Federal Bureau of Investigation (FBI)
Enterprise Security Operations Center (ESOC) Cybersecurity Support
Request for Information (RFI)

1.0 Disclaimer

This notice is for information purposes only. This is not a request for proposal or quote. It does not constitute a solicitation and shall not be construed as a commitment by the Government. Responses in any form are not offers and the Government is under no obligation to award a contract pursuant to this announcement. No funds are available to pay for preparation of responses to this announcement. Any information submitted by respondents to this technical description is strictly voluntary.

All information received in response to this RFI that is marked PROPRIETARY will be handled accordingly. The Government shall not be liable for or suffer any consequential damages for any proprietary information not properly identified. Proprietary information will be safeguarded in accordance with the applicable Government regulations. Responses to the RFI will not be returned. Not responding to this RFI does not preclude participation in any future solicitation, if issued. In accordance with FAR 15.201(e), responses to this notice are not offers and cannot be accepted by the U.S. Government to form a binding contract. It is the responsibility of the interested parties to monitor the Contract Opportunities website at: https://beta.sam.gov/ for additional information pertaining to this RFI.

2.0 Introduction

Purpose:

The U.S. Department of Justice (DOJ), Federal Bureau of Investigation (FBI), DC is requesting information regarding Cybersecurity Support in the context of personnel staffing to perform mission critical services.

Background:

The Federal Bureau of Investigation (FBI) depends upon information technology (IT) to carry out a successful global mission and associated business functions. FBI IT infrastructure includes large, global networks, mission essential criminal justice systems supporting a worldwide law enforcement community, a range of diverse computing platforms, and significant specialized equipment.
The National Institute of Standards and Technology (NIST) 800-37 guidance advises that federal IT systems are subject to serious cyberattacks with adverse impacts. These threats can compromise information availability, confidentiality, and integrity. These impacts strike organizational operations, organizational assets, individuals, other government agencies, and the entire Nation. Cyberattacks on federal IT systems can be aggressive, well-organized, sophisticated, and result in serious or grave damage to national and economic security interests.

The FBI is focused on continuous risk management to address changing policies and standards as well as to take a risk-based approach to assessing, securing, and managing the FBI's information technology. The FBI has invested in research and development, working with other government

agency and private partners. The Cybersecurity Program collaborates with Department of Justice (DOJ), Office of the Director of National Intelligence (ODNI), Committee on National Security Systems (CNSS) and FBI Divisions with the goal of an integrated program approach. The FBI also collaborates other government agencies (OGA) (e.g., Defense Advanced Research Projects Agency (DARPA) and Department of Homeland Security (DHS)) when there are common missions and opportunities to leverage efficiencies.

The primary goal of the FBI's Cybersecurity Program is to protect information, defend systems and networks, provide integrated situational awareness, transform and enable information assurance capabilities, and to create an information assurance empowered workforce. These objectives address mission essential capabilities of the program, as overseen by the Security Division (SecD) and executed by FBI Headquarters and the Enterprise Security Operations Center (ESOC)

The ESOC has been operational since October of 2003 and is chartered by the Director of the FBI to provide Information Technology (IT) Security Operations for FBI IT systems. It is the central organization for IT security operations in the FBI in accordance with FBI Corporate Policy Directive 0388D, Information Systems Security Framework Policy. This policy is consistent with National Institute of Standards and Technology (NIST) and Committee on National Security Systems (CNSS) policies and standards. The ESOC is responsible for continuous monitoring, detection, and response to security incidents that occur on FBI networks, IT services, and systems. This centralization of its IT security functions provides the FBI with a cost effective, synergistic approach to the complexities of monitoring and protecting the FBI IT enterprise.

3.0 Description

The FBI is seeking information regarding Cybersecurity support services. The service areas include but are not limited to: 24/7/365 Watch Floor monitoring, Digital Forensics and Incident Response (DFIR), Mobile Threat Defense (MTD), Cyber Threat Intelligence (CTI), Data Loss Prevention (DLP) and Threat Analytics Platform (TAP) infrastructure support.

The Government's intent is for the requirements described in this section to be performed in multiple locations including Clarksburg, WV and Huntsville, AL, with the period of performance anticipated to begin in Quarter 1 or Quarter 2 of Fiscal Year 2022.

The FBI requests information regarding current performance and capabilities applicable to the above referenced areas of technical expertise and abilities to provide those services. This RFI seeks industry interest applicable to the following service areas and subsequent capabilities in cyber security:

3.1 Cyber Threat Intelligence (CTI)

- 3.1.1 Identification and implementation of Indicators of Compromise (IOC).
- 3.1.2 Threat Hunting
- 3.1.3 General CTI efforts – i.e. reviewing, obtaining, and disseminating cyber threat intelligence
- 3.1.4 Report writing

3.2 Digital Forensics and Incident Response (DFIR)

3.2.1 Escalation of cybersecurity incidents affecting FBI IT systems
3.2.2 Service DFIR Research and Development (R&D) efforts
3.2.3 Advanced digital forensics techniques
3.2.4 Network Forensics capabilities
3.2.5 Malware analysis
3.2.6 Malware testing and IOC validation laboratory construction and development
3.2.7 Rapid and accurate incident response analysis.
3.2.8 After action reviews report generation
3.2.9 Data spills remediation

3.3 Mobile Threat Defense (MTD)

3.3.1 Forensic analysis on smartphones or other mobile devices
3.3.2 Mobile application vetting and testing
3.3.3 Malware analysis for mobile devices
3.3.4 eDiscovery support
3.3.5 MTD tools implementation

3.4 Watch Floor (WF)

3.4.1 Analysis and research of threats and authorizing exceptions
3.4.2 Primary and escalation services for cybersecurity and network monitoring response
3.4.3 Maintenance of 24x7 operations and standard Watch Floor tasks
3.4.4 Malware analysis capability
3.4.5 Network forensics capability
3.4.6 Workforce training on current and emergent tools
3.4.7 Preventative control implementation for security devices, appliances, and applications

3.5 Data Loss Prevention (DLP)

3.5.1 Data collection, trend analysis, and indicator development
3.5.2 Data loss prevention:
- Collection, analysis, and report of data transfer service log results
- Data and case request technical and forensic support
- Generation of potential insider threats
- Development of analytical outputs and technical solutions
- Statistical analysis for research and data exploration

3.6 Threat Analytics Platform (TAP)

3.6.1 Incident Response and Investigative Case direct support
3.6.2 TAP support for major analytic programs through research and development, process implementation, data and systems integration, and advanced analytic solutions
3.6.3 TAP data collection and engineering efforts, including communication of audit requirements with data owners, configuration of collection scripts, maintenance of existing data flows, data modeling and integration

4.0 Requested Information

The Government requests responses from interested firms that provide the following information:

- Ability to meet or exceed the technical services and requirements in Section 3.0 above
- Interest in submitting a proposal for these services and requirements
- Recommendations on acquisition type(s) including, but not limited to, a single or multiple award (e.g., regionalized) approach with associated rationale
- Recommended contract type (e.g., fixed price, cost reimbursement), structure (e.g., mission services; mission and indefinite-delivery, indefinite-quantity (IDIQ); all IDIQ) with associated rationale and method of contracting (GSA, GWAC, another contracting vehicle).
- Summary of capabilities and experience in providing this type of support, including example projects the vendor has performed in the past three years supporting same or similar requirements. This information ensures vendor capability to perform in the stated service areas.
- Any other potential low-cost, high-quality performance solution alternatives

5.0 Response Instructions

Specific instructions for submitting responses are provided below.

5.1 General Response Details:

5.1.1 The RFI response should be comprised of one technical volume (see RFI Section 5.2), one cover sheet, and the RFI Attachment A, Informational Form. Responses should not exceed five pages (one cover sheet and four technical volume pages). Responses to the technical volume should be provided in Microsoft (MS) Word 2016 or later and be single spaced utilizing Times New Roman 12-point font. Attachment A, an MS Excel spreadsheet contains three tabs. Attachment A should remain in Calibri 10-point font and when printed by the Government, should fit to one 8½ x 14 page. Column and row sizes should not be changed. Attachment A is excluded from the page limitation. The Excel spreadsheet should be submitted unlocked and be formattable. No additional data other than the information requested should be included in the attachment.

5.1.2 The cover sheet should include the following at a minimum: Company name, company address, company business size, and the name, phone number, and e-mail address of the designated point of contact.

5.1.3 Providing data/information that is limited or restricted for use by the Government would be of little value and such restricted/limited data/information is not solicited.

5.2 Technical Response Details:

The technical volume should provide the information requested in Sections 3.0 and 4.0 and be submitted in accordance with Section 5.1.1 of this RFI.

6.0 Response Submission Details

All responses to this RFI should be submitted electronically via e-mail to Ms. Dawn Turner at dmturner@fbi.gov and Ms. Beth Howell at bahowell@fbi.gov, no later than 4:00 p.m. Central Time (CT), March 31, 2021.