OCIO

OFFICE OF THE CHIEF INFORMATION OFFICER

FEDERAL BUREAU OF INVESTIGATION

Cybersecurity Section
Cybersecurity Operations Unit (COU)

STATEMENT OF OBJECTIVES

6/6/2018

Federal Bureau of Investigation
935 Pennsylvania Ave, N.W.
Washington, D.C. 20535

Table of Contents

1. Background

The Cybersecurity Operations Unit (COU) (the "Unit") is a new unit within the Associate Deputy Directors Office, Office of the Chief Information Officer, Cybersecurity Section. The section is led by FBI's Chief Information Security Officer (CISO). The Unit strives to continuously assess and enhance the security posture of the FBI through cybersecurity technical operations and information assurance services. The Unit is home to the FBI's *Cybersecurity Red and Blue Team Program* (the "FBI REBL program") and the *Enterprise Compliance and Continuous Monitoring Support Program*.

The FBI REBL program's primary responsibility is to provide remote and deployed cybersecurity services that continuously enhance the FBI's security posture, identify true risk to missions, respond to security incidents, and actively hunt for vulnerabilities and threat activity on FBI systems and networks. In addition, the FBI REBL program will provide similar cybersecurity services in support of FBI operational elements and missions.

The FBI Red and Blue Teams will employ a multitude of methods, tools, and techniques to carry out their assignments and, in doing so, provide FBI leadership with an unvarnished view into the operational security posture of the Bureau's information technology infrastructure. The FBI's Red Team will use offensive tools and techniques to realistically emulate cyber threats to FBI operational systems and networks; varying their approach to mimic both an advanced external threat as well as a trusted insider. The FBI Blue Team will perform advanced operational vulnerability assessments using a variety of subject matter experts to identify risk, support incident response, and hunt for signs of threat activity on FBI systems and networks. Both teams will assess and help to improve the Bureau's ability to:

- **Identify** assets, measure attack surface, understand steady-state
- **Prevent** cyber-based threats from impacting FBI missions
- **Detect** attempts to exploit FBI information, systems and networks
- **Respond** to incidents within FBI systems and networks
- **Recover** from incidents within FBI systems and networks

The REBL programs cybersecurity services will be designed to be flexible, allowing the Unit to adapt to evolving threat tactics and techniques, as well as, to be continuously changing technology environment and threat landscape. The Unit will partner with key programs within the FBI and Intelligence Community (IC) to enhance its capabilities and deliver cybersecurity services that are guided by a clear and current understanding of threats. The Unit will also approach cybersecurity operations with a clear and current understanding of its FBI customer, providing practical and relevant solutions to demonstrable risk to mission.

The REBL program's services are threat and risk-driven; they are not an assessment of compliance to security policies or regulations but rather, go well-beyond the methodologies, boundaries and constraints of security compliance programs to identify risk and actively defend FBI systems and networks. REBL team members will have a great deal of freedom to leverage their skills, knowledge, and creativity to help secure the FBI.

The REBL program will be led by a Government Team Lead and staffed with contracted subject matter experts who will make up the core of each team. Government personnel on temporary or joint-duty assignments will also be part of the Unit.

The Red Team will operate under a blanket set of rules allowing it to conduct 24x7x365 general and tailored operations across the FBI enterprise, mimicking both insider and external threats. General operations will be conceived of and initiated by the Program with Federal oversight. They will be made up of multiple missions performed throughout the year that vary in scope, approach, and objectives. They will be geared towards continuously identifying issues and feeding that information, especially time-sensitive countermeasures, to the relevant areas within FBI. Some missions may not necessarily emulate a true threat, utilizing more of a penetration testing or vulnerability assessment methodology. For example, there may be quarterly phishing exercises aimed at simply improving security awareness or focused application penetration tests.

Tailored Red Team operations will be initiated by FBI customers, may be short or extended in duration, and are true threat emulations; incorporating social engineering, security monitoring evasion, customized tools, and other advanced computer network exploitation techniques to realistically emulate a threat. The blanket set of rules will be tailored appropriately to support these operations. Tailored operations will also be designed to support the FBI's Insider Threat Office and other partners to *realistically* emulate insider threats with specific objectives to identify risk and improve insider threat prevention, detection, and response capabilities. The Red Team may also partner with other areas of the FBI to incorporate more advanced adversarial techniques during their operations.

The Blue Team will conduct advanced operational vulnerability assessments on critical FBI systems and networks for the purpose of identifying true risk to missions. Such assessments will be performed by a team of technical, threat and security experts that have complete access to systems, networks, and people to ensure the most comprehensive assessment possible.

Most, but not all, Blue Team projects will be scoped by the REBL program based on threat intelligence and a threat perspective, that is, not on arbitrary systems boundaries but projects informed by threat intelligence and technical realities in the operational environment. A general rule is that, if a threat can see it, then it's in scope. The Blue Team will also employ a 'best tool or technique for the job' approach to identifying vulnerabilities across all technologies within scope of the project; from network devices, to databases, to operating systems, to applications, etcetera.

The Unit is also home to the *Enterprise Compliance and Continuous Monitoring Support Team*. The team operates within the policies, directives, and boundaries of security auditing and compliance such as ICD 503 and NIST SP 800-53. The team leverages security assessment and vulnerability assessment subject matter experts' adept at interpreting and assessing security controls to support multiple information assurance programs at the FBI, but primarily the Security Assessment and Authorization program and Continuous Monitoring program (ongoing monitoring of FBI enterprise security posture and continuous diagnostic and mitigations).

The team is also responsible for architecting, engineering, operating, and supporting the FBI's enterprise vulnerability assessment solution. In addition, the team will develop, maintain, and support a standardized set of security assessment tools (toolbox) for use by ISSOs and other approved users responsible for performing basic vulnerability assessments and cybersecurity hygiene. Supporting this effort includes developing a training program in the use of the tools as well as SOPs, policy, related to their use on FBI systems.

Table 1: Programs/Teams within Cybersecurity Operations Unit. The Mitigation & Support Team Supports the Entire Unit.

Teams	**Summary**
Red Team	The FBI's Red Team uses offensive tools and techniques to emulate cyber threats to FBI operational systems and networks. Their approach will vary, mimicking both an advanced external threat as well as a trusted insider and are objective based. Operations are conducted under a specific time constraint, with the goal to not simply achieve an objective but to find as many ways as possible to achieve an objective within the time allotted.
Blue Team	The FBI Blue Team performs advanced operational vulnerability assessments using a variety of subject matter experts to identify risk; they also provide incident response, and threat hunting services.
Mitigations & Support Team	Provides administrative support to both teams, manages the Unit's technical infrastructure, conducts threat and vulnerability research, coordinates the Unit's cybersecurity operations, and researches customer solutions.
Enterprise Compliance & Continuous Monitoring Support Team	The team leverages security and vulnerability assessment SMEs adept at interpreting and assessing security controls to support multiple information assurance programs at the FBI. The team is also responsible for building, operating, and supporting the FBI's enterprise vulnerability scanning solution and ISSO toolbox.

2. Scope

The scope of this initiative will encompass two parts.

Part One consists of a broad array of services performed to plan, staff, equip (i.e., in total, "stand-up"), and operate the FBI REBL program. An existing Government resource has been tasked with the early planning for the REBL Program's Initial Operating Capability (IOC) for the program. The Contractor will be expected to contribute to what remains of any planning and then move the program to IOC, followed by what remains of any to Full Operating Capability (FOC). Once FOC is achieved, the Contractor will operate and continuously seek to improve the program.

Part Two consists of a broad array of services engaged to plan, staff, equip (i.e., in total, “stand-up”), and operate the Enterprise Compliance and Continuous Monitoring Support Program. It is expected there will be a ramp-up phase over the first year, where an initial set of capabilities is established using some existing resources and then expanded in the out years.

3. Points of Contact

The FBI Program Manager will provide all day-to-day technical and management direction for all tasks associated with this contract. The FBI Program Manager is:

Mr. Michael Willburn,
Unit Chief, Cybersecurity Operations Unit
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

The FBI Contracting Officer’s Representative (COR) will provide technical and management direction within the Task Order scope. The FBI COR will review; provide sign-off and acceptance of deliverables and work products. The FBI COR is:

TBD
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

4. Contract Type

This is a single-award, Cost Plus Award Fee (CPAF) contract. The Contractor shall provide labor, material, and equipment (save Government Furnished Equipment/Property/Information) as required to execute its approach for supporting the Bureau’s achievement of the Bureau’s Objectives, through the production of the associated Outcomes, delineated at paragraphs **4.1 through 4.3, below**. The Bureau’s requirements are structured into the below tasks.

4.1 General Contract Functions

4.1.1 Expert Knowledge of Threats

4.1.1.1 Objective: The FBI maintains awareness of insider and external threats, including nation-state actors, which would seek to target classified and unclassified FBI systems, networks, and data.

4.1.1.2 Standards:

4.1.1.2.1 Classified and unclassified resources are leveraged to acquire, maintain, and employ knowledge, including key partnerships within FBI and the Intelligence Community.

4.1.1.2.2 Threats and their likely goals and intentions for targeting the FBI, the tools and techniques employed, the current threat activity, and the threats' use of computer network operations are addressed in the threat identification process.

4.1.2 Applicability to FBI

4.1.2.1 Objective: Consistent demonstration of relevant and accurate references to the FBI's technology environment and criminal and national security missions in the creation of any associated work products.

4.1.2.2 Standards:

4.1.2.2.1 FBI partnerships, resources, and past projects are leveraged to acquire, maintain, and employ knowledge of FBI systems, networks, information and criminal and national security missions.

4.1.3 Technical and Security Recommendations

4.1.3.1 Objective: Detailed, accurate, comprehensive, and relevant technical and security recommendations are articulated appropriately for the target audience.

4.1.4 Initial and Full Operating Capabilities

4.1.4.1: Objective: The Program is established in a professional, effective, and efficient manner, following standard project management best practices.

4.1.5 Consistency of Operations

4.1.5.1: Objective: Once full operating capability has been achieved, a consistent quality of service and capabilities is offered to the recipients of the Program's products, throughout its life-cycle.

4.1.6 Investigative Support

4.1.6.1: Objective: Red/Blue Teams leverage their knowledge and expertise to support operational divisions within the FBI on an as needed basis.

4.2 Red Team Functions

4.2.1 Threat Emulations

4.2.1.1 Objective: High-risk vulnerabilities, vulnerability chains, and threat-vectors that impact critical assets on operational FBI systems and networks are identified.

4.2.1.2 Standards:

4.2.1.2.1 Red Team operations adhere to a pre-defined and approved set of standard operation procedures, which are flexible enough to allow for creativity on the part of Red Team Operators and a realistic emulation of threats, but also maintain an appropriate level of control and oversight over operations.

4.2.1.2.2 Red Team operations are comprehensive in their attempt to assess prevention, detection and response capabilities. As many ways to achieve the objective are identified within the time allotted.

4.2.1.2.3 Red Team operations, as much as feasible and possible, realistically emulate a threats tactics, techniques, and procedures (TTPs) when targeting unclassified and classified government systems.

4.2.2 Cohabitation and Incident Response

4.2.2.1 Objective: Red Team operations incorporate threat hunting tactics and techniques to assess if systems targeted by the Red Team have been or are being actively exploited by threats.

4.2.3 Continuous A Operations

4.2.3.1 Objective: Red Team program that conducts all operations under a single blanket set of rules allowing for continuous operations (i.e., 24x7x365) across the FBI.

4.2.3.2 Standards:

4.2.3.2.1 General rules are tailored or added to, as needed, when conducting targeted operations that have unique objectives and require additional rules.

4.2.3.2.2 Red Team operations respond to changes in threat TTPs, the technology landscape, and the priorities of the FBI.

4.2.3.2.3 Continuous operations, those not falling under a targeted operation, are organized around specific goals and objectives established by Red Team members and Government leadership.

4.3 Blue Team Functions

4.3.1 Comprehensive Assessments

4.3.1.1 Objective: Operational security assessments providing comprehensive identification of vulnerabilities; clearly describe their impact to a mission, and clearly articulate mitigation strategies.

4.3.1.2 Standards:

4.3.1.2.1 Blue Team operations adhere to a pre-defined and approved set of standard operation procedures that are flexible enough to allow for creativity on the part of staff and enable a comprehensive vulnerability assessment, but also maintain appropriate level of control, oversight, and consistency of quality and service.

4.3.2 Incident Response and Threat Hunting

4.3.2.1 Objective: A third-tier incident response capability performing, supporting and facilitating activities within the discovery, containment, eradication, recovery and follow-up phases of the incident response process exists.

4.3.2.2 Standards:

4.3.2.2.1 Threat hunting activities are incorporated into Blue Team assessments.

4.3.2.2.2 The Blue Team provides advice, assistance and leadership when requested during the incident response process; leveraging existing capabilities and resources within the FBI throughout the incident lifecycle.

4.4 Mitigations & Support Team Functions

4.4.1. Cybersecurity Remote Operations Center and Flyaway Kits

4.4.1.1 Objective: The creation, operation and maintenance of a Cybersecurity Remote Operations Center (CyROC) for use in conducting remote Red and Blue Team operations at all classification levels. Also included is the creation and maintenance of Red and Blue Team Flyaway Kits that enable deployed operations at all classification levels.

4.4.2. Customized Research

4.4.2.1 Objective: Customized threat, technical, and mitigation research in support of Unit operations.

4.4.3. Unit Operation/Coordination

4.4.3.1 Objective: The initiation, coordination and management of all Unit operations, i.e. red team operations, blue team operations, vulnerability assessments, etc.

4.4.3.2 Standards

4.4.3.2.1 Operating, Staffing, and Milestone Plans are developed and implemented with FBI-approval.

4.4.4. Documentation, Unit Media, and Written Products

4.4.4.1 Objective: Documentation regarding the Unit’s services, business processes, methodologies, and standard operating procedures. Also included are all digital media and written products produced in support of Unit objectives.

4.5 Enterprise Compliance and Continuous Monitoring Support Team Functions

4.5.1. Security Assessment & Authorization (SA&A), and Information Assurance Support

4.5.1.1 Objective: FBI personnel involved with managing, performing, and overseeing the SA&A process and other Information Assurance programs at the FBI receive expert support from the Unit in regards to understanding the technical aspects of security and privacy controls.

4.5.2. Technical Security Assessments

4.5.2.1 Objective: Technical security assessment is accomplished.

4.5.2.2 Standards:

4.5.2.2.1 A standardized set of security tools, of a systems implementation of security and privacy controls in support of SA&A and Continuous Monitoring is used.

4.5.2.2.2 The outcome is not a deep-dive technical assessment, but rather ensures all assigned security controls were implemented following security best practices and policy.

4.5.3. Enterprise Vulnerability Scanning & Reporting

4.5.3.1 Objective: Regular vulnerability scans across the FBI's information technology environment(s) in support of the FBI's security compliance and vulnerability management programs.

4.5.4. Enterprise Vulnerability Scanning System

4.5.4.1 Objective: The architecting, engineering, operation, and maintenance of an automated (and manual) enterprise vulnerability assessment system that is capable of assessing basic security hygiene across the enterprise in accordance with FISMA and other applicable security requirements.