REQUEST FOR PROPOSALS (RFP)

Managed Security Service Provider (MSSP)

SOLICITATION #: 41

ISSUE DATE: April 26, 2021

BrightSpring Health Services
805 N. Whittington Parkway
Louisville, Kentucky 40222

Contents

1.0 GENERAL INFORMATION

1.1 Company Background

Headquartered in Louisville, Kentucky, BrightSpring Health Services and its subsidiaries (BHS) are the leading providers of complementary pharmacy and home and community-based health services for complex populations in need of specialized and/or chronic care. As the largest diversified home and community-based health and human services provider in the U.S., BHS has over 40 years of experience caring for "must-serve" client and patient populations characterized by significant needs, multiple conditions, complexity, high costs, and enduring challenges that are rest-of-life in nature. Through the company's family of brands, including pharmacy, home health, hospice, neurorehabilitation, behavioral health, family and youth, and workforce development, we provide comprehensive and specialized care and clinical services in 49 states, as well as Puerto Rico, the US Virgin Islands, and Canada, to over 60,000 customers, clients, and patients daily. Our mission is to help people live their best life. Since the company's inception in 1974, it has been a forerunner in the movement to provide home and community-based services for people with disabilities and other significant impairments, many of whom would be institutionalized otherwise.

BrightSpring possesses a leading, diversified national network that provides a full spectrum of services to a variety of high need populations in settings that reduce costs to states and payers. The company's client and patient base includes (i) individuals with intellectual and/or developmental disabilities ("I/DD"), (ii) individuals with behavioral challenges and disorders, (iii) aging individuals (seniors/elderly) or individuals with other disabilities (non-I/DD) who need assistance to continue living in their homes/communities, (iv) individuals with neuro-rehabilitation needs as a result of catastrophic injuries and illnesses (for example, acquired/traumatic brain injury and stroke), and (v) at-risk youth with either emotional, behavioral, and/or medical challenges and children with autism.

1.2 Contract Type

The Contract shall be an Indefinite Quantity Contract with Fixed Pricing, as described in each respective Task Order and Work Order to be issued under this Contract, as appropriate to the type of services being requested.

1.3 Contract Duration

The Contract shall start from the date of full contract execution by the parties ("Effective Date"). As of the Notice to Proceed Date, the Contractor shall perform all activities required by the Contract, including the requirements of this solicitation, and the offerings in its Technical Proposal, for the compensation described in its Financial Proposal. The Contract shall be for two (2) years from Contract Effective Date. ResCare, doing business as BrightSpring Health Services, at its sole option, may renew the term of the Contract through one (1) additional one (1) year renewal option for a total potential contract length of up to three (3) years.

1.4 Managed Security Service Provider (MSSP) Representative

The MSSP Representative will be the Single Point of Contact (SPOC) prior to the award of the contract.

Jason Conley
Enterprise Architect
BrightSpring Health Services
(859) 312-4045
jason.conley@brightspringhealth.com

1.5 Pre-proposal Conference

A Pre-Proposal Conference will not be held. However, questions can be submitted. Written questions from prospective contractors may be submitted via email. Emails must contain the Solicitation Number in the subject line. Please have all questions submitted to the Managed Security Services Provider (MSSP) Representative no later than May 10, 2021 by 5:00pm EST.

1.6 Procurement Method

The Contract will be awarded in accordance with; the U.S. federal government's competitive procurement practices and BrightSpring Health Services streamlined procurement policy.

1.7 Proposal Closing Date

All proposals must be received by the MSSP RFP Representative no later than May 17, 2021 by 5:00 pm EST. Requests for extension of this date or time shall not be granted. Contractors mailing Proposals should allow sufficient mail delivery time to ensure timely receipt by the SPOC. Multiple/alternative Proposals will not be accepted. Proposals received after the closing date and time will not be considered.

1.8 Preparation and Award

Proposals should be prepared simply and economically and provide a straightforward and concise description of the Contractor's Proposal to meet the requirements of this RFP. A Contract shall be awarded to the Contractor submitting the Proposal that has been determined to be the most advantageous to BrightSpring Health Services considering price and evaluation factors set forth in this RFP for providing the products/services as specified within. BrightSpring reserves the right to award in full or in part either portion of this RFP. Bidders should specify if they are participating in all aspects of the RFP or just a portion.

1.9 Duration of Proposal

Proposals submitted in response to this RFP are irrevocable for the latest of the following: 180 days following the closing date for submission of proposals, best and final offers (if requested), or the date any protest concerning this RFP is finally resolved. This period may be extended at the SPOC request only with the Contractor's written agreement.

1.10 RFP Revisions

If revisions to the RFP are necessary prior to the due date for Proposals, the SPOC shall provide addenda to all prospective Contractors that were sent this RFP, or which are otherwise known by the SPOC to have obtained this RFP. In addition, an Addenda to the RFP will be posted on the

Company's procurement vehicle. It remains the responsibility of all prospective Contractors to check all applicable websites for any addenda issued prior to the submission of Proposals. Addenda made after the due date for Proposals will be sent only to those Contractors that submitted a timely Proposal and that remain under award consideration as of the issuance date of the addenda.

Acknowledgment of receipt of all addenda to this RFP issued before the Proposal due date shall be included in the Transmittal Letter accompanying the Contractor's Technical Proposal. The acknowledgement of the receipt of addenda to the RFP issued after the Proposal due date shall be in the manner specified in the addendum notice. Failure to acknowledge receipt of an addendum does not relieve the Contractor from complying with the terms, additions, deletions, or corrections set forth in the addendum, and may cause the Proposal to be deemed not susceptible for award.

1.11 Cancellations

BrightSpring Health Services reserves the right to cancel this RFP, accept or reject any and all Proposals, in whole or in part, received in response to this RFP, to waive or permit the cure of minor irregularities, and to conduct discussions with all qualified or potentially qualified Contractors in any manner necessary to serve the best interests of the BrightSpring Health Services. BrightSpring Health Services also reserves the right, in its sole discretion, to award a Contract based upon the written Proposals received without discussions or negotiations.

1.12 Expenses

BrightSpring Health Services will not be responsible for any costs incurred by any Contractor in preparing and submitting a Proposal, in making an oral presentation, in providing a demonstration, or in performing any other activities related to submitting a Proposal in response to this solicitation.

1.13 Protests/Disputes

Any protest or dispute related to this solicitation or the Contract shall be subject to binding, private arbitration.

1.14 Contractor Responsibilities

The successful Contractor shall be responsible for rendering products and services for which it has been selected as required by this RFP. All subcontractors shall be identified and a complete description of their role relative to the Proposal shall be included in the Contractor's Proposal.

If a Contractor that seeks to perform or provide the products/services required by this RFP is the subsidiary of another entity, all information submitted by the Contractor, such as but not limited to, references, financial reports, or experience and documentation (e.g. insurance policies, bonds, letters of credit) used to meet minimum qualifications, if any, shall pertain exclusively to the Contractor, unless the parent organization will guarantee the performance of the subsidiary. If applicable, the Contractor's Proposal shall contain an explicit statement that the parent organization will guarantee the performance of the subsidiary.

While experience and documentation of a Contractor's parent company may be used to satisfy minimum qualifications, a parental guarantee of the performance of the Contractor under this Section will not automatically result in crediting the Contractor with the experience and/or qualifications of the parent under any evaluation criteria pertaining to the actual Contractor's

experience and qualifications. Instead, the Contractor will be evaluated on the extent to which ResCare determines that the experience and qualifications of the parent are transferred to and shared with the Contractor, any stated intent by the parent in its guarantee of performance for direct involvement in the performance of the Contract, and the value of the parent company's participation as determined by BrightSpring Health Services.

1.15 Mandatory Contractual Terms

By submitting a Proposal in response to this RFP, the Contractor, if selected for award, shall be deemed to have accepted the terms and conditions of this RFP and the Contract. The Contract shall reflect the requirements and provisions of the RFP. Any exceptions to this RFP shall be clearly identified as such in the Executive Summary of the Technical Proposal. The volume and severity of exceptions to the terms of the RFP, will be considered in the evaluation process, and may be grounds for finding a Contractor not reasonably susceptible for award.

1.16 Compliance

By submitting a Proposal in response to this RFP, the Contractor, if selected for award, agrees that it will comply with all federal, State, and local laws applicable to its activities and obligations under the finalized Contract. Indicate your intent submit an RFP by May 3, 2021 to the SPOC.

2.0 TIMELINE

Below are the targets dates and milestones for this RFP.

04/26/2021	RFP Submission to Field
05/03/2021	Intent to Respond to RFP
05/10/2021	Questions Due
05/13/2021	BHS Responses to Questions Due
05/17/2021	Submission Deadline
June 2021	RFP Award

Dates outlined are subject to change.

3.0 Contractor Qualifications

3.1 Past Performance

The successful proponent shall have relevant experience providing Managed Security Services Provider (MSSP) solutions to organizations of similar size and scope (50,000+ employees) with similar public sector and industry considerations.

4.0 SCOPE OF WORK

4.1 Objectives

The objective of this RFP is to identify a partner and develop a streamlined process to efficiently manage a preferred Managed Security Services Provider program. Though the intent is to identify one primary partner, BHS may extend to multiple partners, if warranted.

Our objective is to understand the full portfolio of services and options that you offer and to match supplier capabilities with BHS's requirements. BHS will focus on like-for-like offers. However, we also look for potential incremental expense reduction opportunities that might be obtained from alternative options of equal or greater quality and/or improvements to BHS's business processes.

BrightSpring Health Services employs a dynamic workforce, which includes approximately 50,000 direct support staff/caregiver, working in multiple locations, roles, and shifts. The successful partner will work with a group of key BrightSpring

4.2 Requirements

The Partner shall meet the requirements detailed within this section at a minimum, including samples of Service Level Agreement, invoice, and monthly reporting. In addition, selected vendor(s) will commit to Quarterly Business Reviews. The successful proponent will be expected to work closely with the organization's stakeholders. Below are several requirements and questions. Please provide clear responses to the below (preferred) or provide reference location within your proposal for BHS review.

4.2.1 General RFP Terms and Conditions

The successful proponent will be expected to work closely with the organization's stakeholders to:

- Assign a dedicated account manager or single point of contact for day to day management, invoicing, and escalations.
- Meet for monthly checkpoints to assess success, address any gaps or technical issues.
- Present results/reporting to key stakeholder and leadership groups as required.
- Ensure capability of supplying product and services in sufficient quantity, as needed to meet demand.

4.2.1 Managed Security Services Provider (MSSP) Solution Requirements

BHS seeks a Managed Security Service Provider (MSSP) solution that can provide monitoring and response capability to compliment the Security Group. The solution will provide 24x7 detection and response services to protect customer assets against risk.

- Ensure MSSP roadmap that BHS can layer in services overtime as existing solution expire or are deprecated.

4.2.1.1 Company Technical Profile

- Desktop OS Types: Windows 7, Windows 10, and Apple Mac
- IoT Types: various versions of iPads & Android devices
- Multiple Server OS Types: Windows, Linux, and Unix Variants
- Multiple Firewall Vendors: FortiNet, Palo Alto, and Cisco
- Multiple Database Vendors: Microsoft, IBM, and Oracle
- Locations: 2,500+ (650 Core Offices, 1850 Small Sites)
- Servers: 2,000+
- Employees: 20K Knowledge Employee, 40K Field Employees
- 15K Endpoints
- Two Data Centers
- Multiple SIEM Platforms
- Multiple IAAS, PASS, and SAAS services
- Multiple Compliance Requirements (PCI, HIPAA, HITRUST, SOX)

4.2.1.2 Current Solutions

- 1 On-Premise SIEM (25% Coverage)
- 1 Hybrid SIEM (20% Coverage; On-Premise collectors & agents + cloud hosted SIEM)
- 1 Hybrid Vulnerability Management Service (On-Premise and Cloud Scanners + Managed Reporting)

4.2.1.3 Common Solution Criteria

Confirm that you can meet the criteria identified or answer the questions outlined in each of the subsections starting with 4.2.1.3.1 and ending with 4.2.1.3.14.

- **Qualifications and Staffing**
- **Implementation and Service Methodology**
- **Security Event Monitoring**
- **Security Device Management**
- **Security Information Management**
- **Advanced Analytics and Capabilities**
- **Vulnerability Management Services**
- **Incident Response**
- **Operational Technology Capabilities**
- **Internet of Things Capabilities**
- **Portals, Reports and Dashboards**
- **Service Management**

4.2.1.3.1 Qualifications and Staffing

- Indicate how many MSS customers you have.
- Please provide a list of MSS customers in BHS's industry or market sector. This should include three or more references of companies using your service that are of similar size to BHS.
- Indicate the total number of employees in your company, and the number of employees responsible for MSS delivery.
- Please describe the relative distributions of employees in your MSS company providing delivery, project management, customer service, and how these employees are geographically distributed.
- 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? Are there any differences based on geographic location and/or SOC in terms of your staff's certifications and experience?

- Please describe the citizenship requirements per geographic location and/or per security operations center for governance purposes.
- Provide a sample job description and/or resume for your security-monitoring staff. Include a summary of the technical expertise and/or special capabilities required.
- Describe the process for screening and hiring your MSS staff.
- Explain the process of initial and ongoing training of your security-monitoring staff.
- What is the ratio of monitored security devices to personnel? What is the ratio of managed security devices to personnel?
- What is the average employment time of an MSS analyst within your company?
- Describe strategies to maintain consistency in staffing and managing turnover for the customer.
- Describe your customer support tiers, including the capabilities and location of staff at each tier.
- Indicate any industry certifications/attestations your security operation centers hold, such as Statement on Standards for Attestation Engagements (SSAE) 16 Type 2, or International Organization for Standardization (ISO) 27001. If so, please provide evidence.

4.3.1.3.2 Transition and Service Methodology

- Provide a brief overview of your transition approach
- Describe how you address transitioning from one provider to your service.
- Explain your anticipated timeline for transition to your service.
- Please, provide a sample transition plan
- Describe your methodology to provide education to BHS partner teams on the processes and methodologies that will need to be adopted to maximize value of the service

4.3.1.3.3 Mergers & Acquisitions Approach

- Provide an overview of your experience working with a company that is driven by mergers & acquisitions
- How do you handle Day 1 management of the services versus long-term integration plans?
- How do you address Line of Business (LOBs) that will remain separate due to financial and regulatory reason?
- Do you offer assessment services that can help close the loop as new acquisitions or potential mergers to work a partner during the process?
- Describe your experience providing a consolidated service despite multiple companies, LOBs, varying regulatory requirements, and constantly changing landscape

- Please, provide your experience with customers of similar complexity and size.

4.3.1.3.4 Implementation and Service Methodology

- Provide a brief overview of your managed security services and any supporting products.
- Are your SOCs staffed 24/365? Describe your approach to supporting 24/365 remote security event monitoring and device/agent management, including any use of "follow the sun" staffing.
- Describe the architecture of your MSS delivery capability, including elements in your SOC, data center (on your premise, colocations, and private and public cloud services), network and our premises, as well as the centrally delivered log management, analytics and portal tiers, and capabilities for collecting event logs and data from other locations (e.g., software as a service [SaaS] and infrastructure as a service [IaaS]). Provide example architectural diagrams and descriptions. Indicate where there are any regional differences in architectures or technologies used. Finally, include and identify any elements that are delivered by third-party partners.
- List the primary tools used to deliver your services. Describe the function or service offering they support, and indicate whether they are proprietary, commercial, or open source, for example, log collection, log management and storage, analytics, reporting, case management and workflow, and incident response.
- Explain how these services, and any supporting products will use or interface with products BHS has in place. Ensure that you include details on how you intend to connect to BHS's infrastructure to provide support.
- Will your services require the use of proprietary technology that BHS 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 quote.
- Explain how you use external data (e.g., threat intelligence feeds) to analyze potential threats to BHS's environment and describe what access to this BHS will have.
- Please provide an overview of your customer notification and escalation process. Include details on how often a customer is notified of a security event, and on the methods of notification.
- Describe integration capabilities with enterprise directories, and configuration management databases (CMDBs ServiceNow. Explain how these integrations support the delivery of your services.
- Indicate how your services will be delivered in our internal virtual (or cloud-based) infrastructure. Include details about how the services will accommodate the scaling (larger or smaller) of the virtual or cloud-based environment, the implications for technology deployment to support monitoring, and related contractual, license or cost implications.
- Indicate how your services will be delivered in an external or public cloud infrastructure. Include technology and contractual or licensing requirements related to provisioning,

ongoing monitoring, and de-provisioning of services to the cloud infrastructure. Describe the process to add or remove monitoring sources in a public cloud infrastructure.

- Describe your support for monitoring security or other related events from SaaS providers. List which providers can be monitored natively. Do you require and/or support cloud access security brokers (CASBs)?
- Explain how you will complete an initial assessment, and how you will establish a baseline security level. Include specifics on your implementation timeline; infrastructure requirements; data transfer, data storage and segregation, and backup systems; and encryption standards.
- Describe the frequency and opportunities for continuous improvement during the implementation phase.
- Please provide an example of how your services detected and addressed a recent security incident.
- Explain your methodology for detecting custom or targeted attacks directed at our users or systems.

4.3.1.3.5 Security Event Monitoring

- Indicate the capabilities of your services to monitor our firewall, intrusion detection system (IDS), intrusion prevention system (IPS), vulnerability data, etc.
- Please describe the use of signature-based and correlation rules.
- Explain your ability to analyze this data and to provide real-time event correlation between data sources, and real-time alerting of security incidents and system health incidents.
- Explain how your company keeps signatures/rules updated.
- Explain support for the creation and management of customized correlation rules. Explain the capabilities available to our staff for doing so. Describe any limitations, such as data sources, age, and query frequency.
- Explain your ability to analyze this data to identify when changes in behaviors of users or systems represents risk to our environment.
- Explain your methodology for reducing false positives and false negatives and for classifying security-related events that represent a risk to BHS.
- Describe how false positives are managed, and how your company will incorporate false positive feedback from BHS.
- Describe the typical workflow and process that occurs when the security analytics detects a security event, beginning with how that is presented to a SOC analyst for evaluation through the triage, validation, prioritization, and customer alerting/notification process. Indicate where activities are automated versus manually performed by analysts.
- Indicate the level of interaction and support that our staff can expect from your security analysts to assess, investigate, and respond to incidents.

4.3.1.3.6 Security Device Management

- Indicate the capabilities of your services to manage our security technologies in scope. Including but not limited to: Data Loss Prevention technology, firewall, IDS, IPS, vulnerability assessment, web security and messaging security technology, and identity and access management systems.]
- Explain your process for updating software to include signature updates and system patches. How do you ensure that this is done in a nonintrusive manner to your customers?
- For each management service, indicate your change management process and your willingness to modify to meet our requirements.
- For device management services, indicate whether changes are reviewed to assess increased risk, exposure, or the effects on capacity.
- Describe the contractual and cost implications of changing devices from real-time monitoring to collection or reporting (or vice versa).

4.3.1.3.7 Security Information Management

- Indicate the data sources supported for log collection, reporting and retention. Can logs be collected from any source? Describe the collection methods (e.g., forwarded syslog, Windows Management Instrumentation [WMI], local forwarding agent).
- Will all of our raw event logs and data be collected and forwarded to your platform for storage? If no, describe the variation and options for full log event retention (if applicable).
- Will our logs be compressed and encrypted in transit, and is it a guaranteed delivery via a store and forward type of solution? If so, please describe.
- Indicate any limitations to your log collection capabilities, such as peak event rates, volume, or sources.
- Explain the capabilities that allow our staff to search and browse original log data. Describe any limitations to this capability.
- Explain the capabilities of our staff to create and modify reports based on collected log data. Indicate any limitations, such as number of reports, complexity of queries and age of data.
- Indicate your standard data retention policies and ability to modify them to meet our requirements.
- Is there a minimum and maximum of times that log retention can be offered? Describe what is actively available versus what is kept offline. If 366 days of storage is required, how will that be priced for BHS?
- Specify how your company approaches the online/warm/cold types of storage.
- What is the process for adding additional log sources to the scope of service? Include the implications for deployment architecture, integration costs and ongoing costs.

4.3.1.3.8 Advanced Analytics and Capabilities

- Describe your ability to implement watch-lists, both those you define, and those we define.
- What technologies are used to enable advanced analytics?
- How do you profile and monitor entity and user activities and behaviors (e.g., user and entity behavior analytics [UEBA])? Describe specific approaches and models/algorithms used, including any regional variations.
- Describe your use of predictive analytics, including specific approaches and models/algorithms used, and any regional variations.
- Describe any specific network monitoring and/or network forensics features, capabilities, or offerings to detect advanced, targeted attacks.
- Describe any specific payload analysis features, capabilities, or offerings to detect advanced, targeted attacks.
- Describe any specific endpoint behavior analysis and/or endpoint forensics features, capabilities, or offerings to detect advanced, targeted attacks.
- How is streamed data with real-time advanced analytics supported? Describe and list any technologies supported (e.g., Kafka, NiFi).
- Describe the data and threat visualization capabilities available to us via the portal.
- Describe any managed detection and response-type service offerings (e.g., managed endpoint detection and response, threat hunting, remote response, and containment).
- Explain if/how you leverage big data platforms for the collection, retention, and analysis of large volumes of operational and security data for analysis.
- How are big data platforms used to support the collection/analysis of network and endpoint data? Does your company require the deployment of its own network data collection/analysis solution? Can your company use BHS's EDR solution, or is it mandatory that BHS use your company's EDR solution?

4.3.1.3.9 Vulnerability Management Services

- Describe the service capabilities to monitor vulnerability scans internally and externally with the organization.
- Indicate the technologies used to conduct scans, both commercial and open source.
- Provide details on your methodology for collecting and analyzing vulnerability and asset data (e.g., configuration) from all sources in scope
- Describe the process by which vulnerabilities are triaged and prioritized prior to reporting, including the integration of previous scan results and actions carried out. Is the vulnerability management (VM) data also used in the same fashion for MDR services, if applicable?

- Describe integration capabilities with vulnerability assessment data, including how the vulnerability data is used in support of triaging and investigating potential security events, and alerting and reporting capabilities.
- How can vulnerability scans be scheduled, initiated/managed via your MSS portal? How are results viewed in the portal?
- Indicate your ability to intake results from scanning devices already situated in the BHS **virtual perimeter**.
- Indicate the frequency your MSS can scan our environment.
- How frequently is the vulnerability database updated, and what are the data sources used for that?
- Indicate the application-specific scanning that you carry out as part of your VM services.

4.3.1.3.10 Incident Response

- Are there any remote and/or on-site incident response (IR) activities included as part of the service? If so, describe the services provided, including specifics on what is included in the core services versus what is available as an additional service/offering.
- Do you provide incident response activities, including breach response services, via an optional retainer? If so, describe the packages, service-level agreements (SLAs), costs and included services. Do you offer proactive services as part of a retainer? Which services are able to be delivered remotely (both proactive and reactive), and which require your staff to be physically on our site(s)?
- Do you provide any IR activities outside of a retainer, such as a "just in time" type services?
- Do you assist with creating specific IR use cases and maintaining a run book? If so, describe how this is achieved.
- Describe any self-service features for incident response provided via the portal (e.g., automated malware analysis, custom signature, or correlation rule implementation).

4.3.1.3.11 Operational Technology Capabilities

- Describe your support for Operational Technology (OT)/Supervisory Control and Data Acquisition (SCADA)/Industrial Control System (ICS) environment monitoring.
- What OT security technologies do you support for security monitoring and management?
- Describe existing or planned partnerships with OT/SCADA/ICS vendors.
- How many customers do you have where you are monitoring OT devices?

4.3.1.3.12 Internet of Things Capabilities

- What notable Internet of Things (IoT) partnerships do you have?
- Provide some examples of the IoT use cases you support?
- How many customers do you have where you are monitoring IoT devices?

4.3.1.3.13 Portals, Reports and Dashboards

- Indicate any local language support or localization features in your portal and note any regional differences.
- Describe the information provided by and features available through the web-based portal or console associated with your services. Describe the underlying technology (HTML5, Flash, JavaScript, etc.) based on BHS's previously outline technical profile. Also, include details on your support for role-based access control (RBAC), customization of screens and data presentation, predefined correlation rules, and predefined reports.
- Indicate whether all services and MSS features, including those delivered by partners, will be available via a single portal, regardless of region or part of business delivering the services.
- What authentication and identity management system does your portal use? Do you provide support for federated identity management (FIM)?
- How does the portal provide us access to external threat intelligence feeds, in addition to BHS's own threat intelligence feeds?
- Describe support for bidirectional threat intelligence using open standards, such as STIX/TAXII/OpenIoC.
- Can BHS access, and search log event data via your MSS portal?
- Describe user roles available to us for your MSS portal (e.g., administration, view/report, etc.). Describe how user access to data and reports can be restricted based on role and group.
- Describe any real-time chat/instant messaging and/or live video interaction available with your SOC staff.
- Describe any integration capabilities with third-party service desk and ticketing tools and services. How is this achieved (e.g., email, application programming interfaces [APIs], etc.)? Also, indicate if you provide single-direction or bidirectional support, and whether the integrations are subject to additional costs.
- Describe the portal capabilities to enable our staff to create, update and close tickets.
- Describe how much visibility your company provides on the tasks of the workflow. Consider how many alerts there are, your staff level (e.g., Level 1, Level 2, Level 3), and how long they are on a particular phase in the process.
- Is there a smartphone/tablet application available? If so, briefly describe the supported platforms and functionality.
- Describe operational, regulatory, and executive reporting capabilities.
- Indicate the number of predefined reports, including specific regulatory and compliance items supported, that will be available for BHS. Please provide examples.
- Explain how report data can be exported to or used by an external report writer or risk dashboard.

- Explain the capabilities for our staff to create customized, ad hoc queries and reports. Describe any limitations to ad hoc query or report generation, including data sources, data age and query frequency.

4.3.1.3.14 Service Management

- Explain the expected working relationship, roles, and responsibilities between your security staff and BHS's security staff.
- Indicate the frequency of meetings or teleconferences to review performance, issues, threat environment and responses. Explain the types of analyst and account management support provided during those meetings.
- Indicate device/agent management, and real-time event management notification service levels. Explain how they are measured, and how they will be communicated to BHS.
- Provide a sample of an SLA as outlined in the scope, in addition to the service onboarding and delivery phases.
- Describe your problem resolution and escalation procedure.
- Describe your SLA performance reporting. If applicable, indicate whether these methods are used in some or all regions.
- Does your company have standard time frames, after which a given security product is no longer supported? If so, please describe the details, including proprietary and third-party software time frames.
- Please provide details on support agreements. If a third-party software update is required, when does the SLA between you and BHS begin?
- Describe the process for adding services or new technologies. For example, assume that BHS adopted a deep-packet-inspection firewall technology — how would this be supported and incorporated into an SLA?
- What process will determine if a change is within the original scope of the supplied technology or a new feature? How will the costs be determined?
- What access to internal-auditing documentation will you provide if our auditors, customers, or business partners require this documentation in support of legal, regulatory, or contractual requirements? What is your process for requesting documentation? What are the time frames to which you will commit for producing documentation?
- Describe the process should BHS have a complaint.
- Indicate your process for notifying us of your noncompliance with the SLA, and vice versa.
- Describe the remedies available to BHS should you fail to meet any SLAs. Explain any regional variations to remedies.
- Outline early termination penalties and charges. Describe how the costs are calculated to extract all captured data to be moved to another MSSP, if applicable?
- Describe how BHS's data would be obtained during the termination process.

- Describe how BHS's data (including data generated by your company about security events and incidents affecting BHS will be governed and protected in transit. Consider this from a technology perspective, as well as via processes and procedures. How will the treatment of BHS 's confidential data assist with better job performance (e.g., creating internal architecture and topology maps)?
- Provide examples of how your company has met specific regulatory or statutory requirements to the data within specific geographic or political boundaries. Provide answers only for regions or specific countries where there is concern.

MSSP Roadmap Criteria
MSSP is an evolving capability, so the winning company will present a roadmap that provides additional features over 12-18 months.

4.2.3 Pricing

Pricing quotes will remain in effect for 60 days, following full RFP submission. Agreed upon pricing will be firm for the duration of the contract. Should a price increase be warranted, the contracted company will provide an addendum to BrightSpring Health Services 30 days prior to the effective date, detailing justification for the increase.

Invoices should be consistently accurate and reflect true charges incurred by BrightSpring Health Services. Failure to provide accurate invoices will result in a written warning provided by BrightSpring Health Services and may ultimately result in termination of the contract.

- Please provide the name, title and appropriate contact information of the authorized negotiator or contract-signing agent.
- Indicate and describe the licensing model(s) for your MSS offering.
- Indicate and describe the pricing model for managing/monitoring virtualized security devices or log sources.
- Provide the base cost and pricing methodology.
- Please indicate details on the number of devices or data sources (e.g., IDS sensors, firewalls, and servers) that are included in the cost.
- Is pricing differentiated according to the sophistication of analytics used?
- How are costs negotiated for upgrading or expanding services? Can we add devices or data sources without affecting pricing or services?
- How would the purchase of new security devices (or upgrading our current devices) affect pricing?
- Provide details on one-time costs and recurring costs.

5.0 PROPOSAL SUBMISSION DETAILS

5.1 Submission Instructions

The Contractor shall submit 2 copies as well as electronic copies (pdf and an editable version) of the Managed Security Services Provider (MSSP) proposal to the SPOC listed in Section 1.4 on or before the Due Date noted in Section 1.7 of the RFP.

5.2 Volume 1 - Solutions Proposal

The Proposal shall include all items detailed below. In addition to the following instructions, responses in the Contractor's Proposal must be able to be directly mapped to the RFP.
The Solutions Proposal shall include the following documents and information in the order specified as follows.

- Title Page and Table of Contents
- Claim of Confidentiality
- Executive Summary
- Bid Proposal
    - Solution Proposal
    - Licensing & Pricing Schedule
        - With your bid sheet as a base for possible licensing options, but not limited to
            - Bundled Licensing Options for MSSP services
            - A la Carte Licensing for individual services
        - Each major aspect within the individual components, 4.2.1.3.1 through 4.2.1.3.14, need to be priced out.
    - Additional Financial Factors
- Bid/Solution base questions answered/requirements
    - Managed Detection and Response Capability for on-premise and cloud applications/services.
        - Solution will provide 24x7 Coverage
        - Solution must store data within the Continental United States.
        - Solution provides experienced Security Staff to operate Monitoring and Incident Response
        - Solution will provide an SLA under 1 hour for incident detection and response.
        - Solution will provide offer SOAR capabilities to perform automated incident response and triage.
        - Solution will integrate with Customer Service Management platform for ticketing operations.
        - Solution will leverage User Behavioral Analytics and Machine Learning to detect suspicious and malicious activity.

  - Managed Vulnerability Service to assess customer assets and report on vulnerabilities inside the customer ecosystem, including externally hosted customer PAAS and IAAS services.
  - Solution leverages Customer SIEM or bidder proposes a different SIEM platform.
  - Flexible, scalable licensing model to support growth needs.
  - Integration with Company's Cloud Identity and Access Management Solution for Authentication, Authorization, and Accountability (AAA).
  - Capacity, Health, and Availability Monitoring with ability to set system alarms, thresholds, and send notifications using SMTP, Syslog, or API.
  - Solution can resist or prevent tampering and unauthorized modification of software/hardware/services.
  - Service is resilient and will continue to operate in the event the customer experiences a single data center outage.

- Bidder must sign Data Use Agreement and BAA.

- Three References – Preferably similar in size and scope to BHS.

5.3 Volume 2 – Scoring Criteria

MSSP Scoring Capabilities/Roadmap Criteria
Managed Security Services Provider (MSSP) is an evolving capability, so the winning company will present a roadmap that provides additional features over 18-24 months with some core features day one. The progression in scoring aligns with technical assets that are to be deprecated within BHS or aligned with emerging technologies.

Grading Criteria

- Coverage
- Percentage of Customer Ecosystem being monitored by solution.
- Depth of Detection
- User Changes
- Machine Changes
- Endpoint Detection / Response integration
- Geo-Location Tracking
- Incident Event Detail
- Vulnerability Management
- Licensing Model
- Flexible and scalable
- Affordability / Value
- Compliance
- Customer data stored, transmitted, and processed exclusively inside the Continental United States geography.

6.0 PROPOSAL EVALUATION

As a Contractor to the Federal Government, BHS has adopted FAR 15.301 as guidance for Proposal evaluation. As per the FAR regulation, BHS will evaluate the proposals in alignment with the following:

"(a) Proposal evaluation is an assessment of the proposal and the Contractor's ability to perform the prospective contract successfully. An agency shall evaluate competitive proposals and then assess their relative qualities solely on the factors and sub-factors specified in the solicitation. Evaluations may be conducted using any rating method or combination of methods, including color or adjectival ratings, numerical weights, and ordinal rankings. The relative strengths, deficiencies, significant weaknesses, and risks supporting proposal evaluation shall be documented in the contract file.

(1) Cost or price evaluation. Normally, competition establishes price reasonableness. Therefore, when contracting on a firm-fixed-price or fixed-price with economic price adjustment basis, comparison of the proposed prices will usually satisfy the requirement to perform a price analysis, and a cost analysis need not be performed. In limited situations, a cost analysis (see 15.403-1(c)(1)(i)(B)) may be appropriate to establish reasonableness of the otherwise

successful Contractor's price. When contracting on a cost-reimbursement basis, evaluations shall include a cost realism analysis to determine what the Government should realistically expect to pay for the proposed effort, the Contractor's understanding of the work, and the Contractor's ability to perform the contract. (See 37.115 for uncompensated overtime evaluation.) The contracting officer shall document the cost or price evaluation.

(2) Past performance evaluation.

(i) Past performance information is one indicator of a Contractor's ability to perform the contract successfully. The currency and relevance of the information, source of the information, context of the data, and general trends in contractor's performance shall be considered. This comparative assessment of past performance information is separate from the responsibility determination required under subpart 9.1.

(ii) The solicitation shall describe the approach for evaluating past performance, including evaluating Contractors with no relevant performance history, and shall provide Contractors an opportunity to identify past or current contracts (including Federal, State, and local government and private) for efforts similar to the Government requirement. The solicitation shall also authorize Contractors to provide information on problems encountered on the identified contracts and the Contractor's corrective actions. The Government shall consider this information, as well as information obtained from any other sources, when evaluating the Contractor's past performance. The source selection authority shall determine the relevance of similar past performance information.

(iii) The evaluation should consider past performance information regarding predecessor companies, key personnel who have relevant experience, or subcontractors that will perform major or critical aspects of the requirement when such information is relevant to the instant acquisition.

(iv) In the case of a Contractor without a record of relevant past performance or for whom information on past performance is not available, the Contractor may not be evaluated favorably or unfavorably on past performance.

(v) The evaluation should include the past performance of Contractors in complying with subcontracting plan goals for small disadvantaged business (SDB) concerns (see subpart 19.7).

(3) Technical evaluation. When tradeoffs are performed (see 15.101-1), the source selection records shall include—

(i) An assessment of each Contractor's ability to accomplish the technical requirements; and

(ii) A summary, matrix, or quantitative ranking, along with appropriate supporting narrative, of each technical proposal using the evaluation factors.

(4) Cost information. Cost information may be provided to members of the technical evaluation team in accordance with agency procedures.

(5) Small business subcontracting evaluation. Solicitations must be structured to give offers from small business concerns the highest rating for the evaluation factors in 15.304(c)(3)(ii) and (c)(4).

(b) The source selection authority may reject all proposals received in response to a solicitation, if doing so is in the best interest of the Government.

(c) For restrictions on the use of support contractor personnel in proposal evaluation, see 37.203(d).

deficiencies, significant weaknesses, and risks supporting proposal evaluation shall be documented in the contract file.