REQUEST FOR EXPRESSIONS OF INTEREST

CYBERSECURITY CONSULTANTS

Country: The Commonwealth of The Bahamas
Supporting Institution: Inter-American Development Bank
Programmes: Program to Support the Health Sector to Contain and Control Coronavirus and to Mitigate its Effects in Service Provision & Programme to Support the Health System Strengthening of The Bahamas
Project Number: BH-L1053 & BH-L1055
Loan Number: 5179/OC-BH & 5296/OC-BH
Sector: Health
Deadline: 30 November 2022

The Ministry of Health and Wellness (MOHW) of The Bahamas has received financing from the Inter-American Development Bank (IDB), toward the cost of the Program to Support the Health Sector to Contain and Control Coronavirus and to Mitigate its Effects in Service Provision & the Programme to Support the Health System Strengthening of The Bahamas and intends to apply part of the proceeds for the consulting services of **Cybersecurity Consultants**. The successful individual will work as a part of the MOHW on a contractual basis and report to the Chief Medical Officer (or other designated alternate). The successful individuals will also work collaboratively with other leaders from across the Ministry of Health and national health system stakeholders, as well as with other ministries and international partners. The successful individuals will support the Ministry with the design, development, implementation and testing of a Cybersecurity framework inclusive of standards and policies, across the Health Information Exchange (HIE) and other digital health tools to ensure protection of data; as well as a security assessment (Threat Risk Assessment; Penetration Testing, etc.) of the digital health application, infrastructure and HIE architecture to ensure data is protected. These contracts are expected to be completed in a two-year period starting in December 2022.

The Ministry of Health & Wellness now invites eligible Consultants to indicate their interest in providing the Services. Interested Consultants should provide information demonstrating that they have the required qualifications and relevant experience to perform the Services. A Consultant will be selected under the National Competitive Bidding Selection procedures set out in the IDB's: Policies for the Selection and Contracting of Consultants financed by the IDB and it is open to all eligible bidders as defined in these policies. Only Short-Listed Individuals will be contacted.

Consultancy: Cybersecurity Specialist Consultant
Consultancy Location: Nassau, The Bahamas
Reports to: Chief Medical Officer – Ministry of Health & Wellness

Main responsibilities:

The main objective of this consultancy is implementation of a cybersecurity framework with the level of robustness required to protect sensitive personal data captured, processed, transmitted and stored by digital health solutions (e.g., EMR, surveillance, telehealth).

The Consultant will:

- In conjunction with legal support provided by the Ministry of Health and Wellness, advocate for required modifications / improvements to the local legislative framework
- Own and execute the design, development, implementation and testing of the cybersecurity framework (governance, services / processes establishment, human resources, and technologies)
- Design, develop, implement and maintain processes, procedures, and guidelines to improve and increase the effectiveness of the cybersecurity initiatives and operations in the Ministry
- Develop and promote policies and procedures
- Design and execute a cybersecurity awareness program
- Conduct knowledge sharing sessions among other technical personnel on lessons learnt or new findings.
- Develop, implement and promote processes, procedures and guidelines to improve the Ministry's cybersecurity posture
- Assess adequacy of security tools and make recommendations for improvement
- Lead acquisition plan, purchasing and tendering processes
- Establish meaningful measures & metrics for team performance and SLAs/OLAs
- Plan for the business continuity and disaster recovery of operations.
- Coordinate with other department heads / stakeholders on technical matters.
- Produce monthly reports on progress etc.
- Serve as incident commander for high profile cyber incidents with legally sound forensic investigative method used in data breaches, litigation and law enforcement referrals
- Test and maintain incident response plans and processes to address existing and emerging threats
- Organize and maintain documentation for executive and targeted functions for table-top exercises
- Handle Incident Response (IR) retainers and coordinate third party engagements
- Ensure service level commitments.
- Coordinate cross-institutional activities in cybersecurity, including crisis management.
- Oversee and prioritize actions during the detection, analysis, and containment of an incident.
- Convey the special requirements of high severity incidents and work directly with the affected network to research the time, location, and details of an incident.

- Provide threat intelligence and context for an incident and investigate security incidents
- Undertake technology watch, the dissemination of information and other tasks when no incidents are ongoing
- Other duties as assigned

The successful candidate should have the following skills:

- **Education**: Bachelor's Degree in Information and Communications Technologies, Computer Science, Engineering or related field. Master' degree or higher is preferred. Candidates with learning and professional certifications in security such as CISA / CISSP / CISM / GCIA / GCFA / CEH shall have an added advantage.
- **Experience**: Minimum of 10 years of experience as a Cybersecurity Specialist. Experience working in Caribbean/Latin American Region is an advantage.
- **Languages**: Advanced writing, communication, and presentation skills in English
- **Core and technical competencies**: Excellent professional interpersonal skills. Results-driven, self-motivated, self-directed. Flexibility to adjust pre-agreed schedules. Ability to function well in a team-oriented work environment and on projects at various levels within organization. Deep understanding of cyber-security threats, vulnerabilities, controls and remediation strategies in mobile devices and telecommunications infrastructure enterprise environments. Knowledge of cybersecurity policies and regulatory controls, and overall risk profile of The Bahamas. Deep understanding of one or more cyber security frameworks (eg ISO27001, NIST CSF) and security related directives, regulations and international laws and information security risk assessments. Knowledge of risk assessments and cryptographic technologies. Knowledge of a range of IT platforms and technologies, systems and networks as well as typical gaps that could impact the ability of an organization to effectively detect and respond to cyber attacks. Experience with large scale and complex incidents of all types to include Advanced Persistent Threats, DDoS, insider, web and mobile applications, data ex-filtration etc. Ability to communicate complex and technical issues to diverse audiences, verbally and in writing, in an easily-understood, authoritative, and actionable manner. Flexible, exhibit initiative and have the ability to think strategically and innovatively.

Further information can be obtained by e-mail: MOHWPEU@BAHAMAS.GOV.BS. Submit all CVs and qualification documents must be submitted Re: **Cybersecurity Specialist Consultant** to E-mail: MOHWPEU@BAHAMAS.GOV.BS on or before 5:00 pm on **30 November 2022.**

Consultancy: Cybersecurity Analyst Consultant
Consultancy Location: Nassau, The Bahamas
Reports to: Chief Medical Officer – Ministry of Health & Wellness

Main responsibilities:

The main objective of this consultancy is implementation and support of a cybersecurity framework with the level of robustness required to protect sensitive personal data captured, processed, transmitted, and stored by digital health solutions (e.g., EMR, surveillance, telehealth).

The Consultant will:

- As directed, design, develop, implement, and maintain processes, procedures, and guidelines to improve and increase the effectiveness of the cybersecurity initiatives and operations
- Review current product detections to ensure they are performing to the standard
- Develop scripts to analyse and automate cybersecurity activities.
- Perform tasks to enable reduction of false positive detection.
- Analyse binary files to determine if they are legitimate or malicious.
- Address customer questions and concerns as it relates to detections.
- Assist with the design and execution of a cybersecurity awareness program
- Assist with the establishment of meaningful measures & metrics for team performance and SLAs/OLAs
- Support, and in some circumstances, lead planning for business continuity and disaster recovery of operations
- Produce reports on progress as required
- Develop a representative inventory of critical incidents
- Develop procedures to follow during an incident response
- Recommend updates to the incident response plan
- Maintain systems for discovering security incidents involving information resources
- Document security incidents in a tracking system
- Continuously improve the incident response program
- Identify and execute projects that improve our intrusion detection and incident response capabilities
- Perform vulnerability assessments and Penetration testing for Critical Information Infrastructure (CII)
- Develop and implement an ongoing risk assessment program targeting CII; recommend mitigation methods
- Work a flexible shift, which may include either working on a weekend, on a public holiday or at night.
- Other duties as assigned

The successful candidate should have the following skills:

- **Education**: Bachelor's Degree in Information and Communications Technologies, Computer Science, Engineering or related field. Candidates with learning and professional certifications in security such as CISA / CISSP / CISM / GCIA / GCFA / CEH shall have an added advantage.
- **Experience**: Minimum of 3 years of experience as a Cybersecurity Specialist. Experience working in Caribbean/Latin American Region is an advantage.
- **Languages**: Advanced writing, communication, and presentation skills in English
- **Core and technical competencies**: Excellent professional interpersonal skills. Results-driven, self-motivated, self-directed. Flexibility to adjust pre-agreed schedules. Ability to function well in a team-oriented work environment and on projects at various levels within organization. Deep understanding of cyber-security threats, vulnerabilities, controls and remediation strategies in mobile devices and telecommunications infrastructure enterprise environments. Knowledge of cybersecurity policies and regulatory controls, and overall

risk profile of The Bahamas. Deep understanding of one or more cyber security frameworks (eg ISO27001, NIST CSF) and security related directives, regulations and international laws and information security risk assessments. Knowledge of risk assessments and cryptographic technologies. Knowledge of a range of IT platforms and technologies, systems and networks as well as typical gaps that could impact the ability of an organization to effectively detect and respond to cyber-attacks. Experience with large scale and complex incidents of all types to include Advanced Persistent Threats, DDoS, insider, web and mobile applications, data ex-filtration etc. Ability to communicate complex and technical issues to diverse audiences, verbally and in writing, in an easily understood, authoritative, and actionable manner. Flexible, exhibit initiative and have the ability to think strategically and innovatively.

Further information can be obtained by e-mail: MOHWPEU@BAHAMAS.GOV.BS. Submit all CVs and qualification documents must be submitted Re: **Cybersecurity Analyst Consultant** to E-mail: MOHWPEU@BAHAMAS.GOV.BS on or before 5:00 pm on **30 November 2022.**

Consultancy: Junior Cybersecurity Analyst Consultant
Consultancy Location: Nassau, The Bahamas
Reports to: Cybersecurity Specialist – Ministry of Health & Wellness

Main responsibilities:

The main objective of this consultancy is implementation and support of a cybersecurity framework with the level of robustness required to protect sensitive personal data captured, processed, transmitted, and stored by digital health solutions (e.g., EMR, surveillance, telehealth).

The Consultant will:

- Support Cybersecurity activities with the testing and maintenance of the cybersecurity framework (governance, services / processes establishment, human resources, and technologies)
- Maintain processes, procedures, and guidelines to improve and increase the effectiveness of the cybersecurity initiatives and operations in the Ministry
- Support the execution of a cybersecurity awareness program
- Review current product detections to ensure they are performing to the standard
- Develop scripts to analyse and automate cybersecurity activities
- Perform tasks to enable reduction of false positive detection
- Analyse binary files to determine if they are legitimate or malicious
- Address customer questions and concerns as it relates to detections
- Develop procedures to follow during an incident response
- Recommend updates to the incident response plan
- Maintain systems for discovering security incidents involving information resources
- Document security incidents in a tracking system
- Continuously improve the incident response program
- Test and maintain incident response plans and processes to address existing and emerging threats
- Other duties as assigned

The successful candidate should have the following skills:

- **Education**: Bachelor's Degree in Information and Communications Technologies, Computer Science, Engineering or related field. Candidates with learning and professional certifications in security such as CISA / CISSP / CISM / GCIA / GCFA / CEH shall have an added advantage.
- **Experience**: Minimum of 3 years of experience in Information Technology. Experience working in Caribbean/Latin American Region is an advantage.
- **Languages**: Advanced writing, communication, and presentation skills in English
- **Core and technical competencies**: Excellent professional interpersonal skills. Results-driven, self-motivated, self-directed. Flexibility to adjust pre-agreed schedules. Ability to function well in a team-oriented work environment and on projects at various levels within organization. Knowledge of cyber-security threats, vulnerabilities, controls and remediation strategies in mobile devices and telecommunications infrastructure enterprise environments. Knowledge of cybersecurity policies and regulatory controls, and overall risk profile of The Bahamas. Knowledge of one or more cyber security frameworks (eg ISO27001, NIST CSF) and security related directives, regulations and international laws and information security risk assessments. Knowledge of risk assessments and cryptographic technologies. Ability to communicate complex and technical issues to diverse audiences, verbally and in writing, in an easily-understood, authoritative, and actionable manner. Flexible, exhibit initiative and have the ability to think strategically and innovatively.

Further information can be obtained by e-mail: MOHWPEU@BAHAMAS.GOV.BS. Submit all CVs and qualification documents must be submitted Re: **Junior Cybersecurity Analyst Consultant** to E-mail: MOHWPEU@BAHAMAS.GOV.BS on or before 5:00 pm on **30 November 2022.**