CyberSecurity Sample
Performance Work Statement

READ FIRST

This SOW template provides examples of information for a variety of cybersecurity services that can be purchased through GSA. This sample document provides typical language for a cybersecurity solicitation, and provides examples of specific activities and deliverables associated with Cyber Hunt and Continuous Diagnostic and Mitigation (CDM) services.

Material from this and other SOW examples can be copied and pasted directly into a RFQ template or be used as a stand alone document to make your experience easier and more efficient. These templates provide prompts for agencies to input their specific information in red text, provides sample draft language that can be used in blue text, and includes standard SOW language that should be included in black text. While these templates provide information on cybersecurity services, agencies should make sure that solicitations contain the specific requirements of their organization.

To assist with the creation of Statement of Work or a Performance Work Statement, users are encouraged to use the Automated Requirements Roadmap Tool (ARTT). This software uses an interview-based format to transform technical requirements into a useable SOW or PWS that can be proposed to by industry. The link to ARTT can be found here, and is free to use.

1.0 OVERVIEW AND BACKGROUND

<Insert agency name> <describe organization and outline specific departments or systems included for this RFQ>

Sample general Cyber Security Language:

Cybersecurity is the ability to protect or defend information systems from cyber-attacks. Cybersecurity is an umbrella term that incorporates different information technology (IT) strategies that protect networks (e.g., identity management, risk management, and incident management). Information Assurance employs measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating identification, protection, detection, response, and recovery capabilities. As IT evolves, so do the threats to data security, individual privacy, and the continued operation of the Federal Government's IT assets.

Sample CDM language:

The Continuous Diagnostics and Mitigation (CDM) program is a dynamic approach to fortifying the cybersecurity of Government networks and systems. As threats to the nation's information security continue to emerge, Government leaders recognize the need for a modified approach to protecting the Government's cyber infrastructure. The CDM Program enables DHS, Federal Agencies, and state, local, regional, and tribal governments to enhance and further automate their existing continuous network monitoring capabilities, compare and analyze critical cybersecurity related information, and enhance risk-based decision making at the Agency and Federal enterprise level. The CDM Program benefits participating Agencies by helping to identify information security risks on an ongoing basis so that Agencies can rapidly detect and then respond to information security events.

Congress established the CDM Program to provide adequate, risk-based, and cost-effective cybersecurity and more efficiently allocate cybersecurity resources. The CDM Program provides Federal Departments and Agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

Starting in January 2013, DHS (operating on behalf of the participating Agencies) provided tools/sensors and services to execute Phase 1 of the CDM Program, which implemented the CDM Solution at each Agency in this TO. Beginning in June 2016, DHS provided tools/sensors and services to participating Agencies to execute Phase 2 of the CDM Program.

The CDM Program is organized by phases as identified below in Diagram 1: CDM Phases.

Diagram 1: CDM Phases

1.1 PURPOSE OR OBJECTIVE

The contract shall be for nonpersonal services to provide HACS services on <Insert agency name and system name>. The contractor shall provide all personnel and items necessary to perform the functional and technical support described in this SOW, except those items specified as Government furnished equipment/property. The contractor shall perform all tasks identified in this SOW.

Cyber Hunt Sample Language:

This RFQ seeks contractors holding the Multiple Award Schedule (MAS) Information Technology HACS SIN. Additionally, the contractor must be cataloged in the following subcategory under SIN 54151HACS.

- Cyber Hunt

CDM Sample Language:

The purpose of this TO is to resolve CDM capability gaps, enhance existing CDM capabilities, introduce new CDM capabilities, and provide support to the CDM Solution of participating Agencies, leading to a strengthening of their overall cybersecurity posture. The CDM Solution includes CDM approved products, configured to reflect the DHS CDM Program priorities and Agency policies as appropriate, that implement a common set of capabilities and enable increased risk-reduction and alignment with Agency risk tolerance.

2 SCOPE

The scope of this services contract for <Insert agency name and system name> includes the following:

- <Insert scope of services required>

CDM Sample Language:

The scope of this TO is to provide support for all phases of the CDM Program and implement a common set of CDM capabilities across Federal Agencies. The scope of this TO includes:
a. Provisioning Agencies with CDM approved products, supporting ancillary products, and providing the associated services to the participating Agencies.
b. Filling gaps in the existing Agency CDM Solution to achieve a common set of capabilities.
c. Operating and maintaining (O&M) the existing CDM Solution, while continuing to enhance and refresh CDM approved products, as appropriate.
d. Planning for Agency support of provisioning, configuring, operating, testing, and

managing CDM tools, sensors, Agency-level dashboards, and data feeds as well as support for the CDM Solution's governance.
e. Developing, integrating, operating, and maintaining the capability for CDM-approved products to report information to the CDM Agency Dashboard and feed accurate information the CDM Federal Dashboard.
f. Designing, building, deploying, and operating the CDM Solution for component offices of the participating agencies that opt-in to the CDM Program.
g. Providing Agency-specific training for the CDM Solution and the Agency CDM Dashboard and providing CDM governance support.

The performance of this TO is primarily at the contractor's facility. The contractor's facility shall include spaces suitable for a development and test facility and support classified IT storage.

3 GOVERNMENT FURNISHED ITEMS & SERVICES

3.1 Government Furnished Property
3.2 Government Furnished Services
3.3 Government Furnished Material
3.4 Government Furnished Information (Data)

3 REQUIREMENTS

[The following tasks provide example activities for cyber security services. Adjust these tasks to align with your specific requirements and with additional guidance from the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA)]

Helpful Hints:

- Divide the work into tasks
- Use functional descriptions or performance-based descriptions

Cyber Hunt Sample Language:

3.1 The primary purpose of Cyber Hunt services is to proactively and iteratively detect, isolate, and neutralize advanced threats that evade automated security solutions. Cyber Hunt activities start with the premise that threat actors known to target some organizations in a specific industry, or specific systems, are likely to also target other organizations in the same industry or with the same systems. Cyber Hunt activities use information and threat intelligence specifically focused

on the proximate incident to identify undiscovered attacks, and investigate and analyze all relevant response activities.
Cyber Hunt tasks include: collecting intrusion artifacts (e.g., source code, malware, and trojans) and using discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise; coordinating with and providing expert technical support to enterprise-wide Computer Network Defense technicians to resolve Computer Network Defense incidents; and correlating incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation. Deliverables for Cyber Hunt include, but are not limited to, a Cyber Hunt Report including an artifact list, a summary of potential incidents and resolved incidents, and remediation recommendations for vulnerabilities found based on previous incident data.
Knowledge Areas include, but are not limited to:
Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non-nation state sponsored], and third generation [nation state sponsored])
Knowledge of general attack stages (e.g., footprinting and scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks, etc.)
Knowledge of incident categories, incident responses, and timelines for responses
Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.
Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber threat/warning assessments.
Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.
Conducts advanced analysis of collection and open-source data to ensure target continuity, profile targets and their activities, and develop techniques to gain more target information.
Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks, and the applications on them.
Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.

CDM Sample Language:

The objective of this requirement is to operate and enhance the existing Group A CDM Solution. In compliance with applicable standards, this objective will be accomplished, through detection improvement and analysis of IT security events, and in cooperation with the DHS CDM PMO and the Group A end users.

Additional CDM Program objectives for the TO are to:
a. Reduce Agency threat surface through strengthening cybersecurity of Agency IT assets.
b. Achieve the most advantageous cost and price discounts while provisioning Agencies with CDM tools and capabilities.
c. Deliver flexible services that can accommodate dynamic cyber environments.
d. Timely completion of work to ensure delivered CDM capabilities are fully implemented at receiving Agencies.

e. Promote transparent and effective communications that accurately present status to CDM stakeholders.
f. Provide accurate reporting of Agency environments while achieving successful governance of Agency cybersecurity programs.

REQUEST FOR SERVICE (RFS)
The Government requires a flexible approach to support the evolving CDM technical capabilities in a rapidly changing cybersecurity environment during the entire life of the TO. To address the evolving needs of the supported Agencies, the Government will execute a Request for Service (RFS) process that will further define Agency-specific requirements for initial delivery and/or additional support of a CDM capability or service.

The RFS will state the purpose, supported Agency(ies), primary place of performance, anticipated tasks/subtasks required, technical details of the requirement (including references to the CDM Technical Capabilities Requirements Documents, Volume 1 and Volume 2 (**Section J, Attachments Y.1 and Y.2**) when appropriate), other supporting details related to the requirements (e.g., security requirements, expected execution timelines, Government-Furnished Information (GFI), and tailored System Engineering Lifecycle (SELC) requirements), and expected timeline for return of the RFS Response. Each RFS will apply performance-based outcomes and standards as appropriate to the requirement. High quality products and services delivered in a timely and cost-effective manner will be the primary criteria for the work performed under an RFS.

After receiving an RFS, the contractor shall develop and deliver an RFS Response in accordance with **this SOW**. The contractor shall only execute actions identified in the RFS Response after the Government provides written approval. All cost and schedule measures associated with the execution of a specific RFS shall be clearly identified in the Integrated Master Schedule (IMS), cost reports, and invoices.

The RFS Tracking Table (**Section J, Attachment AI**) identifies RFS actions approved for execution during the TO.

TASKS

Task 1: Provide Project Management
Task 2: CDM Solution and Dashboard Support
Task 3: Integrate New CDM Capabilities
Task 4: Expanded Agency Services
Task 5: Surge Cybersecurity Critical Incident Support

Task 1 – PROVIDE PROJECT MANAGEMENT
The contractor shall provide project management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Performance Work Statement (PWS). The contractor shall identify a Project Manager (PM) by name that shall provide

management, direction, administration, quality assurance, and leadership of the execution of this TO.

The contractor shall use industry-best standards and proven methodologies that ensure all TO activities are identified, documented, and tracked so that the TO can continuously be evaluated and monitored for timely and quality service. The contractor shall notify the Federal Systems Integration and Management Center (FEDSIM) Contracting Officer (CO) and Contracting Officer's Representative (COR) and the DHS Technical Point of Contact (TPOC) of any technical, financial, personnel, Organizational Conflict of Interest (OCI), or general managerial problems encountered throughout the life of the TO.

TASK 2 – CDM SOLUTION AND DASHBOARD SUPPORT

The contractor shall provide CDM Solution and CDM Agency Dashboard support entailing necessary testing and security accreditation support to maintain authorization and providing Tier III support to the CDM Solution. This task also entails updating the CDM Agency Dashboard with each new release of the CDM Agency Dashboard, providing Tier II level support to the CDM Agency Dashboard, and establishing and maintaining operational CDM data feeds from the integration layer to the CDM Agency Dashboard and from the CDM Agency Dashboard to the CDM Federal Dashboard. Both the CDM Agency and CDM Federal Dashboards are developed by the CDM Dashboard provider through another CDM TO. This CDM Dashboard provider will provide releases of the CDM Agency Dashboard and Tier III support for the CDM Agency Dashboard to the contractor. The CDM Federal Dashboard is operated and maintained outside of this TO.

TASK 3 – INTEGRATE NEW CDM CAPABILITIES

The Government will identify CDM capabilities that require immediate action for implementation of a specific CDM capability or set of capabilities that have not yet been deployed or are requiring updating into an Agency's infrastructure. CDM capabilities are inclusive of filling gaps in an Agency's current CDM environment, expansion of CDM capabilities through new investments, and the technical refresh of previously installed CDM tools and sensors. CDM capabilities are listed below and defined in the CDM Technical Capabilities Requirements Document Volume 1 (**Section J, Attachment Y.1**).

Phase 1: HWAM, SWAM, CM, VUL
Phase 2: TRUST, BEHAVE, CRED, PRIV
Phase 3: BOUND, MNGEVT, OMI, DBS
Phase 4: Micro-segmentation, DRM, Advanced Data Protection

In response to an RFS, the contractor shall provide a technical plan. After Government approval of the technical plan, the contractor shall purchase, install, configure, and customize the CDM capability to ensure proper operation. The contractor shall thoroughly test the CDM capability before transitioning the operation of the capability to an Agency's designated operations team.

TASK 4 – EXPANDED AGENCY SERVICES (Optional)

Group A Agencies may elect to receive services defined in the following subtasks. The

Government anticipates utilizing the RFS process to initiate contractual actions which will execute the subtasks described in detail below.

TASK 5 – SURGE CYBERSECURITY CRITICAL INCIDENT SUPPORT (Optional)

The Government anticipates surge support will be required on a case-by-case basis when Agencies supported by this TO are impacted by cyber-attacks, in need of penetration testing, or require cyber risk assessment and mitigation activities. The scope of the response shall consist of conducting an initial assessment of the attack, identifying a plan of action, and implementing the approved response.

The Government plans to initiate surge support services using the RFS process (**Section C.5**). The Government will provide the requirements for the timing of the contractor's response upon initiating the support. Surge support shall not result in a decrease of support to other TO requirements unless approved by the FEDSIM CO and FEDSIM COR.

The following applies to performing the cyber-attack surge support:

a. The Government will estimate the scope of surge support required at the time of the cyber-attack.

b. The contractor may be required to provide surge support at Agency spaces.

c. Once a cyber-attack response has ended, the contractor shall proceed with an orderly and efficient transition-out period. During the transition-out period, the contractor shall fully cooperate with, and assist the Government with, activities closing out the matter, developing required documentation, transferring knowledge, training, and lessons learned.

4 DELIVERABLES, INSPECTION, AND ACCEPTANCE

4.1 SCOPE OF INSPECTION

All deliverables will be inspected by the Contracting Officer's Representative (COR) for content, completeness, accuracy, and conformance under this agreement and the specifics of the project.

4.2 BASIS OF ACCEPTANCE

The basis for acceptance shall be compliance with the requirements set forth in the SOW, the contractor's quote, and other terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with the applicable provisions.

1) Reports, documents, and narrative type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected.

2) If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version.
3) All of the Government's comments to deliverables must either be incorporated in the succeeding version or the contractor must demonstrate, to the Government's satisfaction, why such comments should not be incorporated.
4) If the Government finds that a draft or final deliverable contains spelling errors, grammatical errors, improper format, or otherwise does not conform to the requirements stated within this contract, the document may be immediately rejected without further review and returned to the contractor for correction and re-submission. If the contractor requires additional Government guidance to produce an acceptable draft, the contractor shall arrange a meeting with the COR.

4.3 DRAFT AND FINAL DELIVERABLES

All written deliverables require at least two iterations – a draft and a final. The final document must be approved and accepted by the Government prior to payment submission. The contractor shall submit draft and final documents, using <Microsoft Office 2010/add or replace as applicable> or later, to the Government electronically. The Government requires <insert number> business days for review and submission of written comments to the contractor on draft and final documents. The contractor shall make revisions to the deliverables and incorporate the Government's comments into draft and final deliverables before submission. Upon receipt of the Government's comments, the contractor shall have <insert number> business days to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

Any issues that cannot be resolved by the contractor in a timely manner shall be identified and referred to the COR.

The COR is designated by the Contracting Officer (CO) to perform as the technical liaison between the contractor's management and the CO in routine technical matters constituting general program direction within the scope of the contract. Under no circumstances is the COR authorized to affect any changes in the work required under the contract, or enter into any agreement that has the effect of changing the terms and conditions of the contract or that causes the contractor to incur any costs. In addition, the COR will not supervise, direct, or control contractor employees.

Notwithstanding this provision, to the extent the contractor accepts any direction that constitutes a change to the contract without prior written authorization of the CO, costs incurred in connection therewith are incurred at the sole risk of the contractor, and if

invoiced under the contract, will be disallowed. On all matters that pertain to the contract/contract terms, the contractor must communicate with the CO.

Whenever, in the opinion of the contractor, the COR requests efforts beyond the terms of the contract, the contractor shall so advise the CO. If the COR persists and there still exists a disagreement as to proper contractual coverage, the CO shall be notified immediately, preferably in writing. Proceeding with work without proper contractual coverage may result in nonpayment or necessitate submission of a claim.

SAMPLE LIST OF DELIVERABLES

DELIVERABLE	SOW REFERENCE	DELIVERY DATE
Project Management Plans	Insert related SOW reference	No Later Than (NLT) <insert number of days> business days after task assignment
Organizational Conflict of Interest Plan	Insert related SOW reference	NLT <insert number of days> business days after award
Meeting Briefings/Presentations	Insert related SOW reference	NLT <insert number of days> business days prior to scheduled meeting
Status Reports	Insert related SOW reference	NLT the 15th of each month
Rules of Engagement	Insert related SOW reference	NLT <insert number of days> business days after award
Cyber Hunt Report	3.5.1	NLT <insert number of days> business days after task assignment
<Add other deliverables as applicable>	Insert related SOW reference	NLT <insert number of days> business days after task assignment

4.4 NON-CONFORMING DELIVERABLES

Non-conforming products or services will be rejected. Deficiencies will be corrected by the contractor within <insert number of days> business days of the rejection notice. If the deficiencies cannot be corrected within <insert number of days> business days, the contractor shall immediately notify the COR of the reason for the delay and provide a proposed corrective action plan within <insert number of days> business day