to the changing nature of cybersecurity incidents, and the volume may also depend on the number of government entities and/or municipalities assigned to the vCISO. Incidents volumes can fluctuate and the vCISO's role will adapt accordingly to address the specific government needs.

Out-of-Scope Questions

Based on the requirements and scope of services stated in the SCON PRITS-2023-006 "For Comprehensive On-Demand Cybersecurity Support: Virtual CISO (vCISO) Services for Enhanced Government Cyber Resilience," the following questions address confidential information or fall outside the scope of the services requested in this stage; consequently, no responses will be provided to these particular inquiries.

1. What are the anticipated project risks, and is there an established Project Risk Management Plan addressing these risks from a Project Management Perspective)

2. What are the current tools in use for Identity and Access Management? Could you please specify the type of MFA implemented? Is there a regular review of access rights in Active Directory (AD)? Additionally, which version of AD is currently in operation?

3. To contribute to the enhancement of your cybersecurity posture, can you provide an overview of your current cybersecurity posture? This includes existing security protocols and areas of potential vulnerability or concern.

4. What is your existing incident response plan? Are there any specific areas where you believe improvements might be necessary?

5. What is your defined risk tolerance? Is it consistent, or does it vary depending on the government entity.

6. Do you have a Business Impact Analysis (BIA), Incident Response Plan (IRP) or Business Continuity Plan (BCP) currently in effect?

7. How many toolkits you are using for incident response management and containment?

8. How many entities does your security architecture cover, and do you have any existing security diagrams?

9. Does the government have existing risk assessment documentation? Which framework? How many entities are covered under the risk assessment?

10. How many security tools are there per entity? Can you provide with a list of these tools?

11. What is the budget for these services?

12. Is there an expectation of a monthly service/hourly rate?