Administration and Finance
Information & Technology Service

BOSTON PUBLIC HEALTH COMMISSION
REQUEST FOR PROPOSALS (RFP)
No. ITS-002-22

RFP - Managed Security Service Provider (MSSP)

Information Technology Services
Boston Public Health Commission
1010 Massachusetts Ave, 2nd Floor, Boston, MA
02118

ADVERTISEMENT

BOSTON PUBLIC HEALTH COMMISSION
INFORMATION TECHNOLOGY SERVICES

RFP — MANAGED SECURITY SERVICE PROVIDER (MSSP)
BID No. ITS-002-22

INVITATION TO INTERESTED, RESPONSIBLE AND COMPETENT PERSONS OR FIRMS ENGAGED AS AUTHORIZED RESELLER TO APPLY AND RESPOND TO A REQUEST FOR PROPOSAL FOR THE BOSTON PUBLIC HEALTH COMMISSION

The Boston Public Health Commission, acting through its Information Technology Services Department invites competent persons, firms, or corporations to apply for a request for proposal for the Managed Security Service Provider (MSSP) to perform such work in coordination with BPHC Officials as it relates to the enclosed RFP specifications.

Copies of the application and related contact documents may be obtained online at: www.bphc.org/RFP on or after (9/29/2021).

2 SEALED BIDS MUST BE SUBMITTED OR MAILED DIRECTLY TO: INFORMATIONAL TECHNOLOGY SERVICES OF THE BOSTON PUBLIC HEALTH COMMISSION, 1010 Massachusetts Avenue, 2nd Floor, Boston, MA 02118 and ONE ELECTRONIC BID TO BE SUBMITTED VIA EMAIL to Jeff Beers (jbeers@bphc.org). Applications must be in a sealed envelope. The front of the envelope must be labeled "**RFP- Managed Security Service Provider (MSSP)".**

Submission for such work will be accepted until 10/29/2021 at 5:00 pm EST.

LATE PROPOSALS WILL NOT BE ACCEPTED

TimeLine	
Wednesday, September 29, 2021	RFP announcement in The Boston Globe
Wednesday, September 29, 2021 by 10:00 AM EST	RFP available online at www.bphc.org/RFP at 5:00 PM EST
Monday, October 18, 2021 by 5:00 PM EST	Questions about the RFP via email to: Jeffrey Beers Director of Technology Services JBeers@BPHC.org Subject Title: RFP Questions - Managed Security Service Provider (MSSP)
Friday, October 22, 2021 by 5:00 PM EST	Response to questions posted at www.bphc.org/RFP by 5:00 PM EST
Friday, October 29, 2021 by 5:00 PM EST	Sealed Bids submit to: Boston Public Health Commission Information Technology Services 2nd Floor 1010 Massachusetts avenue Boston, MA 02118
Monday, November 1, 2021 by 5:00 PM EST	Submit responses via email to: Jeffrey Beers Director of Technology Services JBeers@BPHC.org Subject Title: RFP Submission – Managed Security Service Provider (MSSP)

PLEASE SUBMIT ALL CORRESPONDENCE AND PROPOSALS
VIA E-MAIL DIRECTLY TO THE PROCUREMENT CONTACT LISTED ABOVE AND INCLUDE ‘RFP-MANAGED SECURITY SERVICE PROVIDER (MSSP)’ IN THE SUBJECT LINE

I. INTRODUCTION

The Boston Public Health Commission a quasi-agency of the City of Boston. In general, technology plays a key role in delivering public health services, and maintaining an open relationship with residents, businesses and visitors to City of Boston. The Information Technology Services provides services such as technology planning and procurement, project management, network infrastructure and support services, helpdesk, data, telephone, GIS, cyber-security, administration to 1200+ employees and serving the community. The City of Boston is one of only a select few cities in Massachusetts that has a quasi public health services department. We are a quasi-entity that includes public health, and EMS services. ITS is staffed by 20 FTE employees currently organized within 5 teams: (a) user services, (b) systems administration (c) network administration (d) IT security, and (e) enterprise applications and business intelligence.

The Commission is also adopting an ITS Strategic Plan which would include Digital Strategic Plan (DSP). With the latter setting priorities, identifying the budget expectations, and scheduling projects and milestones that contribute to transforming its technology. Finally, the Commission is in the process of developing a Cyber Resilience Plan (CRP) which is an important part of establishing the strategy, methodical approach and evolving cyber-security for the Boston Public Health Commission. This CRP plan aligns with the City of Boston vision of reducing cyber-risk exposure, maturing cyber-security capabilities, technologies and systems, and effecting efficient regulatory compliance.

A) PROJECT OBJECTIVE:

The **Boston Public Health Commission** (BPHC) seeks a partnership with a Managed Security Service Provider (MSSP) / Managed Detection and Response (MDR) practitioner for 24/7/365 security monitoring and advanced security detection capabilities within a three plus option of two additional (3) +(2)-years, annually-renewed service contract. The selected vendor is expected to provide a cost-effective solution for the immediate and long-term. This contract will include a trial period with the potential for annual adjustments in scope of services and fees based on a mutually agreed budget. The contract will also include regular Customer status reports to BPHC: ITS staff.

B) OVERVIEW:

Security Operations (SECOPS) is the set of information technology services (ITS) resources, procedures, and tools that implement IT security and assure cyber-resilience within the operational (ITS Production) environment of the Commission. SECOPS typically includes the functions of:

- Security Quality Assurance (QA). Such as pre-Production software/system security testing, quality assurance and promotion into production operations,

- IT Asset Management, IT environmental "Security Hygiene," File/system Integrity Checking, and "Vulnerability Management." Such as discovery and management of hardware and software assets; implementing security configurations; patching; scanning; anti-malware; continuous vulnerability/exposure monitoring; security review and evaluation of proposed change controls impacting firewall rules; etc.,

- Management of Security Sensors, Tools and Systems/services. Including identity and access management (IAM), firewalls/firewall rule changes, intrusion detection/prevention systems (IDS/IPS), filters, gateways, event/system logs, data/file rights/data leak prevention (DLP) systems, user/entity behavior analytics (UEBA) sensors, remote access/VPN, security orchestration and automated response (SOAR) platforms, etc.,

- Connectivity Risk Management. This function may be called by any of several names, especially by one or more of its activities. The management of network connections themselves is addressed through Management of Security Sensors, Tools and Systems/services. Connectivity Risk Management is focused on managing the risk that is inherent from third-parties as a result of their providing services (within, remotely or in a hybrid production environment) or doing work on behalf of the organization. Vendor due diligence, auditing/compliance, risk management; governance and metrics of vendors' cybersecurity and third-party risk programs; and vendor hygiene monitoring are common examples of Connectivity Risk Management activities.

- "Threat Intelligence," "Security Monitoring," and "Incident Response" (IR).
  - Terms that apply to more than one related Functions:
    - **Security Visibility** is a general term used to describe the breadth and depth of Connectivity Risk Management, Threat Intelligence and Security Monitoring across the entire Production environment – on-premise, remote (account-related and hosted/Cloud) and hybrid – and up and down all layers of the Open Systems Interconnection (OSI) model.
    - **Situational Awareness** is another general term used for the fusion Of Strategic, Operational and Tactical/Technical Threat Intelligence, with Security Monitoring workflows and visualizations that enables predictability, targeted attention, and selecting and prosecuting the highest-payback course-of-action before, during and after a cyber-attack.
  - Threat Intelligence is the term used to describe those resources, processes and tools/platforms that collect/aggregate, correlate, and analyze strategic, operational and tactical/technical cyber threat data from multiple sources be they open source, dark web, and/or proprietary. Threat Intelligence data exchange protocols include but are not limited to: Structured Threat Information Expression (STIX), Trusted Automated Exchange of Indicator Information (TAXII), and Open Indicators of Compromise (OpenIoC).
    - **Strategic Threat Intelligence** typically refers to efforts focused on high-level shifts in the threat, exploit, and attack environments such as the rise of Advanced Persistent Threats.
    - **Operational Threat Intelligence** focuses more on details of exploit lifecycle (theoretical, real/ "weaponized," active) and applicability of a specific incoming real attack or focus of a threat actor (such as specific criminal elements' efforts against mobile banking in 2019 or around peak travel seasons)
    - **Tactical/Technical Threat Intelligence** includes focus and discovery of indicators of attacker methodologies, tools, and tactics and activity. Tactical/Technical Threat Intelligence is typically directly and immanently actionable while Operational and Strategic Threat Intelligence may not be as directly actionable or as immanently so.
  - Security Monitoring are those resources, processes and tools/platforms used to scrutinize - whether real-time and/or post-event – run-time computing: Cloud (SaaS, IaaS, PaaS), hyper-converged/virtual, perimeter, network, and server, endpoint device, sensors, and/or logs. It includes the day-to-day monitoring and interpretation of logs/events/sensor values/readings throughout the Production environment (internal as well as external) for possible security incidents (such as, unauthorized behavior, malicious hacks, denial of service (DoS), anomalies), and for trend analysis.
  - Incident Response, as a term, typically refers to either all five of the below lifecycle phases/processes, or one or more of the latter three components. The extent of IR is typically defined by the

organization’s Incident Response Plan, and the nature of the potential incident. IR case management involves activities across part or all of the IR lifecycle phases/processes:

- **Preparation:** Including (i) Security Hygiene, (ii) Integrity Checking, (iii) Vulnerability Management, (iv) Management of Security Sensors, Tools and Systems/services, (v) Threat Intelligence, (vi) IR and Crisis Communications plans and planning, and (vii) exercises (such as table-tops, “red/blue teaming,” and “capture the flag” drills, etc.).
- **Detection, Data Analysis, and Notifications:** Consists of (i) Threat hunting, cross- correlating, identifying and investigating suspicious events and activity to confirm existence of a cyber-incident, (ii) prioritizing the response based on impact and (iii) coordinating notifications of the technologists, business process owners, and Public Information Officer (PIO) throughout an active incident. This component may also be included within Security Monitoring.
- **Containment, Eradication, and Restoration:** Involves (i) Isolating affected systems to prevent collateral damage, escalation and to limit impact, (ii) pinpointing the genesis of the incident and quarantining, neutralizing and removing the threat, (iii) restoring systems and data when a threat has been mitigated. This component is sometimes called “prosecuting the incident.”
- **Cyber-Forensics:** The examination of digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital evidence, events they capture, and those involved. The preserved evidence as well as analysis may be used in Post-Incident Activities. Additionally, a hand-off between resources is also involved or addressed in an IR Retainer.
- **Post-Incident Activities:** Including (i) Recovery/rebuilding of systems and business operations, (ii) identifying improvements needed in Preparation, Security Monitoring, and Prosecuting the Incident, and then executing remediation projects to effect same, and may include (iii) administrative, insurance, legal or other civil actions.

- Depending upon the technologies in the Production environment, SECOPS may also extend to
  - Agile development platforms, processes and tools (SECDEVOPS), and/or to
  - Operational Technologies (OT) such as, Industrial Control Systems/Supervisory Control And Data Acquisition (ICS/SCADA), and Internet of Things (IoT) capabilities. OT is also called “cyber- physical” systems and infrastructure.

Generally speaking, MDR is tactical/technical Threat Intelligence (such as advanced threat detection and response also known as “threat hunting”) as well as threat remediation and restoration, and may also include security hygiene, and vulnerability management services. MSSP similarly may include Security Hygiene and Vulnerability Management services as well as Management of Security Systems/Services, includes operational and strategic monitoring of potentially applicable threats (within Threat Intelligence), and always includes some degree of Security Monitoring and IR.

C) SPECIFIC INTENTIONS:

1. The Commission expects to contract a trusted third-party for a comprehensive – delivering across the entire life-cycle of a security event (addressing the "before," "during" and "after"), and is conscientious, detailed, effective and efficient – unified MSSP/MDR capability whose response times will be consistent with the operational demands of the cyber-threat. And, who does so employing a strong professional and experienced SECOPS staff that:
    a. Owns the cyber-threat and collaborates with Commission from beginning to end. The MSSP/MDR is not permitted to subcontract any services without approval from the Commission employing an authorized contract amendment/supplement. MSSP/MDR will act as the Commission's single point of contact for any portion ofthe Services whether that is subcontracted and is responsible for resolution of all matters and escalations related to their use of subcontractors.
    b. Supplements and integrates well with, as well as will grow and mature over the long-term, the Information Technology Services (ITS) existing capabilities to detect and identify known and unknown threats. Does so (supplements, integrates, grows and matures ITS capabilities) using a staged approach wherein essentials are tackled in the first year, and enhancements and options are dealt with in out years.

    The Commission expects that the combined team – the MSSP/MDR vendor and BPHC-ITS staff – creates and fulfills the SysAdmin, Audit, Network and Security (SANS) Institute vision of SECOPS – namely: "prevents more, detects faster, and resolves more surgically."

2. It is also the Commission's intention to augment existing security tools and ITS processes through this partnership over the duration of the contract.
    a. All equipment and reliability standards shall conform to specifications as "new."
    b. For the initial installation and all subsequent installations of hardware over the duration of the term of the Contract, all equipment must be new and assembled for the first time from new components from the manufacturer. The Commission shall be the first user of the new equipment with no previous placements in the MSSP/MDR's or customer location as a demonstration unit including MSSP/MDR's offices.
    c. All equipment shall be guaranteed and warranted for the entire period of the engagement. The MSSP/MDR shall be prepared to exchange all equipment that proves defective during the Contract.

3. Thirdly, it is the Commission's intention to make use of a two-stage transition period. The transition period will consist of a typical vendor on-boarding project followed by an operational Proof-of-Concept (PoC) stage. A PoC is essentially a trial period using the artifacts produced from the on-boarding engagement that documents that a potential service can be successful. It allows the Commission and the Vendor to determine whether or not the relationship is a good fit for their needs,

while providing the vendor with the opportunity to make good on their claims. It also allows the MSSP/MDR to identify potential technical and logistical issues that might interfere with success and solicit feedback along the way from Commission components and stakeholders – IT Infrastructure and Operations, application and vendor coordinators, and auditors/regulators.

4. In addition to the Commission's intentions, said MSSP/MDR must meet and/or exceed the requirements set forth by (i) Commission's operational and technology partners and service providers (ITSP), including its Cloud ITSP (CSP), (ii) State and Federal laws and agencies, and (iii) regulators – comprising of, but not limited to:
    - Health Insurance Portability and Accountability Act (HIPAA),
    - Payment Card Industry Data Security Standard (PCI DSS),
    - Federal Department of Justice (US DOJ)/Criminal Justice Information Services Security Policy (CJIS),
    - Massachusetts Attorney General's Office
    - Massachusetts Operational Services Division (OSD)
    - Massachusetts Department of Public Health (DPH),
    - Massachusetts Department of Revenue (DOR),
    - Suffolk County, and
    - National Institute of Standards and Technology (NIST).

II. SCOPE OF SERVICES

Successful responder will be expected to provide to the Boston Public Health Commission a proposal including, but not be limited to, on each of the following:

1. Security Operations Functions.
   a. Vulnerability Management
   b. Strategic, Operational and Tactical/Technical Threat Intelligence
   c. 24x7x365 Security Monitoring
   d. Incident Response (IR) processes/activities, including but not limited to case management, across the IR lifecycle.

   The proposed solution must be scalable, modular and flexible in nature. Ideally, the solution should allow the Commission to be able to pick from the capabilities/offerings and build out or scale it back to fit its need. This will avoid wastage on bundled packages as the Commission may not want or need some of the capabilities in a bundled package. Details and limitations (such as gaps, options, etc.) of respondent's SECOPS capabilities within the list of functions must be identified and priced in the submitted proposal. For example, "We don't offer any Security QA capabilities." Or, "Our IR Cyber-forensics and Post- Incident Activities capabilities are offered on a Labor and Materials basis only at $ average blended rate."

   Proposals and demonstrations must additionally identify "how" the respondent conducts and delivers each proposed SECOPS capability. "How" the respondent handles IR resource hand-offs (such as with Commission SECOPS staff, and with separately arranged resources during IR Forensics and post-Incident activities), as well as any caveats or requirements around IR retainer (respondent's or separately resourced) must be addressed in the proposal. And, "how" respondent MSSP/MDR intends to align their capabilities with those of the Commission. Proposals must also specify delineation triggers of "when" alignment becomes a custom request and, then any applicable, price adjustments.

   In addition to the above and as an option, responders may address Agile development and/or Operational Technologies (OT): (i) functions, (ii) support services/resources, and (iii) offerings.

2. Service Management and Case Management Functions. In order to maximize the operational functions and relationship between the Commission and MSSP/MDR, Service Management and Case Management will include:
   a. **Predefined processes, RACI matrix, deliverables and SLAs**. A common set of defined processes (use-cases, playbooks, etc.) is required and these processes are expected to change with the emergence of novel threats, with organizational changes, and with changes in the operational and Production environments. A RACI matrix (Responsible, Accountable, Consulted and Informed) will include demarcated (i) leadership (supporting/supported) of SECOPS and threat ownership assignment as well as (ii) specific roles and responsibilities expectations and assignment for periodic reviews, daily operations, and casework. Effectiveness and efficiency SLAs (Service Level Agreements) will be employed to measure and control processes within mutually agreed timelines and quality levels on

deliverables and operations. Respondents shall provide information on their average response time as measured by how long it takes them to detect a threat to communicating it back to their customer. And, also how they address "alert fatigue" so that only meaningful alerts are being reported on to ITS Operations and Infrastructure staff.

b. **Augmentation** through collaboration, handoffs, and some interconnections and access between MSSP/MDR and Commission ITS Production environments (on-premise, Cloud-based, and hybrid). Augmentation relies upon visibility and extension: (i) a common operating picture into security- related routine and *in extremis* activities is paramount; (ii) neither organization operating solely within itself as a silo. Positive hand-offs (with articulated *veto* powers) will include an expectation of collective next steps, two-way communications and escalation. A portal and workflow engine, as a minimum, is anticipated for interconnectivity and mutual access. Case Management and service/trouble ticketing must be available through the portal and/or other means of interconnections and access between MSSP/MDR and the Commission. The portal itself must have: (i) role-based access control that integrates with the Commission's Microsoft Active Directory infrastructures, (ii) dashboards, (iii) tools, (iv) ticket/case information, (v) asset information, and (vi) reporting; and (vii) a single pain of glass (SPOG) that packages all the information gathered and provided in an easily digestible format for multiple audiences – CIO, ITS Directors, Information Security Officer, Privacy Officer, and auditors/regulators.

c. **Related security sensors, tools and systems and services**. This may include a prescribed and dedicated technology stack within Commission's ITS Production environments (on-premise, Cloud-based, and hybrid), as well as MSSP/MDR. The initial technology stack within the Boston Public Health Commission's current and Fiscal Year 2021 planned and budgeted set of same. Some minor changes may be discovered and proposed during MSSP/MDR onboarding and Proof-of-Concept (PoC) stages and will be evaluated and implemented, Commission resources permitting. The common technology stack is expected to change with the emergent threat, operational and Production environments, and will be planned (as much as possible) in coordination with the Commission budget cycle.

d. **Reporting**. During the onboarding and PoC stages, reporting and meetings will be constrained to those engagements themselves and their project management. After the MSSP/MDR onboarding and PoC stages, a monthly status meeting will, among other topics, review progress, performance metrics, and provide updates on trends. Performance metrics will, at a minimum, track fulfillment and compliance with the statement of work (SoW). This meeting will be in addition to and will make full use of reports and dashboards provided through the means of interconnections and access between MSSP/MDR and the Commission (portal and/or other). Additionally, after action reports will be used to identify and track progress in Post-Incident Activities, including (at a minimum) remediation of discovered gaps and errors in SECOPS and IR capabilities as well as restoral of Commission environments and systems/applications.

3. Relationship Governance Function. To ensure on-going and overall alignment, both parties must be aware of planned changes in the environments and operations/businesses. To that end, a regular governance protocol and cadence will be included in the delivery of SECOPS capabilities as well as Service Management and Case Management. The purpose of this protocol and cadence will be to update each party on current state, issues and trends in the relationship and to evolve the relationship over the life of the contract, including the end of the contract and the potential for termination and separation at that juncture. Governance activities will thus include, but not be limited to, preparations and support for the Boston Public Health Commission budget cycle.

III. SUBMISSION REQUIREMENTS

All proposals shall include the following information, organized as separate sections of the proposal. The proposal should be concise and to the point.

A. Contractor Identification:

Provide the name of the firm, the firm's principal place of business, the name and telephone number of the contact person and company tax identification number.

B. Contractor Qualifications and Capabilities:

Provide a narrative summarizing firm's qualification, and operational and financial capability/capacity to perform the work described herein. Respondents are encouraged to include past performance history and verifiable accomplishments of both the firm and staff identified to perform work under the resulting contract. Inclusion of information that speaks to firm's competitive differentiators and market reputation in the practice of cybersecurity and in selling the final deliverables in strongly encouraged.

Additionally, provide documentation on or responses to each of the following:

Financials
1. An audited copy of your company's financial statements for the past three (3) years. 2. Do you have venture capital or other funding supporting your MSSP/MDR services or your business as a whole? If so, please provide the names of investors and provide characterization of the investment, including objective (such as, strategic or financial), round (such as, Seed Money, Start-up, First-Round, Second-Round, Mezzanine, or Bridge), linkage (such as, loose or tight) and the degree (such as intensity of capital use and extent of integration). 3. What percentage of your security service revenue for the trailing twelve (12) months is from your MSSP/MDR services? What percentage is from security professional services or consulting? What percentage is from other revenue sources (such as hardware and software lease/sales)? 4. What percentage of your company's revenue is spent on MSSP/MDR research and development (R&D)?
Experience
5. How many years have you been providing MSSP and how many for MDR? 6. How many MSSP customers do you have and how many for MDR? 7. What are the past five (5) years contract renewal rates for MSSP and for MDR? 8. How many Government (Federal, State, Local or Tribal) Customers do you provide monitoring and security device management (MSSP/MDR Customers Only) services for?
Operations

9. Indicate the number of years your company has offered each of the proposed SECOPS functions in your MSS/MDR portfolio. Please provide the number of Customers and revenue for each of these services.
10. Indicate how many security operation centers (SOCs) you have, and where each one is located.

Staffing

11. Describe the process for screening and hiring your MSSP/MDR staff.
12. What percentage of your staff has security certifications (list the certifications), and what is the average number of years of experience they have in performing security monitoring or security consulting? What specific differences are there, based on geographic location and/or SOC, in terms of your staff's certifications and experience?
13. Identify the citizenship requirements per geographic location and/or per SOC.
14. Provide a sample job description and/or resume for each position within your security-monitoring staff. Include a summary of the technical expertise and/or special capabilities required for each position/job specification.
15. Explain the process of initial and ongoing training of your security-monitoring staff.
16. What is the average employment time of an MSSP/MDR analyst within your company?
17. What is the ratio of monitored customers to personnel?
18. What is the ratio of managed security devices to personnel?

Performance & Customer Relationship

19. Explain the expected working relationship, roles and responsibilities between your customer care or account manager and Commission's staff.
20. Describe your customer support tiers, including the capabilities and location of staff at each tier.
21. Please provide a sample Service Level Agreement (SLA).
22. Describe your problem resolution and escalation procedure.
23. Describe your SLA performance reporting.
24. Indicate your process for notifying us of your noncompliance with the SLA.
25. If Commission is not satisfied with the work performed, then what recourse does Commission have?

Future-proofing

26. Describe alliances with other companies you have that are related to your MSSP/MDR services, such as using a third-party software as part of your MSSP/MDR portfolio.
27. Will your services require the use of proprietary technology that Boston Public Health Commission must purchase or install? If so, please list all pertinent information related to this technology, including hardware, software, networking, middleware and database requirements. Include any associated costs as a separate line item in your Price Proposal. Identify which of the costs are an operating/on-going expense (OPEX) or a capital/one-time expense (CAPEX).
28. Provide details on support agreements. If a third-party software update is required, when does the SLA between you and the Boston Public Health Commission begin?
29. Does your firm have standard time frames, after which a given security product is no longer supported (life-cycles, product refresh cycles, end-of-service, etc.)? If so, then please describe the details, including proprietary and third-party software time frames.
30. Please provide an overview of your plans for continuity of service to Boston Public Health Commission.

Compliance

31. Describe all documented policies, procedures and audit requirements that will ensure maintaining the privacy and confidentiality of Boston Public Health Commission's data from the data of your other customers.
32. Indicate any industry certifications/attestations held by/for each of your SOCs hold, such as Statement on Standards for Attestation Engagements (SSAE) 16 Type 2, or International Organization for Standardization (ISO) 27001. And, please provide evidence.
33. What access to your internal-auditing documentation will you provide if our auditors, customers or business partners require this documentation in support of legal, regulatory or contractual requirements?
34. Indicate which of the following sets of requirements you meet/exceed or are certified as compliant. Cite referential issuances as applicable. Where you are not able to state positively, indicate so by the initials "TBD."

Operational/Technology Partners/Service Providers - State & Federal Laws/Agencies - Regulators	**Meet/Exceed**	**Certified**
• Health Insurance Portability and Accountability Act (HIPAA)		
• Payment Card Industry Data Security Standard (PCI DSS)		
• Federal Department of Justice (US DOJ)/Criminal Justice Information Services Security Policy (CJIS)		
• Massachusetts Attorney General's Office		
• Massachusetts Operational Services Division (OSD)		
• Massachusetts Department of Public Health (DPH)		
• Massachusetts Department of Revenue (DOR)		
• Suffolk County		
• National Institute of Standards and Technology (NIST)		
• Center for Internet Security Critical Security Controls for Effective Cyber Defense (CIS Top 20)		

C. <u>Customer References</u>:

Provide a minimum *of five (5)* Customer references. References should be Massachusetts or New England States cities or other similarly situated public sector entities where possible. Private sector entities may be included where the Customer is using the same or similar MSSP/MDR services as you propose for Commission and that are of similar size to the Commission. Provide the designated person's name, title, organization, address, telephone number, and the project(s) that were completed under that Customer's direction.

D. <u>Approach to Work</u>:

Provide a narrative describing the proposed approach and methodologies to be used to ensure the Boston Public Health Commission's objectives for this project are met. Include a *pro forma* project plan complete with key tasks, milestones and deliverable, as well a resource requirement. Include a sample of a similar plan prepared for another organization. For the purpose of preparing the *pro forma* project plan assume a notice to proceed date of October 31, 2021.

a. <u>Transition Plan</u>.

   a. **On-Boarding**. The vendor shall submit and follow a standard onboarding project management methodology, which will include the following:

I. Oversight / Governance Plan
II. Communication Plan
III. Risk Management Assessment and Plan
IV. As Is Assessment and Scope Management Plan
V. Detailed Project Timeline and Work Plan
VI. Plans for Initiation of each Service, including Knowledge Transfer
VII. Issue Escalation and Management Plan
VIII. Organization Change Management Assessment and Action Plan, and Reporting (as applicable).

b. **Proof-of-Concept (PoC)**. The vendor shall also submit, separately, a proposed Transition Plan. Proposed Transition Plan will include the vendor's plan for conducting a Proof-of-Concept (PoC)/trial period with the Commission. The PoC is a trial period that will address and demonstrate delivery of the selected set of potential SECOPS functions in accordance with Service and Case Management to the Boston Public Health Commission in a manner consistent with the proposed solution. **The best candidate shall agree to deliver a PoC at no additional cost to the Commission**. The terms, scope, and success criteria will be determined at a later date which will be agreed upon by both the vendor and the Commission.

The vendor will provide all necessary hardware, software, agents, training, configuration or other support with the exception of any installation or configuration on Commission systems. The vendor will collect, analyze, correlate, and report on data from identified systems/devices that are defined as "in-scope" as part of the PoC. The scope of devices (sources and sensors) will be limited to a specified number of pre-identified devices identified in the best candidate's SECOPS architecture designed to demonstrate the capabilities of the solution and the Commission's use-cases as applicable. BPHC- ITS system/device details will be provided to the vendor at or after time of selection as the best candidate. Systems/devices included in PoC should include certain minimal and mainstream devices. For example, including (but not limited to) the following:

- VMware Infrastructure and Hypervisor
- Servers – Domain Controller(s), Directory Servers and/or DNS servers
- Cloud Resources – Microsoft Azure, Office 365, other SaaS applications/providers, Azure Active Directory, Cloud Access Security Broker (CASB), etc.
- Backup Systems and Mounts
- Endpoint Security and Anti-malware
- Email and Web Filters
- Firewalls (FW)
- Virtual Private Networks (VPNs) Gateways and Concentrators, and VPN/Remote Access Monitoring and Control Systems
- Mobile Device Management (MDM), System Configuration and File Integrity Checkers/Monitoring Systems
- Ingress and Egress Load Balancers

- IDS/IPS and other Sensors, Logs and Alert systems
- Vulnerability scanners
- IT Operations Application and System Monitoring Utilities
- Phone System (VoIP) Servers
- For respondents including OT as an option:
    - **Building Management Systems (BMS)**
    - IP Cameras

c. **Knowledge Transfer.** The vendor shall also submit, separately, a proposed Knowledge Transfer Protocol. Knowledge transfer within the Transition period will address the Commission's roles and responsibilities within the selected set of potential SECOPS functions in accordance with Service and Case Management and will be tied to a payment milestone. Knowledge transfer will also be an ongoing process throughout the life of the contract driven by contract change control, and so will be assessed accordingly and tied to recurring payments.

b. **Proposed Solution**. Along with the above, companies are required to propose the most cost-efficient and manageable solution for the following as defined in this solicitation:

- Security Operations
- Service Management
- Case Management
- Relationship Governance
- Performance and Metrics Reporting

Ability to Deliver. Proposed Solution should demonstrate expertise with proposed services and activeness within each of the above functions and with leading security technologies (network, platform, firewall, IDS/IPS, logging, monitoring, STIX/ TAXII/OpenIoC, SOAR, etc.)

E. **Price Proposal**:

The proposal shall include pricing for all services. Pricing shall be all inclusive unless indicated otherwise on a separate pricing sheet. The Proposal shall itemize all services, including hourly rates for all professional, technical and support personnel, and all other charges related to completion of the work shall be itemized. **The Boston Public Health Commission anticipates a fixed fee for this service with any annual increases as agreed upon as part of contract negotiations upon selection.** All proposals shall be held firm for a minimum of 120 days after the proposal due date to allow adequate time for the Commission to consider each proposal and make an award. Price proposal must specifically include:

1. The name, title and appropriate contact information of the authorized negotiator or contract-signing agent if different from the contact person identified in the proposal.
2. Indicate and describe applicable licensing model(s) for your MSSP/MDR proposed functions and other related offerings.
3. Provide the base cost and pricing methodology.
4. Indicate and describe the pricing model for each SECOPS function proposed in your solution.
5. What process will determine if a change is within the original scope of the supplied

technology or a new feature? How will costs be determined?

6. As applicable, indicate details on the number of devices or data sources (e.g., IDS sensors, firewalls and servers) that are included in the cost.
7. Is pricing differentiated according to the sophistication of analytics used?
8. How are costs negotiated for upgrading or expanding services? How do we add devices or data sources without affecting pricing or services?
9. How would the purchase of new security devices, or upgrading our current devices, or vulnerability of products affect pricing?
10. Provide details on one-time costs and recurring costs.
11. Is there a minimum commitment for particular usage, total volume, and individual spend (or aggregate spend) in order to receive the rates and terms provided in the proposal? If so, explain.
12. Provide any licensing and warranty information for third-party products you may require the Commission to purchase in support of this service.
13. Indicate the discounts available, based on volume of services and contract length.
14. Indicate any consulting support hours built into your standard MSSP/MDR contracts.
15. Indicate hourly or daily pricing for additional consulting hours Commission can purchase during the MSSP/MDR engagement.

F. **Contract Terminations**:

If your organization has had a contract terminated in the last five (5) years, describe such incident. Termination for default is defined as notice to stop performance due to the vendor's non-performance or poor performance and the issue of performance was either (a) not litigated due to inaction on the part of the vendor, or (b) litigated and such litigation determined that the vendor was in default. Submit full details of the terms for default including the other party's name, address, and phone number. Present the vendor's position on the matter. The Commission will evaluate the facts and may, at its sole discretion, reject the proposal on the grounds of the past experience. If the firm has not experienced any such termination for default or early termination in the past five (5) years, so indicate.

IV. SELECTION CRITERIA

The following criteria will be considered, although not exclusively, in determining which firm is hired.

1. References: 15%

2. Costs: 25%

3. Capabilities and Qualifications: 50%

4. Proposal Itself: 10%

Responses will be evaluated by a selection panel composed of Commission (departmental) and City of Boston DoIT staff and other parties with expertise or experience in the goods and/or services being evaluated.

V. PAYMENT

Invoices: Invoices must be fully itemized, must include purchase order number and provide sufficient information for approving payment and audit. Invoices must be accompanied by receipt for services in order for payment to be processed. We prefer invoices to be emailed to accountspayable@bphc.org.

Payments: The Boston Public Health Commission will make payment to the vendor within 30- days of receipt of a correct and complete invoice.

VI. BOSTON PUBLIC HEALTH COMMISSION REQUIREMENTS

A. Vendor Obligation:

Boston Public Health Commission Requests for Bids, Requests for Proposals and Requests for Qualifications can be accessed on the Boston Public Health Commission's website, www.bphc.org under 'RFPs and BIDS'.

B. Addenda:

The Boston Public Health Commission may make changes to this Solicitation. Oral or other interpretations, clarifications or submittal instructions will be without legal effect. Any information modifying a solicitation will be furnished in a formal, written addendum. Addenda will be posted to the Boston Public Health Commission's web site and conveyed to those potential submitters.

C. Pre-Proposal Conference:

Proposals must be received via email on or before the date and time outlined on the front page of this RFP. Send your electronic submittal to:

JBeers@bphc.org

Name of Firm, Managed Security Service Provider (MSSP) (Subject Line)

Please submit one electronic copy in Adobe Acrobat PDF format, including all appendices. Submittals need to be limited to 9 MB in total email size. It is the Consultant's responsibility to verify the receipt of the submittal. Electronic verification will be provided upon request.
***Late proposals will not be accepted by the Boston Public Health Commission. Proposals received after the stated date and time will not be reviewed and shall be deemed non-responsive.**
All proposals submitted shall be valid and binding on the submitting firm for a period of ninety days following the Proposal submittal deadline and for any extension of time granted by the submitting firm.

D. Evaluation and Award Process:

An evaluation team will review each proposal and evaluate all responses received based upon the criteria listed herein. The Boston Public Health Commission may request clarifications or additional information, if needed. After the evaluation team individually scores each proposal, the scores are tallied, and the firms are ranked based on the scores.

A selection may be made based on the proposals and initial evaluation criteria alone.

Alternatively, the evaluation team may create a short list of the top ranked firms and invite the short-listed firms in for interview and/or check references. Scores for reference checks and interviews will be tallied and added to the short-listed firm's initial evaluation scores. Final selection will be based on reference checks and interviews.
The Boston Public Health Commission intends to select the Proposer who represents the best value to the Boston Public Health Commission and begin the negotiation and award process based on the evaluated scores.

The selected Vendor will be invited to enter contract negotiations with the Boston Public Health Commission. Should the Boston Public Health Commission and the selected firm(s) not reach a mutual agreement, the Boston Public Health Commission will terminate negotiations and move to the next highest ranked firm and proceed with negotiations.

The Boston Public Health Commission reserves the right to accept or reject any or all information in its entirety or in part and to waive informalities and minor irregularities and to contract as the best interest of the Boston Public Health Commission may require. The Boston Public Health Commission reserves the right to reject any or all Proposals submitted as non-responsive or non-responsible.

Procedure When Only One Proposal is received

In the event that a single responsive proposal is received, the Proposer shall provide any additional data required by the Boston Public Health Commission to analyze the proposal. The Boston Public Health Commission reserves the right to reject such proposals for any reason.

E. <u>Costs Bore by Proposers:</u>
All costs incurred in the preparation of a Proposal and participation in this RFP and negotiation process shall be borne by the proposing firms.

F. <u>Public Disclosure:</u>
Proposals submitted under this Solicitation will be considered public documents and, with limited exceptions, will become public information and may be reviewed by appointment by anyone requesting to do so following the conclusion of the evaluation, negotiation, and award process. This process is concluded when a signed contract is completed between the Boston Public Health Commission and the selected Consultant.

If a firm considers any portion of its response to be protected under the law, the vendor shall clearly identify each such portion with words such as "CONFIDENTIAL," "PROPRIETARY" or "TRADE SECRET" on each page for which the protection is sought. If a request is made for disclosure of such portion, the Boston Public Health Commission will notify the vendor of the request and allow the vendor not less than ten (10) days to seek a protective order from the Courts or other appropriate remedy and/or waive the claimed confidentiality. Unless such protective order is obtained and provided to the Boston Public Health Commission by the stated deadline, the Boston Public Health Commission will release the requested portions of the Proposals. By submitting a response, the vendor assents to the procedure outlined in this paragraph and shall have no claim against the Boston Public Health Commission on account of actions taken under such procedure.

VII. OTHER REQUIREMENTS

A. Insurance

The selected contractor will be required to maintain general liability insurance in the minimum amount of $2,000,000, automobile liability insurance in the minimum amount of $1,000,000 and a professional liability insurance policy in the amount of $2,000,000 to cover any claims arising out of the performance of the contract. The general liability and automobile insurance must name the Boston Public Health Commission, its officers, agents, volunteers and employees as additional insureds.

Technology Professional Liability Errors and Omissions Insurance appropriate to the Vendor's profession and work hereunder, with limits not less than $2,000,000 per occurrence. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by the Vendor in this agreement and shall include, but not be limited to, claims involving infringement of intellectual property, copyright, trademark, invasion of privacy violations, information theft, release of private information, extortion and network security. The policy shall provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring expenses with limits sufficient to respond to these obligations.

a. The Policy shall include, or be endorsed to include, property damage liability coverage for damage to, alteration of, loss of, or destruction of electronic data and/or information "property" of the Agency in the care, custody, or control of the Vendor. If not covered under the Vendor's liability policy, such "property" coverage of the Agency may be endorsed onto the Vendor's Cyber Liability Policy as covered property as follows:

b. Cyber Liability coverage in an amount sufficient to cover the full replacement value of damage to, alteration of, loss of, or destruction of electronic data and/or information "property" of the Agency that will be in the care, custody, or control of Vendor.

c. The Insurance obligations under this agreement shall be the greater of 1—all the Insurance coverage and limits carried by or available to the Vendor; or 2—the minimum Insurance requirements shown in this agreement. Any insurance proceeds in excess of the specified limits and coverage required, which are applicable to a given loss, shall be available to Agency. No representation is made that the minimum Insurance requirements of this agreement are sufficient to cover the indemnity or other obligations of the Vendor under this agreement.

B. Worker's Compensation Insurance:

A selected contractor who employs any person shall maintain workers' compensation insurance in accordance with state requirements. Sole proprietors with no employees are not required to carry Worker's Compensation Insurance.

VIII. RECOMMENDATIONS

A. Small Business and Disadvantaged Business Opportunities:

The Boston Public Health Commission encourages Certified Underrepresented Business Enterprises (CUBEs) to respond to this RFP. CUBE's are identified as; Disability-owned Business Enterprise (DOBE), Lesbian Gay Bisexual Transgender-owned Enterprise (LGBTBE), Minority-owned Business Enterprise (MBE), Small Local Businesses Enterprise (SLBE), Women-owned Business Enterprise (WBE), Veteran-owned Business Enterprise (VBE).