NOTE: All personnel for this Task Order must be full U.S. citizens. All personnel for this Task Order will be required to comply with a Non-Disclosure Agreement concerning the work performed in support of this Task Order.

1. Background

The National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. NIST's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems. In advancing its mission objectives, NIST must validate cryptographic modules, cryptographic algorithms, as well as ensure independent labs accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) are meeting performance criteria.

2. Objectives

NIST's Computer Security Division's (CSD) objective for this tasking includes operational and development support to the validation programs in the Security Testing, Validation, and Measurement (STVM) Group. Operational support includes tasks such as reviewing test reports, providing guidance to labs and vendors, and updating written documents for each of the validation programs. Development support includes tasks such as developing software that supports automation or process improvement for the validation programs, system maintenance, and system configuration.

3. Scope

The contractor shall provide support to the validation programs in the following areas:

1. Operational support to include test report review (Firm-Fixed Price)
2. Documentation support (Firm-Fixed Price)
3. Develop, integrate, and support testing tools and automation software (Labor Hour)

This task order is under the Cybersecurity and Privacy Support Services (CAPSS) IDIQ and is a hybrid firm-fixed price (FFP) and Labor Hour (LH) task order.

4. Related Documents

The following document is referenced in this Task Order and is relevant to the work specified. This document is publicly available at http://csrc.nist.gov/publications:

1. Federal Information Processing Standard (FIPS) 140, *Security Requirements for Cryptographic Modules*

5. Tasks

The contractor shall provide all labor, project oversight, administration, and technical execution of this project. The contractor is responsible for maintaining accurate records of project activities and shall provide the services described below.

5.1. Cryptographic Module Validation Program (CMVP) Operational Support (Firm-Fixed Price)

When Cryptographic and Security Test Laboratory (CSTL) test reports are submitted to the CMVP for review, there are multiple reviews of the test report to ensure the report findings satisfy the defined test requirements. The review process often involves coordination with the labs as questions about the reports are resolved. After all questions and comments about a report have been resolved and it is determined that the module satisfies defined test requirements, the module is awarded a validation certificate.

The test reports shall be reviewed for compliance to all current versions of FIPS 140 (see links below), the FIPS 140 Annexes, the Derived Test Requirements (DTR), and programmatic Implementation Guidance (IG) or the approved successors. Current versions of FIPS 140 documents, DTR, and IG can be downloaded from:

- **FIPS 140-2**: https://csrc.nist.gov/publications/detail/fips/140/2/final
- **FIPS 140-2 DTR**: https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/fips140-2/fips1402dtr.pdf
- **FIPS 140-2 IG**: https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/fips140-2/fips1402ig.pdf
- **FIPS 140-3**: https://csrc.nist.gov/publications/detail/fips/140/3/final
- **FIPS 140-3 DTR**: https://csrc.nist.gov/publications/detail/sp/800-140/final
- **FIPS 140-3 IG**: https://csrc.nist.gov/CSRC/media/Projects/cryptographic-module-validation-program/documents/fips%20140-3/FIPS%20140-3%20IG.pdf

The contractor shall use the current versions of CMVP documents as directed by the Technical Lead. The review of CMVP Test Reports may contain vendors' proprietary information and therefore will need to be controlled in a manner approved by STVM.

The contractor shall perform the review of up to 250 test reports following the current review procedures. If less than 250 test reports are available for review, then the contractor shall complete the review or coordination of all test reports that are assigned to the contractor.

5.2. Documentation Support

5.2.1. Cryptographic Validation Program (CVP) Automation Systems Documentation - (Firm-Fixed Price)

The contractor shall produce system design documentation, user documentation, and system deployment documentation for the software developed to automate cryptographic validation testing. The System Design Document shall describe all architectural details of the application. The User Document shall describe all application functionality. The Deployment Document shall describe application installation instructions.

5.2.2. CMVP Operational Documentation Support (Firm-Fixed Price)

The CMVP updates the Implementation Guidance (IG) document as needed to provide clarification of derived test requirements and report submission requirements. The contractor shall work with the NIST

COR and Technical Lead to update the IG on an as-needed basis (not to exceed 4 times per year) as identified by the COR and technical lead. The Government estimates this shall take no more than 80 hours during each of the task order periods.

5.3. Cryptographic Validation Program (CVP) Development and Deployment (Labor Hour)

The contractor shall develop and optimize automated capabilities to support the CVP which consists of the Cryptographic Algorithm Validation Program (CAVP) and the Cryptographic Module Validation Program (CMVP). The automated portion of the CAVP is referred to as the Automated Cryptographic Validation Program (ACVP). Software shall integrate with existing automation systems such as Resolve and the ACVP administrative application. In addition, software shall be capable of posting certificates on the NIST Computer Security Resource Center (CSRC). All software and services shall comply with NIST security requirements.

5.3.1. CAVP Systems

The contractor shall maintain and develop CAVP capabilities and services. The existing ACVP service shall be maintained to include bug fixes, security updates, and the new capabilities to accommodate changes in the validation program such as the addition of new algorithms. The integrated algorithm validation systems shall provide validation team members with a single web interface for processing test data, issuing and managing validation certificates, and coordinating with the laboratories, vendors, and validation program partners. ACVP Testing service shall be available for authorized users to submit algorithm test data for processing. If the test results comply with the algorithm specifications, then a validation certificate will be issued by the Government. All certificates shall be available on the CSRC site.

The contractor shall provide system engineering support to CAVP development projects such that they:

- Serve as primary system administration duties for the ACVP environment, to include:
  - Server maintenance, application of hotfixes, patches, and other updates (Windows, MSSQL, Java, JBoss, Teamcity, etc.) across all environments (up to four)
  - Conduct server instance health checks
- Create/update process documentation as needed relative to the environment and network architecture
- Receive and process requests from external users who request access to the ACVP Demo environment
  - Generate and install certificates for external users in Demo
- Administer, monitor, and maintain continuous build server configuration (TeamCity)
- Conduct ACVP software updates and quick fixes to the ACVP environments (Dev, Test, Demo and Prod)
- Work with ACVP development team members to assist in troubleshooting issues/bugs as they are discovered in the various environments
- Administer and maintain the virtual machines in local and cloud environments
- Conduct research and testing to help determine best path forward on upcoming feature implementations (such as distributed processing applications and the associated architecture requirements)

5.3.2. CMVP Systems

The contractor shall maintain and develop CMVP capabilities and services. The existing automation system, Resolve, shall be maintained to include bug fixes, security updates, and the addition of new capabilities to accommodate updates to the cryptographic module validation program. Changes to the CMVP may include, but are not limited to, changes in programmatic guidance, approved algorithms, or changes to the test requirements. Resolve shall provide validation program team members with a single web interface for processing test data, managing certificates, coordinating with laboratories, vendors, and other validation program partners. The contractor shall coordinate with the NIST technical lead on a biweekly basis prior to integrating the proposed solution in code. The work plan shall describe the contractor's proposed solution and milestones for delivery. As part of development and deployment, the contractor shall satisfy all CSD/NIST security requirements for the Authority to Operate (ATO). The contractor shall include deployment instructions. The contractor is expected to provide additional suggestions that may enhance the CVP program interaction with users, including vendors and CSTLs.

The contractor shall provide system engineering support to CMVP development projects such that they:

- Serve as primary system administration duties for the CMVP environment, to include:
    - Server maintenance, application of hotfixes, patches, and other updates (Windows, MSSQL, C#, Teamcity, etc.) across all environments (up to four)
    - Conduct server instance health checks
- Create/update process documentation as needed relative to the environment and network architecture
- Work with CMVP development team members to assist in troubleshooting issues/bugs as they are discovered in the various environments
- Conduct research and testing to help determine best path forward on upcoming feature implementations (New Cryptik, new processes for better automation and workflow)

5.4. Planning and Reporting (Firm-Fixed Price)

5.4.1. Kick-off Meeting and Work Plan

All work to be accomplished under this task order shall be managed through an Integrated Project Work Plan (IPWP). The contractor shall provide the initial IPWP at the kick-off meeting within 10 business days after award. NIST will approve the IPWP or provide comments for revision within 10 business days of delivery of the IPWP. After the contractor accepts and incorporates the comments, the IPWP will be considered the baseline for the work effort. The contractor shall provide status on the IPWP monthly and send the updated IPWP to the project stakeholders, to include the Government Contracting Officer's Representative (COR), Technical Lead and Project Sponsor (optional), as well as the contractor's Task Order Manager and Key Personnel (optional) at least 3 days prior to the monthly status meeting. The project plan shall contain government dependencies highlighted in yellow. Updates to the plan that do not impact the critical path can be resolved at the monthly status meeting as a function of the project plan. Changes that extend the period of performance or impact product delivery (i.e., removing PWS defined deliverables or adding new deliverables) will be addressed. However, no changes may be made to the contract without the Contracting Officer's approval. All anticipated changes shall be communicated to the Contracting Officer prior to execution of any changes to the Statement of Work and, if approved, will be formally revised by way of a bilateral modification via SF30 form. No work shall be performed outside of the established tasks or obligated funding without formal approval and execution by the Contracting Officer.

Also, at the kick-off meeting, the contractor shall provide their critical path analysis of the IPWP and the decomposition of the government Work Breakdown Structure (Figure 1) to the level of work packages. The IPWP shall include an identification of contractor resources, deliverables and completion dates, sequence of events, start dates, and duration for each activity.

5.4.2. Project Reporting

In addition to the Monthly IPWP updates described in Section 5.4.1, the contractor shall provide weekly technical status reports to ensure work progress is consistent with and will lead to successful completion of all tasks within the IPWP according to schedule.

Weekly status reports shall detail progress made during the prior week, progress expected during the next week, resources expended in terms of hours, any significant problems or issues encountered, recommended actions to resolve identified problems, and any variances from the baseline IPWP.

The contractor Task Order Manager for this work effort shall attend the standing monthly Program Manager’s meeting to provide a full status of the project using Microsoft Project, or similar application, to the government Program/Project Manager (P/PM), COR, and Project Sponsors. This meeting will typically be held on the NIST Gaithersburg campus and will typically last for 1 to 2 hours per meeting; however, if campus access is restricted at the time of this meeting due to COVID-19 restrictions, the meeting will be held virtually. A conference room with a projection system will be provided for use by the contractors to present their updates. This meeting will be hosted by the NIST P/PM for the contract (or their designee) and will typically be attended by the relevant government CORs, all relevant contractor PMs, and potentially government Tech Leads or Sponsors. A teleconference capability may be furnished if needed. At the discretion of the P/PM or COR, the contractor may be asked to conduct a monthly status meeting with the government technical leads and key personnel to resolve issues identified/presented at the standing monthly Program Manager’s meeting.

[This space intentionally left blank.]

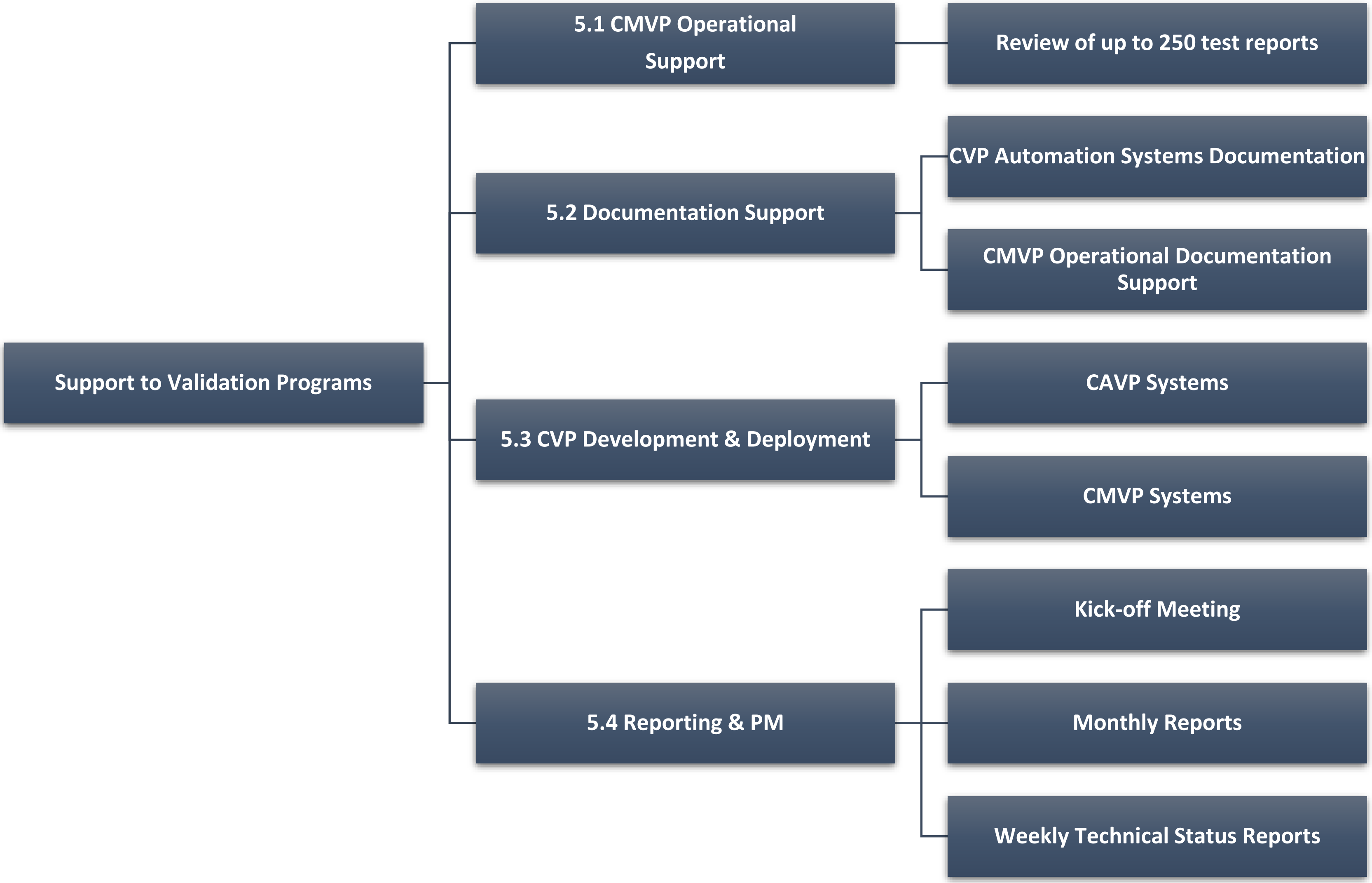
Support to Validation Programs
5.1 CMVP Operational Support
Review of up to 250 test reports
5.2 Documentation Support
CVP Automation Systems Documentation
CMVP Operational Documentation Support
5.3 CVP Development & Deployment
CAVP Systems
CMVP Systems
5.4 Reporting & PM
Kick-off Meeting
Monthly Reports
Weekly Technical Status Reports

Figure 1: Government Work Break Down Structure (WBS)

6. Deliverables, due dates, and Performance Requirements Summary (PRS)

All deliverables shall be posted to NIST’s shared drive or via another secure method (i.e., PGP files via email for proprietary information) as identified by the Technical Lead or the COR. Deliverables will be evaluated by the COR and the Technical Lead for completeness and the COR will either accept or reject the deliverables within 10 calendar days of contractor submission. All deliverables shall be provided to the COR.

Deliverable and Task	Description	Projected Completion Date	Media / Performance Standard	Monitoring Method
D1 – 5.1	Comment and Coordination of 250 CMVP Reports	Ongoing during period of performance	• MS Office • Comment sheet that can be tracked by STVM reviewers using Resolve	Submission package and resultant comments will be reviewed by CMVP qualified staff COR & Tech Lead will review feedback provided by CMVP qualified staff
D2 – 5.2.1	CVP Automated Systems Documentation	Ongoing during period of performance	• MS Word • System Design Document describes all architectural details of the application • User Document describes all application functionality • Deployment Document describes application installation instructions • Documents must be technical correct	CVP staff and Tech Lead will review for correctness and completeness. Tech Lead will confer with COR
D3 – 5.2.2	CMVP Operational Documentation	Monthly	• MS Word • Implementation Guidance sufficiently addresses the technical details of a particular cryptographic implementation issue to make the application of the standard understandable to the laboratory and vendor	CVP staff and Tech Lead will review for correctness and completeness. Tech Lead will confer with COR
D4 – 5.3.1	Logs of applied hotfixes, patches, and other updates	Ongoing during period of performance	• System logs • Logs clearly show when hotfixes, patches and other updates were made and by whom	CVP staff and Tech Lead will review for correctness and completeness. Tech Lead will confer with COR
D5 – 5.3.1	Evidence of server instance health checks	Ongoing during period of performance with	• MS Office / system logs • Evidence shows routine, periodic health checks of all applicable systems	CVP staff and Tech Lead will review for correctness

Deliverable and Task	Description	Projected Completion Date	Media / Performance Standard	Monitoring Method
		milestone dates to be set in the IPWP		and completeness. Tech Lead will confer with COR
D6 – 5.3.1	Updated documentation relative to the environment and network architecture	Ongoing during period of performance with milestone dates to be set in the IPWP	• MS Office • System Design Document describes all architectural details of the application • User Document describes all application functionality • Deployment Document describes application installation instructions • Documents must be technically correct	All updates will be reviewed by the Tech Lead before new versions of documents are considered final
D7 – 5.3.1	Completed JIRA tickets or other traceable evidence of responses to requests from external users	Ongoing during period of performance	• JIRA tickets / MS Office • JIRA tickets or other evidence clearly show who completed the responses and when • Completed tickets are marked appropriately	CVP staff and Tech Lead will review for correctness and completeness. Tech Lead will confer with COR
D8 – 5.3.1	Completed JIRA tickets or other traceable evidence of generated and installed certificates for external users	Ongoing during period of performance	• JIRA tickets / MS Office • JIRA tickets or other evidence clearly show who completed what certificates for whom • Completed tickets are marked appropriately	CVP staff and Tech Lead will review for correctness and completeness. Tech Lead will confer with COR
D9 – 5.3.1	New version of software must be uploaded to the various systems	Ongoing during period of performance with milestone dates to be set in the IPWP	• System logs • New versions of software must be fully tested and deployed on each system in turn • New versions of software will not be deployed straight to PROD without permission from the Tech Lead	CVP staff and Tech Lead will review for correctness and completeness. Tech Lead will confer with COR
D10 – 5.3.1	Completed JIRA tickets or other traceable evidence of updates made to the ACVP environments	Ongoing during period of performance with milestone dates to be set in the IPWP	• JIRA tickets / MS Office • JIRA tickets or other evidence clearly show who made what updates to which system and when • Completed tickets are appropriately marked	CVP staff and Tech Lead will review for correctness and completeness. Tech Lead will confer with COR
D11 – 5.3.1	Completed JIRA tickets or other traceable evidence of troubleshooting completed	Ongoing during period of performance	• JIRA tickets / MS Office • JIRA tickets or other evidence clearly show who did what troubleshooting, any changes made to the software or systems, and when • Completed tickets are appropriately marked	CVP staff and Tech Lead will review for correctness and completeness. Tech Lead will confer with COR

Deliverable and Task	Description	Projected Completion Date	Media / Performance Standard	Monitoring Method
D12 – 5.3.1	Functioning virtual machine infrastructure	Ongoing during period of performance	• System logs • All appropriate patches are applied according to NIST IT rules • Virtual machines in local and cloud environments are up and available 90% of the time per event logs	CVP staff and Tech Lead will review for correctness and completeness. Tech Lead will confer with COR
D13 – 5.3.1	Research notes and testing results	Ongoing during period of performance with milestone dates to be set in the IPWP	• MS Office / testing outputs • Research notes are clear and off professional quality • Testing results are complete and easily traceable to results of changes made	CVP staff and Tech Lead will review for correctness and completeness. Tech Lead will confer with COR
D14 – 5.3.2	Logs of applied hotfixes, patches, and other updates	Ongoing during period of performance	• System Logs • Logs clearly show when hotfixes, patches and other updates were made and by whom	CVP staff and Tech Lead will review for correctness and completeness. Tech Lead will confer with COR
D15 – 5.3.2	Evidence of server instance health checks	Ongoing during period of performance with milestone dates to be set in the IPWP	• MS Office / system logs • Evidence shows routine, periodic health checks of all applicable systems	CVP staff and Tech Lead will review for correctness and completeness. Tech Lead will confer with COR
D16 – 5.3.2	Updated documentation relative to the environment and network architecture	Ongoing during period of performance with milestone dates to be set in the IPWP	• MS Office • System Design Document describes all architectural details of the application • User Document describes all application functionality • Deployment Document describes application installation instructions • Documents must be technically correct	All updates will be reviewed by the Tech Lead before new versions of documents are considered final
D17 – 5.3.2	Completed JIRA tickets or other traceable evidence of troubleshooting completed	Ongoing during period of performance	• JIRA tickets / MS Office • JIRA tickets or other evidence clearly show who did what troubleshooting, any changes made to the software or systems, and when • Completed tickets are appropriately marked	CVP staff and Tech Lead will review for correctness and completeness. Tech Lead will confer with COR
D18 – 5.3.2	Research notes and testing results	Ongoing during period of performance with	• MS Office / testing outputs	CVP staff and Tech Lead will review for correctness

Deliverable and Task	Description	Projected Completion Date	Media / Performance Standard	Monitoring Method
		milestone dates to be set in the IPWP	• Research notes are clear and off professional quality • Testing results are complete and easily traceable to results of changes made	and completeness. Tech Lead will confer with COR
D19 – 5.4.1	Kick-off Meeting and Project Work Plan (IPWP)	Within 10 business days after award	• MS Excel / MS Project / email • Electronic copy of the agenda should be delivered to the COR at least 2 business days before the meeting • The Project Work Plan will be delivered no later than the Kick-off Meeting • The Project Work Plan shall include an identification of contractor resources, deliverables and completion dates, sequence of events, start dates, and duration for each activity • The Work Plan will be available in electronic format	COR Review
D20 – 5.4.2	Bi-Weekly Technical Status Report	Bi-Weekly	• MS Word / MS Outlook • Weekly status reports shall detail progress made during the prior week, progress expected during the next week, resources expended in terms of hours, any significant problems or issues encountered, recommended actions to resolve identified problems, and any variances from the baseline Project Work Plan	COR or Tech Lead review
D21 – 5.4.2	Monthly Status Report	Monthly	• MS PowerPoint / MS Project • Monthly status reports shall detail progress made during the prior month, progress expected during the next month, resources expended in terms of hours, any significant problems or issues encountered, recommended actions to resolve identified problems, and any variances from the baseline Project Work Plan • Current spend rate for any LH portions of the contract shall be listed	COR Review

7. Government-Furnished Property, Material, Equipment, or Information (GFP, GFM, GFE, or GFI)

Government-furnished property (materials, equipment, and/or information) (laptops, access tokens, and PIV Badges when appropriate) will be provided in conjunction with required performance under this task order. All work that is performed as a part of this effort will be conducted on government furnished equipment. All GFE will be utilized and maintained in accordance with NIST IT Security Rules.

8. Key Personnel Minimum Qualifications

All personnel for this Task Order must be full U.S. citizens. All personnel for this Task Order will be required to comply with a Non-Disclosure Agreement concerning the work performed in support of this Task Order.

It is expected that this work will require the contractor to assign at least four (4) key personnel. Contractor Key Personnel shall meet the following minimum qualifications for each of the respective required key personnel positions.

8.1. Program Manager 2 – Task Order Level

Minimum/General Experience:
This position requires a minimum of 6 years' general project management experience and 4 years' experience in managing projects involving physical sciences, engineering, mathematics, or IT-related fields, including cybersecurity and/or privacy. At least 2 years' experience managing contracted projects for a US federal agency. Experience includes increasing responsibilities in project management.

Functional Responsibilities: Duties may include but are not limited to: Serves as project manager for a large, complex task order and shall assist the Lead Program Manager in working with the ordering activity Contracting Officer (CO), the Federal Acquisitions Contract - Project/Program Manager (FAC-P/PM), the contract-level Contracting Officer's Representative (COR), and the task order-level COR(s), ordering activity management of personnel and NIST representatives. The Project Manager is responsible for the overall management of the specific task order(s) and ensuring that the technical solutions and schedules in the task order are implemented in a timely manner. Performs enterprise-wide horizontal integration planning and interfaces to other functional systems.

Minimum Certification/Education: Must either be certified as a.) Project Management Professional (PMP) by the Project Management Institute (PMI) or other such credentialing organization, or b.) Have been or currently are certified as a FAC- Program/Project Manager (P/PM) (Mid or Senior level). A Defense Systems Management College (DSMC) Program Management (PM) certification of Level 2 or 3 will be considered equivalent to a FAC-P/PM Mid or Senior Level. A Master's Degree in Project Management can be substituted for 2 years' project management experience.

8.2. Additional Key Personnel

In addition to the Program Manager 2 key personnel, the contractor shall assign key personnel for the additional positions detailed below. The following Labor Category titles are not necessarily required, they are examples of potentially relevant Labor Categories. However, the information given below is Specialty Knowledge that is required in addition to the minimum qualifications found in the list of IDIQ required labor categories. Key personnel proposed for these positions must be proposed under labor categories from the list of required IDIQ labor categories, must meet the minimum qualifications associated with the labor category they are proposed under, plus meet the Specialty Knowledge requirements listed below:

Developer 4 and/or 5 - Specialty Knowledge (C# Developer):
Developer shall have at least 2 years of developing web-based applications using the Microsoft .Net framework.

Developer 4 and/or 5 Specialty Knowledge (SQL Server Database Developer):
Shall have 2 years of experience in developing applications that use a SQL Server database. Shall have experience with SQL, stored procedures, schema creation, XML integration, and automated import/export scripts.

Developer 4 and/or 5 Specialty Knowledge (Cryptographic modules):

Personnel will be expected to learn and understand the business logic of the CAVP/CMVP workflows and help assess and implement that logic into the tools they develop. It is expected that in performing the submission reviews, the contractor will become familiar with the business processes, aiding all validation work.

9. Travel

No Travel is required for this Task Order.

10.Risk Level

The risk level for this Task Order is considered Moderate.

11.Place of Performance

All work shall be performed virtually until COVID-19 restrictions have been lifted from NIST’s Gaithersburg campus. When those restrictions are lifted, a percentage of the work will occur on campus. This percentage will be determined by the COR and Tech Lead based on the needs of the program at that time.

12.Period of Performance

The period of performance shall be for 12 months from effective date of award.