Government of Bermuda

Cabinet Office and Digital Innovation

Department of Information and Digital Technologies

Addenda

For

Managed Detection and Response Services (Restricted Request For Proposals)

Procurement No.: **BDA-CAB-IDT-SECURITY-2026-04**

Issued: **Friday May 15th, 2026**

Submission Deadline: **Thursday May 21, 2026 05:00:00 PM AST**

Addenda No. **001**

Addenda Type: **Questions and Responses**

The following addendum supersedes information contained in the solicitation document issued for this procurement to the extent referenced. This Addendum forms part of the solicitation documents and will be subject to all of the conditions set out in the contract conditions.

Questions and Reponses to Questions

Question 1	In relation to Appendix D, Section D.1.1 (Mandatory Technical Requirements – The Company), we would be grateful if the Government could confirm that, in the context of a joint submission under Section 1.3, the certification requirements at D.1.1.1 (SOC2) and D.1.1.2 (ISO 27001) may be satisfied by the combined certification posture of the prime contractor and the named delivery partner, rather than requiring both certifications to be held by a single legal entity.
Answer 1	D.1.1 - Project Team Qualifications: Joint submissions certifications can be combined. Please note that the certifications are ISO27001 OR SOC 2 (Type II).
Question 2	What form or format is expected for the certification — a standalone signed declaration, a section within the technical proposal, or another prescribed document?
Answer 2	D.1.1 - Project Team Qualifications: A standalone signed declaration of the certification is required.
Question 3	What evidence or supporting documentation is required to substantiate the certification (e.g. historical performance data, test results, vendor SLAs)
Answer 3	D.1.1 - Project Team Qualifications: Any documentation from Audits, policies and procedures would be required
Question 4	Are there defined evaluation criteria that will be used to assess the credibility or sufficiency of the certification?
Answer 4	D1.1 - Project Team Qualifications: Any documentation from Audits, policies and procedures would be required
Question 5	Bermuda’s public privacy materials under PIPA require assessment of overseas transfers, comparable protection, applicable foreign laws, third-party access, and cloud-service risks, including remote access from outside Bermuda and potential disclosure to third countries by court order or request against a cloud provider or parent company.

	For this MDR service, please clarify the Government's data-sovereignty requirements for citizen data, employee data, SIEM logs, EDR/XDR telemetry, MDR case records, forensic evidence, vulnerability data, email-security data, administrative audit logs, and threat-intelligence enrichment.
Answer 5	This additional information will be provided to the successful bidder
Question 6	Should any of these data classes be required to remain in Bermuda or in a Bermuda-controlled environment, including SIEM/log retention, MDR evidence storage, encryption keys, backup copies, administrative access, and regional SOC support access? If Bermuda-only hosting is not mandatory, please confirm the preferred or permitted jurisdictions, required safeguards, and whether on-island SIEM/evidence retention should be treated as mandatory, preferred, or optional.
Answer 6	This additional information will be provided to the successful bidder
Question 7	The RFP identifies existing investments in Cortex XDR, Microsoft Defender, NodeZero, Criminal IP, and Fortinet. To avoid unnecessary replacement costs, please confirm what is currently licensed, deployed, and operational. Specifically, does the Government have only Cortex XDR endpoint licensing, or also Cortex Data Lake, XSIAM, XSOAR, Broker VMs, log ingestion, extended retention, APIs, host isolation, and alert forwarding? For Microsoft, please confirm whether Defender XDR, Defender for Endpoint P1/P2, Defender for Office 365, Defender for Identity, Entra ID P1/P2, Sentinel, Logic Apps/playbooks, and relevant connectors are licensed and active. For this MDR service, please clarify the Government's data-sovereignty requirements for citizen data, employee data, SIEM logs, EDR/XDR telemetry, MDR case records, forensic evidence, vulnerability data, email-security data, administrative audit logs, and threat-intelligence enrichment. Should any of these data classes be required to remain in Bermuda or in a Bermuda-controlled environment, including SIEM/log retention, MDR evidence storage, encryption keys, backup copies, administrative access, and regional SOC support access? If Bermuda-only hosting is not mandatory, please confirm the preferred or permitted jurisdictions, required safeguards, and whether on-island SIEM/evidence retention should be treated as mandatory, preferred, or optional.
Answer 7	All stated investments are currently operational and licensed. Government only has Cortex XDR license. All additional information will be provided to the successful bidder

Question 8	Please confirm the preferred approach for consolidating alerts from Cortex XDR, Microsoft Defender, Fortinet, NodeZero, Criminal IP, email security, identity, cloud/SaaS, Windows, Linux, iSeries, Google Platform Services, and network infrastructure. Should proponents retain, augment, or replace any existing SIEM/SOAR platform such as LogRhythm, Sentinel, XSIAM/XSOAR, FortiAnalyzer/FortiSIEM, Splunk, Elastic, QRadar, or Wazuh? Also, which platform should be the authoritative system of record for incidents: Government ITSM, provider SOC platform, SIEM/SOAR, or another tool?
Answer 8	Cortex XDR will be the primary system for alerts. FortiAnalyzer will have the networking alerts. The authoritative system of records for incidents will be Government ITSM
Question 9	Please clarify which SLA set should govern the contract: the stricter 1-10-60 requirement in the Deliverables section, or the later Operational Expectations metrics showing MTTD under 100 minutes and MTTC under 5 hours. Please also confirm which containment actions may be pre-approved under MDR runbooks, including Cortex host isolation, account suspension, session revocation, Fortinet blocking, email purge/quarantine, endpoint file/process containment, and cloud workload isolation.
Answer 9	Section A.2.1 Appendix D - Strategic Speed of Detection and Containment: The 1-10-60 requirements should be used
Question 10	Would the Government support a hybrid model where on-site Bermuda-based Tier 1 SOC analysts are hired, vetted, trained, and mentored locally, while a regional 24×7 Tier 2/Tier 3 SOC provides advanced investigation, threat hunting, forensics, escalation, and after-hours coverage?
Answer 10	Yes
Question 11	Please also confirm whether augmentations should be included in the base bid or priced separately, including on-island SIEM/log retention, sovereign email security, expanded forensic storage, SOAR, local analyst training labs, and additional Cortex/Sentinel/LogRhythm/Wazuh capabilities.
Answer 11	Any augmentations should be priced separately

Question 12	What form or format is expected for the certification — a standalone signed declaration, a section within the technical proposal, or another prescribed document?
Answer 12	A standalone signed declaration of the certification is required.
Question 13	What evidence or supporting documentation is required to substantiate the certification (e.g. historical performance data, test results, vendor SLAs)?
Answer 13	Any documentation from Audits, policies and procedures would be required
Question 14	Are there defined evaluation criteria that will be used to assess the credibility or sufficiency of the certification?
Answer 14	Any documentation from Audits, policies and procedures would be required
Question 15	Section A.2.1 of Appendix D establishes the "1-10-60 Rule" with targets of MTTD within 1 minute, MTTA within 10 minutes, and MTTC within 60 minutes. The SLA table in Section B.6.3 sets MTTD at less than 100 minutes, MTTA at less than 15 minutes, and MTTC at less than 5 hours. Could the Government please clarify which set of values is authoritative for proposal pricing and contractual commitment, and whether the discrepancy is intentional or will be corrected by addendum?
Answer 15	Section A.2.1 Appendix D: The 1-10-60 requirements should be used
Question 16	Achievement of a 90% or higher completion rate for annual security awareness training across all 5,000 endpoints/users." Could the Government confirm that for this KPI should be the 3,000 user count rather than 5,000 endpoints, given that training completion is measured per user rather than per device?
Answer 16	Correct. This should be used for the number of employees and not number of assets.

Question 17	The RFP mentions 5000 endpoints and 3000 users. Can you confirm the user counts (inc. Google Workspace and/or O365 users) and Server counts (physical dedicated servers & VMs)? Full users: Google Workspace Users: O365 Users: Servers:
Answer 17	Full users: approx. 4000 Google Workspace Users: none under IDT control O365 Users: approx. 2330 Servers: approx. 500
Question 18	Can you provide more info on the Internet/Egress bandwidth at the locations that would be in scope? How many sites have >= 300Mbs? How many sites have >= 3Gbps? Have many sites have < 3 Gbps?
Answer 18	How many sites have >= 300Mbs: approx. 26 How many sites have >= 3Gbps: approx. 115 Have many sites have < 3 Gbps: approx. 141
Question 19	Existing Security Tooling & Platform Management Q1. [Ref: Section A.1 / B.5] For the referenced technologies within the RFP (Cortex XDR, Microsoft Defender, Node Zero, Criminal IP, Fortinet, Cisco), can the Government clarify: (a) which platforms are currently operational, (b) which are planned or future-state, and (c) which systems are considered the authoritative security monitoring platforms?
Answer 19	Please refer to Section A.1 /B.5: All tools are operational. Cortex XDR is the authoritative security monitoring platform
Question 20	[Ref: Section A.1] Are the current security solutions Government-owned and internally managed, vendor-managed, or operated under a co-managed/shared responsibility model?
Answer 20	Please refer to Section A1: Current security solutions are Government owed. The Fortinet tools are Government owned by co-managed with vendor

Question 21	[Ref: Section A.1] Is the successful bidder expected to: (a) monitor existing tools only, (b) fully administer and maintain the platforms, or (c) provide engineering, optimisation, health monitoring, tuning, and lifecycle management services as part of the engagement?
Answer 21	Please refer to Section A.1: (a) Monitor existing tools and make recommendations for improvements, (b) Internal Government staff will administer the platform, (c) Internal Government staff will manage these points but the security partner will provide recommendations as required.
Question 22	[Ref: Section A.1] Can the Government clarify whether active vendor licensing and support agreements already exist for all in-scope platforms?
Answer 22	Please refer to Section A.1: Vendor licensing and support agreements exist
Question 23	[Ref: Section A.1.1] Can the Government confirm the Cortex XDR licensing model currently in place (e.g., Cortex XDR Pro per endpoint), and whether the proponent will be granted full administrative access for alert triage, automated containment actions, and custom detection rule creation — as these are prerequisites for meeting the 1-minute MTTD and 60-minute MTTC targets?
Answer 23	Please refer to Section A.1.1: Confirmed. Cortex XDR is licensed and the proponent will have full admin access
Question 24	[Ref: Section A.1] If the Government retains ownership of existing tools, does the Government also require operational management and tuning services for those platforms under this engagement?
Answer 24	Please refer to Section: A.1: Internal Government staff will manage the existing tools
Question 25	Alternative & Supplementary Tooling Q7. [Ref: Section A.1.2] Is the Government open to bidders proposing supplemental or alternative security technologies where additional operational value, automation, or

	detection capability can be demonstrated — while continuing to leverage the existing platforms?
Answer 25	Please refer to Section A.1.2: For this RFP no alternate security technologies are required.
Question 26	[Ref: Section A.1.2] Would the Government consider a layered or hybrid operating model where the bidder's tooling integrates alongside existing Government platforms, rather than requiring a full replacement approach?
Answer 26	Please refer to Section A.1.2: Yes
Question 27	[Ref: Section A.1.2] If alternative tooling is permitted, who would retain long-term ownership and operational responsibility for licensing, administration, maintenance, and platform support?
Answer 27	Please refer to Section A.1.2: For this RFP no alternate security tooling are required.
Question 28	Q10. [Ref: Section A.2 / B.6] The SLAs in Section B.6 (Material Disclosures) appear to differ materially from the KPIs in Section A.2. For example, MTTD is stated as <100 minutes in Section B.6.3 versus 1 minute in Section A.2.1.1, and MTTC is stated as <5 hours in Section B.6.3 versus 60 minutes in Section A.2.1.3. Can the Government clarify which set of SLAs represents the binding performance targets for contractual purposes?
Answer 28	Please refer to Section A.2.1 Appendix D: The 1-10-60 requirements should be used
Question 29	[Ref: Section A.2] The RFP references the "1-10-60" detection and containment model. Can the Government clarify whether these are existing operational benchmarks currently being achieved, or target-state objectives expected from the successful bidder?

Answer 29	Please refer to Section A.2.1 Appendix D: The 1-10-60 requirements should be used
Question 30	[Ref: Section A.2.1.1] Can the Government clarify the intended interpretation of the MTTD requirement and whether this measurement applies to all ingested events, correlated alerts, or validated security incidents only?
Answer 30	Please refer to Section A.2.1.1: This refers to validated security incidents
Question 31	[Ref: Section A.2 / B.6] The RFP references operational metrics including MTTD, MTTA, MTTI, MTTC, and MTTR. Can the Government clarify how these metrics are currently measured, what tooling presently supports these measurements, and whether historical performance baselines are available for reference?
Answer 31	Please refer to Section A.2 /B.6: This is a new process in progress, so no historical performance baselines are available
Question 32	[Ref: Section A.2] Can the Government provide estimated monthly metrics for: (a) alert volume, (b) incident volume, (c) log/event ingestion rates, and (d) average escalation frequencies? These are essential for accurate SOC staffing and pricing.
Answer 32	Please refer to Section A.2: Approximately 150 alerts and 110 Incidents per month. 25 incidents per month are normally escalated.
Question 33	What is the Government’s estimated annual data ingestion volume into the SIEM?
Answer 33	Estimate is unavailable
Question 34	If that estimate is unavailable, could you please provide the quantities and types of all relevant technologies and log sources so that we can develop an accurate estimate?

Answer 34	Currently, the server and workstations logs will need to be sysloged to the SOC.
Question 35	In addition to the technologies listed in the RFP, are there any other technologies or platforms whose data must be ingested into the SIEM?
Answer 35	No. Currently all data is injested into Cortex XDR and then send out to the SOC for analysis
Question 36	Please specify scope and applicable products for the following where relevant: o Windows Servers o Linux Servers o Fortinet ecosystem (which products) o Cisco ecosystem (which products) o IBM iSeries / AS400 (which products) o Google Platform Services / Google Cloud (which products) o Cortex XDR o Microsoft Defender o NodeZero o Criminal IP
Answer 36	Additional information will be provided to the successful bidder.
Question 37	Is a FedRAMP or Assured Workloads compliant deployment required for the solution? If so, what compliance level is required (e.g. Moderate, High, etc.)?
Answer 37	FedRAMP and Assured Workload is not required
Question 38	Is the provider expected to supply the tooling and/or security awareness training platform required for the annual security awareness training program?
Answer 38	No. We have a Security Awareness program in place
Question 39	Are there any specific detection use cases that must be included in the solution from day one?
Answer 39	No

Question 40	Are there any specific response and automation use cases that must be included in the solution from day one?
Answer 40	No
Question 41	Are there any specific dashboard or analytics use cases that must be included in the solution from day one (e.g. MITRE ATT&CK, NIST, etc.)?
Answer 41	No
Question 42	What is involved in the Government’s formal CAB process
Answer 42	CAB meets weekly to review and approve changes to the infrastructure. No changes are allowed without CAB approval
Question 43	Section 6.1 references a “Service Desk”. Should this instead refer to a Security Operations Center (SOC)?
Answer 43	Please refer to Section 6.1: This refers to the SOC's Service Desk response times.
Question 44	For the remote resources that need vetting, what should we plan for regarding the Bermuda Police Service process, including, but not limited to: o Whether the individuals will need to travel to Bermuda for any part of the process o Whether we are expected to cover the cost of any international or third-party vetting, background checks, or certifications o Any documentation, identification, or notarization requirements o Expected timelines for completion and approval o Whether there are approved or preferred third-party providers for overseas vetting o Any renewal or ongoing compliance requirements for remote resources

Answer 44	Travel to Bermuda: In most cases, remote resources will not need to travel to Bermuda for vetting. The process can generally be completed from the resource's home location using certified documentation. If in-person attendance is needed for any specific case, we'll let the successful bidder know. Costs: Bidders are expected to cover the costs of vetting their own remote resources, including police certificates, notarisation, translations, courier fees, and any third-party provider charges. Documentation: The responsibility for ensuring that all required vetting documentation is properly completed, certified, and made available rests with the bidder. The bidder must ensure that formal documentation for each remote resource is prepared in accordance with Bermuda Police Services requirements and provided to the Bermuda Government IDT team in a timely manner. Any delays or deficiencies in documentation will be the bidder's responsibility to resolve. Timelines: Bidders should plan for roughly twelve to twenty weeks from submission of a complete application to final clearance. We'd encourage you to factor this into your mobilisation timelines. Third-Party Providers: There isn't a prescribed list of approved providers. Bidders are welcome to use reputable international background screening firms, provided they comply with Bermuda's Personal Information Protection Act (PIPA). Please flag your intended provider to us before engaging them. Ongoing Compliance: Clearances will need to be kept current throughout the engagement, with renewals typically every two to three years. Please let us know promptly if anything changes that might affect a resource's clearance status.
Question 45	Section B.6.3 lists two distinct metrics both abbreviated "MTTR": "Mean Time to Resolve (MTTR) variable 4 to 24 hrs" and "Mean Time to Recover (MTTR) less than 30 minutes." Could the Government please confirm that these are intended to be two separate KPIs? and if so, would you consider renaming the second metric (for example, "Mean Time to Restore Service" or "MTTRS") to eliminate the acronym collision or glossary that defines both? In addition, could the Government clarify the intended sequencing, given that in standard incident response lifecycles "Recover" follows "Resolve" rather than preceding it with a faster target?
Answer 45	Please refer to Section B - 6.3 Event Reaction & Resolution: Order would be Mean Time to Recovery followed by Mean time to Resolve

Question 46	"Achievement of a 90% or higher completion rate for annual security awareness training across all 5,000 endpoints/users." Could the Government confirm that for this KPI should be the 3,000 user count rather than 5,000 endpoints, given that training completion is measured per user rather than per device?
Answer 46	Please refer to Section 3.3: Governance & Awareness: Confirmed 3000 users for Security Awareness training and not the 5000 assets.
Question 47	Section A.3.1.1 (Virtual CISO and Security Governance) requires "Completion and executive approval of an updated 3-year Cybersecurity Strategic Roadmap within the first 90 days of the contract." Section A.5.3.1 (Risk Assessment and Strategic Roadmap) requires "Delivery of a 3-year Strategic Roadmap within 90 days, where 100% of initiatives are prioritized by Risk Reduction vs. Cost of Implementation." Please clarify whether these requirements constitute a single combined roadmap or two distinct deliverables, and if they are distinct, how each is intended to relate to or inform the other?
Answer 47	Bidders should plan for one consolidated roadmap that satisfies both requirements.

End of Addenda No, 001