(U) STATEMENT OF OBJECTIVE

VERSION 1.0

HIVE-IQ

8 May 2020

Table of Contents

1 (U) Background

The USCYBERCOM J9 coordinates, integrates, and prioritizes cyberspace capability development efforts to rapidly deliver joint operational products through integrated project delivery, enabling full-spectrum cyberspace operations. The J9 plans and synchronizes joint capability development for the cyberspace domain, rapidly delivers mission-ready operational products and services required for generating, facilitating, or monitoring effects, and operates and maintains USCYBERCOM's technical baseline to enable the Command to execute its missions.

This effort fulfills an urgent need in USCYBERCOM to prepare and protect the US election systems in support of the 2020 Presidential elections, with Primary elections beginning in February 2020. This effort shall support the national security requirements to understand nation-state operations targeting US critical infrastructure.

1.1 (U) Scope

The contractor shall refine and integrate the CYBER 9-Line concept into technology and practice for the State National Guard (NG) elements and Cyber National Mission Force (CNMF). This effort shall support refinement and integration of technical indicator sharing, such as Indicators of Compromise (IOCs) and malware, as well as promote and facilitate collaboration to defend the nation across federal, state, and local authorities to defend the nation.

2 (U) Objectives

2.1 Task 1 - Integrate & Refine the CYBER 9-Line

(U//~~FOUO~~) The Contractor shall prototype rapid information exchange formats to encourage collaboration and timely situational awareness across the CNMF and State NG elements, particularly in support of the 2020 elections. This task includes the definition and documentation of the information needs and standards to create consistency across tactical, operational, and strategic information reports. Adoption of this model requires relationships with the State NG elements and their connections to their Critical Infrastructure and Key Resources (CIKR) communities. This task includes coordination of architecture, technology, and processes to streamline information exchanges at the speed of need. This task will document and utilize Application Program Interfaces (APIs) to exchange information across tactical, operational, and strategic technology platforms and create interoperability with the HIVE-IQ platform and USCYBERCOM systems, such as Big Data Platform (BDP). USCYBERCOM CNMF will refine requirements throughout the stated effort, while state NG elements will provide requirements and feedback. The effort will support knowledge gained from cyber exercises and operational opportunities to validate and refine requirements.

This effort shall result in in the following:

- Situational awareness of adversary tactics in the Homeland
- Identified opportunities for collaboration and joint operations
- Streamlined processes for information exchange across USCYBERCOM and State NG elements

- CYBER 9-Lines captured by the NG using Hive-IQ and sent to a USCYBERCOM designated destination (e.g., an email address, S3 bucket, or documented system API)

2.1.1 Refine the CYBER 9-Line Format

The Contractor shall coordinate with USCYBERCOM, NGB, DHS, and State NG elements. The Contractor shall gather data and refine requirements from stakeholders and utilize documented inputs to modify and refine the 9-line format specification.

2.1.2 Integrate 9-Line input into Hive-IQ

The Contractor shall integrate the 9-Line format for NG elements to input the desired information via Hive-IQ. The Contractor shall demonstrate the process in exercises and in support of missions as necessary.

2.1.3 Integrate 9-Line export from Hive-IQ

The Contractor shall enable the 9-Line template for export from Hive-IQ. The Contractor shall deliver the 9-Line to designated USCYBERCOM systems. Method of delivery may include one or all of the following: email address, S3 bucket or documented system API. The Contractor shall provide feedback on USCYBERCOM processes and tools to streamline system-to-system integration. The Contractor shall demonstrate the process in exercises and in support of missions as necessary.

2.2 Task 2: Integrate Technical Indicator Sharing

The Contractor shall enable rapid exchange of technical indicators (such as IoCs, sensor data, and malware) to encourage collaboration and timely situational awareness across the CNMF and State NG elements, particularly in support of the 2020 elections. The effort shall include definition and documentation of the information needs and standards to create consistency across tactical, operational, and strategic information reports. The Contractor shall support the coordination of architecture, technology, and processes to streamline information exchanges at the speed of need for a variety of file types, including STIX, CSV, PDF, netflow, and binaries. The Contractor shall enable APIs to exchange information across tactical, operational, and strategic technology platforms as needed to deliver technical information to interoperable USCYBERCOM systems. This effort shall utilize cyber exercises and operational opportunities to validate and refine requirements. This effort shall enhance situational awareness of adversary tactics, and identify opportunities for collaboration and joint operations. This effort shall develop streamlined processes for information exchange across USCBERCOM and State NG elements. The technical indicators captured by the NG shall be provided to a USCYBERCOM designated destination (e.g. an email address, S3 bucket or documented system API).

2.2.1 Information Types and Format

The Contractor shall document expected information types and formats. This data shall be coordinated with USCYBERCOM, National Guard Bureau, Department of Homeland

Security, and State NG elements. The data shall be gathered, and refined from the stakeholders. Documented inputs shall be delivered to the 9-Line format specification.

2.2.2 Hive-IQ integration

The Contractor shall integrate Technical Indicator Sharing Input into Hive-IQ. This shall include the integration of the information types and formats for input into Hive-IQ. The Contractor shall establish a documented process for related platform integration requirements, and as necessary, demonstrate process in exercise and missions as necessary.

2.2.3 Technical Indicator Export

The Contractor shall support technical indicator sharing export from the Hive-IQ platform. The Contractor shall integrate the information types and formats for export from Hive-IQ, as designated by USCYBERCOM. The contractor shall enable the delivery of technical indicators from Hive-IQ to USCYBERCOM designated systems. The Contractor shall provide feedback on USCYBERCOM processes and tools to streamline system-to-system integration, and as necessary, demonstrate processes in exercises and missions as necessary.

2.3 (U) Task 3: Triage and Enrichment

The Contractor shall support triage and analysis of threat information across USCYBERCOM and State NG elements to enable rapid decision making and improve situation awareness. The Contractor shall leverage existing malware analysis, cyber threat information and incident analysis products and data sources. USCYBERCOM CNMF shall identify and refined requirements throughout this effort while State NG units shall provide requirements and feedback throughout. This effort shall utilize cyber exercises and operational opportunities to validate and refine processes. This effort shall result in actionable information being provided to the State NG at the tactical level, and the CNMF at the operational level.

2.3.1 – Triage and Enrichment

The Contractor shall conduct triage and enrichment of State NG element information. The Contractor shall provide proactive and responsive cyber threat information. The Contractor shall provide automated malware analysis for designated partners. The Contractor shall prioritize task assignments based on mission needs, as well as generate and deliver metrics.

2.3.2 – Support to CNMF J3

The Contractor shall convey insights and coordinate enrichment and response with the USCYBERCOM Operations Enabling Cell (OEC).

2.4 Period of Performance

The Period of Performance shall consist of a base period of 12 months from date of award.

2.5 Place of Performance

The primary place of performance for this effort shall be the Contractor's facility. The Contracting Officer (KO) may designate other sites as required for performance of this effort. As directed by the Contracting Officer, the contractor shall continue performance in emergency or mission essential conditions. Additionally, the contractor may be required to account for the whereabouts of their personnel should this information be requested by the COR.

3. Delivery Schedule

The contractor shall create, maintain, and update the deliverables in the performance of this effort, as indicated

3.1 Kick off Meeting

Within five (5) days after date of contract, the contractor shall participate in a virtual meeting, up to two (2) hours, with USCYBERCOM / CNMF representatives. The meeting will introduce key players and provide knowledge leveling on contract mechanics and mission objectives.

3.2 Project Management Plan

The Contractor shall generate a project management plan (PMP) that shall be delivered within two (2) weeks of award. The plan shall be approved by the COR. The project management plan shall be a tailored document that includes a Work Breakdown Schedule (WBS), a schedule, financial plan, processes for management and addresses when the plan needs to be updated.

3.3 Monthly Financial Report

An unclassified itemized financial status report which shall include actual hours by employee, details of ODC expenses, expected funds depletion date, a chart of budgeted cost for work performed (BCWP), actual cost for work performed (ACWP) and variance at completion (VAC) is to be delivered to the COR. Tables, lists and charts shall also be delivered in editable Microsoft Excel format. Monthly Financial Reports are due no later than ten (10) working days after the end of the month.

3.4 Monthly Assessment Report

The monthly assessment report, up to 3 pages, will highlight status of efforts to create JSON format for CYBER 9-Line report template; workflow improvements within HIVE-IQ to populate the CYBER 9-Line report with technical Indicators of compromise; and delivery of said JSON file, with associated attachments (enrichment reports with citations) to USCYERCOM / Big Data Platform Analyst Dashboard. Assessment can highlight ease

of / challenges with use of USCYBERCOM Big Data Platform API. Monthly Assessment Reports are due no later than ten (10) working days after the end of the month.

3.5 HIVE-IQ User Accounts

Within 30days after data of contract, contractor shall provide up to ten (10) user accounts to USCYBERCOM / Cyber National Mission Force (CNMF) military and government personnel. These user accounts will be used to enable unclassified collaboration and synchronization with National Guard users of HIVE-IQ.

3.6 System Software Developed

Delivered at 6 months after date of contract award and updated at end of contract with any revisions. Process flow documentation, as well as, description of the user experience, data and JSON formats, system connections, enrichments and security / authentication mechanisms.

3.7 Triage and Enrichment

During period of performance, enable State and National Guard analyst who use HIVE-IQ to easily leverage local data sources, and provides those enriching data sources, with appropriate citation, that are sharable with USCYBERCOM / CNMF. Include State and National Guard analysts' commentary that provides further context and judgement with respect to the malicious Cyber activity, to be incorporated into the Cyber 9 Line report.

3.8 Contract Exit Transition Plan

Delivered, NLT 180 days after contract award, to a follow-on contractor to operate the information exchange developed under this contract, and updated 30 days before the end of this contract. The contractor shall submit a plan for transitioning the necessary tasks, and activities, from the incumbent. The plan shall identify transition planning strategy, schedule, risks, roles and responsibilities to assist new partners to create a cyber9line template, populate the template with technical Indicators of compromise, and deliver this report in JSON format to USCYBERCOM / Bid Data Platform Analyst Dashboard. The Transition Plan will focus on the data formats, processes, and requirements so that it is generally applicable to any platform that a follow-on contractor may utilize and will not be specific to HIVE-IQ.

3.9 Final Summary Report

Shall be delivered NLT one month prior to the end of the period of performance. The Contractor shall deliver to the PM/COR a Final Summary Report of all the activities that

captures findings, lessons learned, best practices, recommendations for future courses of action and all requirements.

Reference	Deliverable	Frequency	Due Date	Delivery Method/Format
3.1	Kick Off	Once	5 Days ADC	Virtual meeting
3.2	Project Management Plan	Once	15 Days ADC	Email
3.3	Monthly Financial report	Monthly	As Requested	Email
3.4	Monthly Assessment report	Monthly	As Requested	Email
3.5	HIVE-IQ User Accounts	A requested	30 Days ADC	Email
3.6	System Software Developed	As requested	180 Days ADC	Email
3.7	Triage and Enrichment	As Requested	As Requested	As Requested
3.8	Contract Exit Transition Plan	Once	180 Days ADC	As Requested
3.9	Final Summary Report	Once	As Requested	Site Visit/VTC

4. Description of Labor Categories

Contractor shall provide a description and allocation of labor categories estimated for the performance of each task.

5.0 (U) DATA RIGHTS

All reference process development, material, documents, training support material, and all other information obtained, produced, or developed by the contractor, inclusive of subcontractors, in support of this effort shall become the property of the U.S. Government and shall be delivered to the Government. The Government shall have unlimited and unrestricted right to use, modify, reproduce, perform, display, or disclose all technical and software data that is developed, updated, modified, or converted under this effort. The contractor shall not distribute or use the information and/or data without the express and specific written approval of the Contracting Officer's Representative. See also DFARS 252.227-7013(a)(16), 252.227-7014(a)(16), as applicable.

5. Subcontractors

(U//~~FOUO~~) Subcontractors and consultants are anticipated. Use of subcontractors and consultants other than those included in the contactor's proposal shall require prior approval by the Contracting Officer.

6. Administrative Information

(U//~~FOUO~~) Technical discussions held by the Contractor with end-users, sponsors, or others do not authorize ANY change to cost, schedule, or scope of this effort. Such matters must be resolved by the Contracting Officer.

7. Travel

Travel is only authorized only when virtual presence cannot be accommodated for participation in cyber exercises and design review sessions with National Guard elements and National Guard Bureau. All contractor travel shall be approved by the COR prior to occurrence.