



**GENERAL SERVICES ADMINISTRATION
Federal Supply Service
Authorized Federal Supply Schedule Price List**

**Schedule Title: Multiple Award Schedule
FSC Group: 7030, J070, D305, D399, U012**

On-line access to contract ordering information, terms and conditions, up-to-date pricing, and the option to create an electronic delivery order are available through GSA Advantage!®, a menu-driven database system. The INTERNET address GSA Advantage!® is: GSAAdvantage.gov.

Contract Number: 47QTCA19D008R
Contract Period: March 27, 2019 through March 26, 2024

MERLIN INTERNATIONAL, INC.
8330 Boone Blvd., Ste 800
Vienna, VA 22182-2624
Phone: 703-752-2928
Fax: 703-752-2935
Internet Address: www.merlin-intl.com

Business Size: Large

For more information on ordering from Federal Supply Schedules go to the GSA Schedules page at GSA.gov.

Pricelist Current Through Modification #0020

CUSTOMER INFORMATION

1a. Table of awarded special item number(s) with appropriate cross-reference to item descriptions and awarded price(s).

Special Item No. 511210 Software Licenses*

Special Item No. 54151 Software Maintenance Services*

Special Item No. 518210C Cloud & Cloud Related IT Professional Services*

Special Item No. 541519CDM Continuous Diagnostics and Mitigation (CDM) Tools*

Special Item No. 611420 Information Technology Training*

Special Item No. OLM Order Level Materials (OLM)*

**All SINs awarded under Cooperative Purchasing and Disaster Recovery*

1b. Identification of the lowest priced model number and lowest unit price for that model for each special item number awarded in the contract.

See GSA Price List

1c. If the Contractor is proposing hourly rates:

Not Applicable

2. Maximum order.

SIN 611420: \$250,000

SIN OLM: \$250,000

All other SINs: \$500,000

**Ordering activities may request a price reduction at any time before placing an order, establishing a BPA, or in conjunction with the annual BPA review. However, the ordering activity shall seek a price reduction when the order or BPA exceeds the simplified acquisition threshold. Schedule contractors are not required to pass on to all schedule users a price reduction extended only to an individual ordering activity for a specific order or BPA.*

3. Minimum order.

\$100

4. Geographic coverage (delivery area).

Domestic delivery is delivery within the 48 contiguous states, Alaska, Hawaii, Puerto Rico, Washington, DC, and U.S. Territories. Domestic delivery also includes a port or consolidation point, within the aforementioned areas, for orders received from overseas activities.

5. Point(s) of production (city, county, and State or foreign country).

United States



6. Discount from list prices or statement of net price.
Government prices are net.

7. Quantity discounts.
None

8. Prompt payment terms.
0% - 30 days from receipt of invoice or date of acceptance, whichever is later.
Information for Ordering Offices: Prompt payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions.

9. Foreign items.
None

10a. Time of delivery.	<i>DELIVERY TIME (Days ARO)</i>
<i>SPECIAL ITEM NUMBER</i>	
<i>511210</i>	<i>30 Days</i>
<i>54151</i>	<i>Upon mutual agreement with Ordering Agency</i>
<i>518210C</i>	<i>Upon mutual agreement with Ordering Agency</i>
<i>541519CDM</i>	<i>Upon mutual agreement with Ordering Agency</i>
<i>611420</i>	<i>Upon mutual agreement with Ordering Agency</i>
<i>OLM</i>	<i>Upon mutual agreement with Ordering Agency</i>

10b. Expedited Delivery.
Contact Contractor for availability

10c. Overnight and 2-day delivery.
Contact Contractor for availability

10d. Urgent Requirements.
Contact Contractor

11. F.O.B. point(s).
Destination

12a. Ordering address:
Merlin International, Inc.
8330 Boone Blvd., Ste 800
Vienna, VA 22182-2624

12b. Ordering procedures: For supplies and services, the ordering procedures, information on Blanket Purchase Agreements (BPA's) are found in Federal Acquisition Regulation (FAR) 8.405-3.

13. Payment address.
Contact Contractor

14. Warranty provision.
Unless specified otherwise in this contract, manufacturer's standard commercial guarantee/warranty, as stated in manufacturer's standard commercial terms and conditions, will apply to this contract.

Contractor warrants and implies that the items delivered hereunder are merchantable and fit for use for a particular purpose described in this contract, except to the extent that such implied warranties have been excluded in the applicable manufacturer's standard commercial terms and conditions in accordance with FAR 12.204(b)(2). Except as otherwise provided by an express or implied warranty, the Contractor will not be liable to the ordering activity for consequential damages resulting from any defect or deficiencies in accepted items.

15. Export packing charges:
Not Applicable

16. Terms and conditions of rental, maintenance, and repair (if applicable)
Contact Contractor

17. Terms and conditions of installation (if applicable)
Products are normally self-installable; if assistance is necessary with installation, contact Contractor.

18a. Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices (if applicable).
Not Applicable

18b. Terms and conditions for any other services (if applicable).
Not Applicable

19. List of service and distribution points (if applicable).
Not Applicable

20. List of participating dealers (if applicable).
Not Applicable

21. Preventive maintenance (if applicable).

Not Applicable

22a. Special attributes such as environmental attributes

None

22b. If applicable, indicate that Section 508 compliance information is available on Electronic and Information Technology (EIT) supplies and services and show where full details can be found (e.g. contractor's website or other location.) The EIT standards can be found at: www.Section508.gov/.

Contact Contractor for availability of Voluntary Product Accessibility Template (VPAT) or equivalent qualification from the applicable manufacturer.

23. Data Universal Number System (DUNS) number.

07-352-1101

24. Notification regarding registration in System for Award Management (SAM) database.

CAGE Code: 1XAZ0

TERMS AND CONDITIONS APPLICABLE TO TERM SOFTWARE LICENSES
(SPECIAL ITEM NUMBER 511210), AND MAINTENANCE AS A SERVICE
(SPECIAL ITEM NUMBER 54151) OF GENERAL PURPOSE COMMERCIAL
INFORMATION TECHNOLOGY SOFTWARE

1. INSPECTION/ACCEPTANCE

The Contractor shall only tender for acceptance those items that conform to the requirements of this contract. The ordering activity reserves the right to inspect or test any software that has been tendered for acceptance. The ordering activity may require repair or replacement of nonconforming software at no increase in contract price. The ordering activity must exercise its post acceptance rights (1) within a reasonable time after the defect was discovered or should have been discovered; and (2) before any substantial change occurs in the condition of the software, unless the change is due to the defect in the software.

2. ENTERPRISE USER LICENSE AGREEMENTS REQUIREMENTS (EULA)

Manufacturer EULAs are incorporated as part of this contract.

3. GUARANTEE/WARRANTY

a. Unless specified otherwise in this contract, the Contractor's standard commercial guarantee/warranty as stated in the contract's commercial pricelist will apply to this contract.

b. The Contractor warrants and implies that the items delivered hereunder are merchantable and fit for use for the particular purpose described in this contract. If no implied warranties are given, an express warranty of at least 60 days must be given in accordance with FAR 12.404(b)(2)

c. Limitation of Liability. Except as otherwise provided by an express or implied warranty, the Contractor will not be liable to the ordering activity for consequential damages resulting from any defect or deficiencies in accepted items.

4. TECHNICAL SERVICES

The Contractor, without additional charge to the ordering activity, shall provide a hot line technical support number 703-752-2928 for the purpose of providing user assistance and guidance in the implementation of the software.

5. SOFTWARE MAINTENANCE

a. Software maintenance as it is defined:

Software Maintenance as a Product (SIN 511210) Software maintenance as a product includes the publishing of bug/defect fixes via patches and updates/upgrades in function and technology to maintain the operability and usability of the software product. It may also include other no charge support that is included in the purchase price of the product in the commercial marketplace. No charge support includes items such as user blogs, discussion forums, on-line help libraries and FAQs (Frequently Asked Questions), hosted

chat rooms, and limited telephone, email and/or web-based general technical support for user's self-diagnostics. Software maintenance as a product does NOT include the creation, design, implementation, integration, etc. of a software package. These examples are considered software maintenance as a service. Software Maintenance as a product is billed at the time of purchase.

Software Maintenance as a Service (SIN 54151)

Software maintenance as a service creates, designs, implements, and/or integrates customized changes to software that solve one or more problems and is not included with the price of the software. Software maintenance as a service includes person-to-person communications regardless of the medium used to communicate: telephone support, on-line technical support, customized support, and/or technical expertise which are charged commercially. Software maintenance as a service is billed arrears in accordance with 31 U.S.C. 3324. Software maintenance as a service is billed in arrears in accordance with 31 U.S.C. 3324.

b. Invoices for maintenance service shall be submitted by the Contractor on a quarterly or monthly basis, after the completion of such period. Maintenance charges must be paid in arrears (31 U.S.C. 3324). PROMPT PAYMENT DISCOUNT, IF APPLICABLE, SHALL BE SHOWN ON THE INVOICE.

6. PERIODS OF LICENSES (SIN 511210) AND MAINTENANCE (SIN 54151) a. The Contractor shall honor orders for periods for the duration of the contract period or a lesser period of time.

b. Term licenses and/or maintenance may be discontinued by the ordering activity on thirty (30) calendar days written notice to the Contractor

c. Annual Funding. When annually appropriated funds are cited on an order for term licenses and/or maintenance, the period of the term licenses and/or maintenance shall automatically expire on September 30 of the contract period, or at the end of the contract period, whichever occurs first. Renewal of the term licenses and/or maintenance orders citing the new appropriation shall be required, if the term licenses and/or maintenance is to be continued during any remainder of the contract period.

d. Cross-Year Funding Within Contract Period. Where an ordering activity's specific appropriation authority provides for funds in excess of a 12-month (fiscal year) period, the ordering activity may place an order under this schedule contract for a period up to the expiration of the contract period, notwithstanding the intervening fiscal years. e. Ordering activities should notify the Contractor in writing thirty (30) calendar days prior to the expiration of an order, if the term licenses and/or maintenance is to be terminated at that time. Orders for the continuation of term licenses and/or maintenance will be required if the term licenses and/or maintenance is to be continued during the subsequent period.

7. CONVERSION FROM TERM LICENSE TO PERPETUAL LICENSE

Conversion from Term License to Perpetual License is not offered.

8. TERM LICENSE CESSATION

Term License Cessation is not offered.

9. UTILIZATION LIMITATIONS - (SIN 511210 AND SIN 54151)

a. Software acquisition is limited to commercial computer software defined in FAR Part 2.101.

b. When acquired by the ordering activity, commercial computer software and related documentation so legend shall be subject to the following:

(1) Title to and ownership of the software and documentation shall remain with the Contractor, unless otherwise specified.

(2) Software licenses are by site and by ordering activity. An ordering activity is defined as a cabinet level or independent ordering activity. The software may be used by any subdivision of the ordering activity (service, bureau, division, command, etc.) that has access to the site the software is placed at, even if the subdivision did not participate in the acquisition of the software. Further, the software may be used on a sharing basis where multiple agencies have joint projects that can be satisfied by the use of the software placed at one ordering activity's site. This would allow other agencies access to one ordering activity's database. For ordering activity public domain databases, user agencies and third parties may use the computer program to enter, retrieve, analyze and present data. The user ordering activity will take appropriate action by instruction, agreement, or otherwise, to protect the Contractor's proprietary property with any third parties that are permitted access to the computer programs and documentation in connection with the user ordering activity's permitted use of the computer programs and documentation. For purposes of this section, all such permitted third parties shall be deemed agents of the user ordering activity.

(3) Except as is provided in paragraph 9.b(2) above, the ordering activity shall not provide or otherwise make available the software or documentation, or any portion thereof, in any form, to any third party without the prior written approval of the Contractor. Third parties do not include prime Contractors, subcontractors and agents of the ordering activity who have the ordering activity's permission to use the licensed software and documentation at the facility, and who have agreed to use the licensed software and documentation only in accordance with these restrictions. This provision does not limit the right of the ordering activity to use software, documentation, or information therein, which the ordering activity may already have or obtains without restrictions.

(4) The ordering activity shall have the right to use the computer software and documentation with the computer for which it is acquired at any other facility to which that computer may be transferred, or in cases of Disaster Recovery, the ordering activity has the right to transfer the software to another site if the ordering activity site for which it is acquired is deemed to be unsafe for ordering activity personnel; to use the computer software and documentation with a backup computer when the primary computer is inoperative; to copy computer programs for safekeeping (archives) or backup purposes; to transfer a copy of the software to another site for purposes of benchmarking new hardware

and/or software; and to modify the software and documentation or combine it with other software, provided that the unmodified portions shall remain subject to these restrictions.

(5) "Commercial Computer Software" may be marked with the Contractor's standard commercial restricted rights legend, but the schedule contract and schedule pricelist, including this clause, "Utilization Limitations" are the only governing terms and conditions, and shall take precedence and supersede any different or additional terms and conditions included in the standard commercial legend.

10. SOFTWARE CONVERSIONS - (SIN 511210)

Full monetary credit will be allowed to the ordering activity when conversion from one version of the software to another is made as the result of a change in operating system , or from one computer system to another. Under a perpetual license, the purchase price of the new software shall be reduced by the amount that was paid to purchase the earlier version. Under a term license, conversion credits which accrued while the earlier version was under a term license shall carry forward and remain available as conversion credits which may be applied towards the perpetual license price of the new version.

11. DESCRIPTIONS AND EQUIPMENT COMPATIBILITY

The Contractor shall include, in the schedule pricelist, a complete description of each software product and a list of equipment on which the software can be used. Also, included shall be a brief, introductory explanation of the modules and documentation which are offered.

12. RIGHT-TO-COPY PRICING

Right-to-copy licenses are not offered.

TERMS AND CONDITIONS APPLICABLE TO PURCHASE OF CLOUD & CLOUD RELATED IT PROFESSIONAL SERVICES (SPECIAL ITEM NUMBER 518210C)

1. SCOPE

The prices, terms and conditions stated under Special Item Number (SIN) 518210C Cloud & Cloud-Related IT Professional Services apply exclusively to Cloud Computing Services (i.e. IaaS, etc.) and Cloud-Related Professional Services within the scope of this Information Technology Schedule. This SIN provides ordering activities with access to Cloud (i.e. SaaS, etc.) technical services that run in cloud environments and meet the NIST Definition of Cloud Computing Essential Characteristics. Cloud Services [(i.e. SaaS, etc.)] relating to or impinging on cloud that do not meet all NIST essential characteristics should be listed in other SINs. The scope of this SIN is limited to cloud capabilities provided entirely as a “pay as you go” service and cloud-related IT professional services. Hardware, software and other artifacts acquired to supporting the physical construction of a private or other cloud are out of scope for this SIN. Currently, an Ordering Activity can procure the hardware and software needed to to build private on premise cloud functionality, through combining different services on other IT SINs.

Sub-categories in scope for this SIN are the three NIST Service Models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Offerors may optionally select a single sub-category that best fits a proposed cloud service offering. Only one sub-category may be selected per each proposed cloud service offering. Offerors may elect to submit multiple cloud service offerings, each with its own single sub-category. The selection of one of three sub-categories does not prevent Offerors from competing for orders under the other two sub-categories. See service model guidance for advice on sub-category selection. Sub-category selection within this SIN is optional for any individual cloud service offering, and new cloud computing service (i.e. IaaS, etc.) technologies that do not align with the aforementioned three sub-categories may be included without a sub-category selection so long as they comply with the essential characteristics of cloud computing as outlined by NIST.

2. DESCRIPTION OF CLOUD COMPUTING SERVICES

Merlin International, Inc. will respond to each service requirement as it relates to each cloud computing service offered under the contract.

3. RESPONSIBILITIES OF THE CONTRACTOR

The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character.

a. Acceptance Testing Any required Acceptance Test Plans and Procedures shall be negotiated by the Ordering Activity at task order level. The Contractor shall perform acceptance testing of the systems for Ordering Activity approval in accordance with the approved test procedures.

- b. Training If training is provided commercially the Contractor shall provide normal commercial installation, operation, maintenance, and engineering interface training on the system. Contractor is responsible for indicating if there are separate training charges.
- c. Information Assurance/Security Requirements The contractor shall meet information assurance/security requirements in accordance with the Ordering Activity requirements at the Task Order level.
- d. Related Professional Services The Contractor is responsible for working with the Ordering Activity to identify related professional services and any other services available on other SINs that may be associated with deploying a complete cloud service (i.e. IaaS, etc.) solution. Any additional substantial and ongoing IT professional services related to the offering such as assessing, preparing, refactoring, migrating, DevOps, developing new cloud based applications and managing/governing a cloud implementation may be offered per the guidelines below.
- e. Performance of Cloud Computing Services (i.e. IaaS, etc.) The Contractor shall respond to Ordering Activity requirements at the Task Order level with proposed capabilities to Ordering Activity performance specifications or indicate that only standard specifications are offered. In all cases the Contractor shall clearly indicate standard service levels, performance and scale capabilities. The Contractor shall provide appropriate cloud computing services (i.e. IaaS, etc.) on the date and to the extent and scope agreed to by the Contractor and the Ordering Activity.
- f. Reporting The Contractor shall respond to Ordering Activity requirements and specify general reporting capabilities available for the Ordering Activity to verify performance, cost and availability. In accordance with commercial practices, the Contractor may furnish the Ordering Activity/user with a monthly summary Ordering Activity report.

4. RESPONSIBILITIES OF THE ORDERING ACTIVITY

The Ordering Activity is responsible for indicating the cloud computing services requirements unique to the Ordering Activity. Additional requirements should not contradict existing SIN or IT Terms and Conditions. Ordering Activities should include (as applicable) Terms & Conditions to address Pricing, Security, Data Ownership, Geographic Restrictions, Privacy, SLAs, etc. Cloud services typically operate under a shared responsibility model, with some responsibilities assigned to the Cloud Service Provider (CSP), some assigned to the Ordering Activity, and others shared between the two. The distribution of responsibilities will vary between providers and across service models. Ordering activities should engage with CSPs to fully understand and evaluate the shared responsibility model proposed. Federal Risk and Authorization Management Program (FedRAMP) documentation will be helpful regarding the security aspects of shared responsibilities, but operational aspects may require additional discussion with the provider.

a. Ordering Activity Information Assurance/Security Requirements Guidance

(1) The Ordering Activity is responsible for ensuring to the maximum extent practicable that each requirement issued is in compliance with the Federal Information Security Management Act (FISMA) as applicable.

(2) The Ordering Activity shall assign a required impact level for confidentiality, integrity and availability (CIA) prior to issuing the initial statement of work.² The Contractor must be capable of meeting at least the minimum security requirements assigned against a low-impact information system in each CIA assessment area (per FIPS 200) and must detail the FISMA capabilities of the system in each of CIA assessment area.

(3) Agency level FISMA certification, accreditation, and evaluation activities are the responsibility of the Ordering Activity. The Ordering Activity reserves the right to independently evaluate, audit, and verify the FISMA compliance for any proposed or awarded Cloud Computing Services.

(4) The Ordering Activity has final responsibility for assessing the FedRAMP status of the service, complying with and making a risk-based decision to grant an Authorization to Operate (ATO) for the cloud computing service, and continuous monitoring. A memorandum issued by the Office of Management and Budget (OMB) on Dec 8, 2011 outlines the responsibilities of Executive departments and agencies in the context of FedRAMP compliance.

(5) Ordering activities are responsible for determining any additional information assurance and security related requirements based on the nature of the application and relevant mandates.

b. Deployment Model If a particular deployment model (Private, Public, Community, or Hybrid) is desired, Ordering Activities are responsible for identifying the desired model(s). Alternately, Ordering Activities could identify requirements and assess Contractor responses to determine the most appropriate deployment model(s).

c. Delivery Schedule The Ordering Activity shall specify the delivery schedule as part of the initial requirement. The Delivery Schedule options are found in Information for Ordering Activities Applicable to All Special Item Numbers.

d. Interoperability Ordering Activities are responsible for identifying interoperability requirements. Ordering Activities should clearly delineate requirements for API implementation and standards conformance.

e. Performance of Cloud Computing Services The Ordering Activity should clearly indicate any custom minimum service levels, performance and scale requirements as part of the initial requirement.

f. Reporting The Ordering Activity should clearly indicate any cost, performance or availability reporting as part of the initial requirement.

g. Privacy The Ordering Activity should specify the privacy characteristics of their service and engage with the Contractor to determine if the cloud service is capable of meeting Ordering Activity requirements.

h. Accessibility The Ordering Activity should specify the accessibility characteristics of their service and engage with the Contractor to determine the cloud service is capable of meeting Ordering Activity requirements. For example, a requirement could require assurance that the service is capable of providing accessibility based on Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d).

i. Geographic Requirements Ordering activities are responsible for specifying any geographic requirements and engaging with the Contractor to determine that the cloud services offered have the capabilities to meet geographic requirements for all anticipated

task orders. Common geographic concerns could include whether service data, processes and related artifacts can be confined on request to the United States and its territories, or the continental United States (CONUS).

j. Data Ownership and Retrieval and Intellectual Property Intellectual property rights are not typically transferred in a cloud model. In general, CSPs retain ownership of the Intellectual Property (IP) underlying their services and the customer retains ownership of its intellectual property. The CSP gives the customer a license to use the cloud services (i.e. IaaS, etc.) for the duration of the contract without transferring rights. The government retains ownership of the IP and data they bring to the customized use of the service as spelled out in the FAR and related materials.

General considerations of data ownership and retrieval are covered under the terms of Information Technology Terms and the FAR and other laws, ordinances, and regulations (Federal, State, City, or otherwise). Because of considerations arising from cloud shared responsibility models, ordering activities should engage with the Contractor to develop more cloud specific understandings of the boundaries between data owned by the government and that owned by the cloud service provider, and the specific terms of data retrieval. In all cases, the Ordering Activity should enter into an agreement with a clear and enforceable understanding of the boundaries between government and cloud service provider data, and the form, format and mode of delivery for each kind of data belonging to the government. The Ordering Activity should expect that the Contractor shall transfer data to the government at the government's request at any time, and in all cases when the service or order is terminated for any reason, by means, in formats and within a scope clearly understood at the initiation of the service.

k. Service Location Distribution The Ordering Activity should determine requirements for continuity of operations and performance and engage with the Contractor to ensure that cloud services have adequate service location distribution to meet anticipated requirements. Typical concerns include ensuring that:

(1) Physical locations underlying the cloud are numerous enough to provide continuity of operations and geographically separate enough to avoid an anticipated single point of failure within the scope of anticipated emergency events.

(2) Service endpoints for the cloud are able to meet anticipated performance requirements in terms of geographic proximity to service requestors. Note that cloud providers may address concerns in the form of minimum distance between service locations, general regions where service locations are available, etc.

5 subcategories represent the scope of the CDM program and reflect widely exercised functional and operational scenarios that CDM is interested in identifying, monitoring and addressing from a security perspective. To provide a holistic security approach, these capabilities adhere to the National Institute of Science and Technology (NIST) Cybersecurity Framework security functions to identify, protect, detect, respond and recover. CDM also supports and can be used in the NIST Risk Management Framework (RMF) to achieve ongoing assessment and authorization. As shown in Table 1, the 5 CDM Tools SIN subcategories cover the previous CDM BPA 15 CDM Tool Functional Areas (TFAs) and allow for future innovation. Table 1: SIN to TFA mapping

TERMS AND CONDITIONS APPLICABLE TO CONTINUOUS DIAGNOSTICS AND MIGRATION TOOLS (SPECIAL ITEM NUMBER 541519CDM)

1. SCOPE

a. Special Item Number (SIN) 541519CDM Continuous Diagnostics and Mitigation (CDM) Tools is a solutions SIN. This SIN includes both hardware and software products and any associated services for the products to include installation, maintenance, and training. NOTE: All hardware and software may remain under those SINs unless the items are specific to the CDM SIN.

b. CDM Tools SIN products and associated services shall comply with all certifications and industry standards as specified by the ordering activity.

c. The Contractor shall provide services at the Contractor's facility and/or at the ordering activity location, as agreed to by the Contractor and the ordering activity. The Contractor shall deliver to any location within the geographic scope of this contract.

d. 541519CDM - Continuous Diagnostics and Mitigation Tools - SUBJECT TO COOPERATIVE PURCHASING - Includes Continuous Diagnostics and Mitigation (CDM) Approved Products List (APL) hardware and software products/tools and associated services. The full complement of CDM subcategories includes tools, associated maintenance, and other related activities such as training.

e. The 5 subcategories CDM capabilities specified under this SIN are:

- (1) Manage "What is on the network?": Identifies the existence of hardware, software, configuration characteristics and known security vulnerabilities.
- (2) Manage "Who is on the network?": Identifies and determines the users or systems with access authorization, authenticated permissions and granted resource rights.
- (3) Manage "How is the network protected?": Determines the user/system actions and behavior at the network boundaries and within the computing infrastructure.
- (4) Manage "What is happening on the network?": Prepares for events/incidents, gathers data from appropriate sources; and identifies incidents through analysis of data.
- (5) Emerging Tools and Technology: Includes CDM cybersecurity tools and technology not in any other subcategory.

5 subcategories represent the scope of the CDM program and reflect widely exercised functional and operational scenarios that CDM is interested in identifying, monitoring and addressing from a security perspective.

To provide a holistic security approach, these capabilities adhere to the National Institute of Science and Technology (NIST) Cybersecurity Framework security functions to identify, protect, detect, respond and recover. CDM also supports and can be used in the NIST Risk Management Framework (RMF) to achieve ongoing assessment and authorization.

As shown in Table 1, the 5 CDM Tools SIN subcategories cover the previous CDM BPA 15 CDM Tool Functional Areas (TFAs) and allow for future innovation.

Table 1: SIN to TFA mapping

5 SIN Subcategories	15 CDM BPA TFAs
1. Manage “What is on the network?”	<ul style="list-style-type: none"> ● TFA 1 – Hardware Asset Management ● TFA 2 – Software Asset Management ● TFA 3 – Configuration Settings Management ● TFA 4 – Vulnerability Management
2. Manage “Who is on the network?”	<ul style="list-style-type: none"> ● TFA 6 – Manage Trust in People Granted Access ● TFA 7 – Manage Security-Related Behavior ● TFA 8 – Manage Credential and Authentication ● TFA 9 – Manage Account/Access/Manage Privileges
3. Manage “How is the boundary protected?” for BOUND	<ul style="list-style-type: none"> ● TFA 5 – Manage Network Access Controls
4. Manage “What is happening on the network?” for MNGEVT	<ul style="list-style-type: none"> ● TFA 10 – Prepare for Contingencies and Incidents ● TFA 11 – Respond to Contingencies and Incidents
4. Manage “What is happening on the network?” for DBS	<ul style="list-style-type: none"> ● TFA 12 – Design and Build in Requirements Policy and Planning ● TFA 13 – Design and Build in Quality
4. Manage “What is happening on the network?” for OMI	<ul style="list-style-type: none"> ● TFA 14 – Manage Audit Information ● TFA 15 – Manage Operation Security
5. Emerging Tools and Technologies	Future innovations

(1) Manage “What is on the network?”

Focus: The primary focus of Manage Assets is to identify “What is on the network?”; that is, to identify the existence of hardware, software, configuration characteristics and known security vulnerabilities.

Manage hardware and software baseline system inventory is based on Phase 1 Hardware Asset Management (HWAM) and Software Asset Management (SWAM) requirements that requires the discovery and identification of devices to define a baseline of inventory hardware and software assets to establish the Agency's span of control.

Hardware and software configurations are based on Phase 1 Configuration Settings Management (CSM) requirements to ensure that hardware and software (specifically the operating system and installed applications) assets are securely configured and hardened.

Manage vulnerabilities is based on Phase 1 Vulnerability Management (VUL) requirements to identify and manage vulnerabilities in software installed on network devices to minimize exploitation of known software weaknesses.

These CDM capabilities cover verification and validation for the existence of hardware infrastructure devices; the accurate identification of approved software components; verification and validation that hardware devices have the correct security configuration settings, and system platform is hardened to reduce the platform attack surface; and the identification and management of risks presented by known software weaknesses that are subject to exploitation. These CDM capabilities support the Cybersecurity Framework functions of: identify, protect and detect.

(2) Manage "Who is on the network?"

Focus: The primary focus of Manage People is to determine "Who is on the network?"; that is, identify and determine the users or systems with authorized access.

Manage People is based on Phase 2 PRIV, CRED, TRUST and BEHAVE requirements that require the management of users/accounts as an asset to assure the appropriate individual has the right access to the right resource.

This CDM capability covers the verification and validation of allowed user privileges, issuance and management of user owned credentials, appropriate user security behavior training, trustworthiness, authenticated permissions, and management of resource access rights granted to users.

These CDM capabilities support the Cybersecurity Framework functions of: identify, protect and detect.

(3) Manage "How is the boundary protected?"

Focus: The primary focus of Mange Boundary Protection is to determine "How is the boundary protected?"; that is, to determine the user/system actions and behavior at the physical/logical network boundaries and within the computing infrastructure.

“How is the boundary protected?” is based on Phase 3 BOUND requirements to defend physical and logical network boundaries and identify abnormal behavior (of networks and users) that may identify that an incident has occurred.

This CDM capability covers verification and validation of logical and physical network interfaces to reduce intrusive, malicious, and disruptive attacks; cryptographic mechanisms ensure confidentiality and integrity of data on the network; and methods to identify security incidents.

These CDM capabilities support the Cybersecurity Framework functions of: identify, protect and detect.

(4) Manage “What is happening on the network?”

Due to the complexity to manage “What is happening on the network?”, this area is covered by three focus areas:

- a. Manage Events (MNGEVT)
- b. Operate, Monitor and Improve (OMI)
- c. Design and Build in Security (DBS)

Manage Events

Focus: Manage Events is responsible for preparing for events/incidents, gathering appropriate audit data from appropriate sources, identifying incidents through analysis of data, and performing ongoing assessment.

Manage Events is based on the Phase 3 MNGEVT requirements to prepare for incidents/events (through processes, policies, and procedures), gather appropriate audit/log data from appropriate sources, and identify events/incidents (network and user abnormal behavior) through the analysis of audit/log data

Manage Events supports the runtime collection of attributes (actual state) and continuous monitoring of the policies related to attributes for Ongoing Assessment (actual state vs. desired state) to enhance current or apply new security and privacy controls and countermeasures. The results of the Ongoing Assessment will be used as inputs to OMI Ongoing Authorization risk assessment process to determine if the level of risk remains acceptable for a given information system to support continued authorization and operation.

Ongoing Assessment is the continuous process of comparing security related attributes between the Actual State and the Desired State. This comparison is performed by the CDM Policy Decision Point (PDP). The discrepancy between Actual State and Desired state impacts the security posture of the implementation of NIST SP 800-53 controls and countermeasures. The results of the Ongoing Assessment are used to evaluate the changes in risk posture associated with the discrepancy. Ideally, the Ongoing Assessment

process is fully automated with the Desired State being encoded in the CDM PDP and the Actual State being measured using CDM sensors.

This CDM capability covers verification and validation of processes, policies, and procedures supporting cybersecurity preparation, audit and log data collection, security analysis of audit/log data, incident reporting to provide forensic evidence of malicious or suspicious behavior, and ongoing assessment.

To provide a holistic security approach, this capability adheres to the Cybersecurity Framework security functions to identify, protect, detect, respond and recover CDM also supports and can be used in the NIST Risk Management Framework (RMF) to achieve ongoing assessment and authorization.

Operate, Monitor and Improve

Focus: Operate, Monitor and Improve is responsible for audit data aggregation, correlation, and analysis, incident prioritization and response, and post-incident activities (e.g., information sharing).

Operate, Monitor and Improve is based on Phase 3 OMI requirements for audit data aggregation, correlation and analysis, incident prioritization and response, and post incident activities (e.g., information sharing).

Ongoing Authorization is the continuous evaluation of the change in risk level related to changes in security policies concerning static object attributes (i.e., actual state and desired state) for threat behaviors that impact the security posture. This impact to security is measured by capturing changes in existing safeguards (e.g., NIST SP 800-53 controls and countermeasures) and identification of new component weaknesses and vulnerabilities.

This CDM capability covers verification and validation of processes/procedures to aggregate, correlate, and analyze audit/log data, to prioritize incidents and associated response actions, to quickly mitigate the impact of an incidents, to take appropriate remediation actions to eliminate the impact (restore normal operations) of the same incident, to support information sharing and collaboration (both internal and external) to minimize or prevent impact of future incidents, and ongoing authorization.

To provide a holistic security approach, this capability adheres to the Cybersecurity Framework security functions to identify, protect, detect, respond and recover. CDM also supports and can be used in the NIST Risk Management Framework (RMF) to achieve ongoing assessment and authorization.

Design and Build in Security

Focus: Design and Build in Security is responsible for preventing exploitable vulnerabilities from being effective in the software/system while in development or deployment. The Design and Build in Security process is focused on identifying, controlling and removing weaknesses/vulnerabilities from the software/system. Exploitable vulnerabilities may include software/system design, coding errors, software/system designs that leave a large and complex attack surface that cannot be defended, and weaknesses that can only be exploited during system/software execution.

Design and Build in Security is based on the Phase 3 DBS requirements that extend the focus of Phase 1 Software Asset Management and Vulnerability Management to achieve a level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle and that the software functions in the intended manner.

The U.S. government and critical infrastructure sectors are increasingly dependent on commercial products and systems, which present significant benefits including low cost, interoperability, rapid innovation, a variety of product features, and choice among competing vendors. However, with some of these benefits there is an increase in the risk of a threat event which can directly or indirectly affect the supply chain, which often go undetected, and may result in risks to the acquirer. The purpose of Supply Chain Risk Management (SCRM) is to enable the provisioning of the least vulnerable solutions to agencies, through a robust assessment of supply chain risks, communication about those risks to the agencies, and appropriate response and monitoring of those risks throughout the entire system lifespan.

This CDM capability covers verification and validation of processes/procedures to prevent and detect software vulnerabilities, to determine the provenance of system components, and to measure software assurance for built and acquired software components.

To provide a holistic security approach, this capability adheres to the Cybersecurity Framework security functions to identify, protect, detect, respond and recover to security infractions due to malicious behavior and unintentional user actions during normal operations.

(5) Emerging Tools and Technologies

Focus: Innovative capabilities to cybersecurity not currently encompassed by the other capability areas.

2. STANDARDS COMPLIANCE

Vendor's providing offerings through the CDM Tools SIN must provide compliant products and services in accordance with the laws and standards cited applicable to specific orders and Blanket Purchase Agreements.

3. ORDER

a. Written orders, EDI orders (GSA Advantage! and FACNET), credit card orders, and orders placed under blanket purchase agreements (BPA) agreements shall be the basis for purchase in accordance with the provisions of this contract. If time of delivery extends beyond the expiration date of the contract, the Contractor will be obligated to meet the delivery and installation date specified in the original order.

b. All delivery or task orders are subject to the terms and conditions of the contract. In the event of conflict between an order and the contract, the contract will take precedence.

4. INSPECTION/ACCEPTANCE

The Contractor shall only tender for acceptance those items that conform to the requirements of this contract. The ordering activity reserves the right to inspect or test any product that has been tendered for acceptance. The ordering activity may require repair or replacement of nonconforming item at no increase in contract price. The ordering activity must exercise its post acceptance rights (1) within a reasonable time after the defect was discovered or should have been discovered; and (2) before any substantial change occurs in the condition of the item, unless the change is due to the defect in the item.

5. COMMERCIAL SUPPLIER AGREEMENTS

Commercial Supplier Agreements to include Enterprise User License Agreements or Terms of Service (TOS) agreements. The Contractor shall provide all Commercial Supplier Agreements to include Enterprise User License Agreements or Terms of Service (TOS) agreements in an editable Microsoft Office (Word) format for review prior to award.

6. WARRANTY

a. Unless specified otherwise in this contract, the Contractor's standard commercial guarantee/warranty as stated in the contract's commercial pricelist will apply to this contract.

b. The Contractor warrants and implies that the items delivered hereunder are merchantable and fit for use for the particular purpose described in this contract. If no implied warranties are given, an express warranty of at least 60 days must be given in accordance with FAR 12.404(b)(2).

c. Limitation of Liability. Except as otherwise provided by an express or implied warranty, the Contractor will not be liable to the ordering activity for consequential damages resulting from any defect or deficiencies in accepted items.

d. If inspection and repair of defective equipment under this warranty will be performed at the contractor's plant the address is as follows: Contact Merlin for product specific requirements.

7. PURCHASE PRICE FOR ORDERED EQUIPMENT

The purchase price that the ordering activity will be charged will be the ordering activity purchase price in effect at the time of order placement, or the ordering activity purchase price in effect on the installation date (or delivery date when installation is not applicable), whichever is less

8. TRANSPORTATION OF EQUIPMENT FOB DESTINATION.

Prices cover equipment delivery to destination, for any location within the geographic scope of this contract.

9. TECHNICAL SERVICES

The Contractor, without additional charge to the ordering activity, shall provide a hot line technical support number 703-752-2928 for the purpose of providing user assistance and guidance in the implementation of the software.

10. PERFORMANCE OF SERVICES ASSOCIATED WITH PRODUCTS

a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity.

b. The Contractor agrees to render services during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.

c. The ordering activity should include the criteria for satisfactory completion of each order. Services shall be completed in a good and workmanlike manner.

d. Any Contractor travel required in the performance of the CDM Tools SIN for a specific requirement at the order level must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel. Contractors cannot use GSA city pair contracts. All travel will be agreed upon with the client prior to the Contractor's travel.

11. RESPONSIBILITIES OF THE CONTRACTOR

a. The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character. If the end product of an order is software, FAR 52.227-14 Rights in Data is in the schedule contract.

b. The Contractor shall comply with contract clause (FAR 52.204-21) for the basic safeguarding of contractor information systems that process, store, or transmit Federal data received by the contract in performance of the contract. This includes contract documents and all information generated in the performance of the contract.

12. RESPONSIBILITIES OF THE ORDERING ACTIVITY

Subject to security regulations, the ordering activity shall permit Contractor access to all facilities necessary to perform the requisite services.

13. INVOICES

The Contractor, upon completion of the work ordered, shall submit invoices. FAR 52.212-4 in the contract contains terms for commercial items. Progress payments may be authorized by the ordering activity on individual orders if appropriate. Progress payments shall be based upon completion of defined milestones or interim products. Invoices shall be submitted monthly for recurring services performed during the preceding month.

14. CONVERSION FROM TERM LICENSE TO PERPETUAL LICENSE

Conversion from Term License to Perpetual License is not offered.

15. TERM LICENSE CESSATION

Term License Cessation is not offered.

16. SOFTWARE CONVERSIONS

Full monetary credit will be allowed to the ordering activity when conversion from one version of the software to another is made as the result of a change in operating system, or from one computer system to another. Under a perpetual license, the purchase price of the new software shall be reduced by the amount that was paid to purchase the earlier version. Under a term license, conversion credits which accrued while the earlier version was under a term license shall carry forward and remain available as conversion credits which may be applied towards the perpetual license price of the new version.

17. DESCRIPTIONS AND EQUIPMENT COMPATIBILITY

The Contractor shall include, in the schedule pricelist, a complete description of each software product and a list of equipment on which the software can be used. Also, included shall be a brief, introductory explanation of the modules and documentation which are offered.

18. RIGHT-TO-COPY PRICING

Right-to-copy licenses are not offered.

19. DESCRIPTION OF PRODUCTS AND SERVICES AND PRICING

See GSA Price List for Descriptions and Details

20. TOTAL SOLUTION

Labor categories/qualifications are not included in this SIN, however, ordering activities may acquire a total solution to meet a specific requirement for an order or BPA involving multiple IT SINs



21. CDM TOOLS SIN CONTRACT LEVEL PROGRAM REPORTING REQUIREMENT

Contractors are required to provide quarterly reports on orders received to include ordering agency, quantity, product description, manufacturer part number, SIN and Subcategory, and price.

TERMS AND CONDITIONS APPLICABLE TO PURCHASE OF INFORMATION
TECHNOLOGY TRAINING (SPECIAL ITEM NUMBER
611420)

1. SCOPE

- a. The Contractor shall provide training courses normally available to commercial customers, which will permit ordering activity users to make full, efficient use of general purpose commercial IT products. Training is restricted to training courses for those products within the scope of this solicitation.
- b. The Contractor shall provide training at the Contractor's facility and/or at the ordering activity's location, as agreed to by the Contractor and the ordering activity.

2. ORDER

Written orders, EDI orders (GSA Advantage! and FACNET), credit card orders, and orders placed under blanket purchase agreements (BPAs) shall be the basis for the purchase of training courses in accordance with the terms of this contract. Orders shall include the student's name, course title, course date and time, and contracted dollar amount of the course.

3. TIME OF DELIVERY

The Contractor shall conduct training on the date (time, day, month, and year) agreed to by the Contractor and the ordering activity.

4. CANCELLATION AND RESCHEDULING

- a. The ordering activity will notify the Contractor at least seventy-two (72) hours before the scheduled training date, if a student will be unable to attend. The Contractor will then permit the ordering activity to either cancel the order or reschedule the training at no additional charge. In the event the training class is rescheduled, the ordering activity will modify its original training order to specify the time and date of the rescheduled training class.
- b. In the event the ordering activity fails to cancel or reschedule a training course within the time frame specified in paragraph a, above, the ordering activity will be liable for the contracted dollar amount of the training course. The Contractor agrees to permit the ordering activity to reschedule a student who fails to attend a training class within ninety (90) days from the original course date, at no additional charge.
- c. The ordering activity reserves the right to substitute one student for another up to the first day of class.
- d. In the event the Contractor is unable to conduct training on the date agreed to by the Contractor and the ordering activity, the Contractor must notify the ordering activity at least seventy-two (72) hours before the scheduled training date.

5. FOLLOW-UP SUPPORT

The Contractor agrees to provide each student with unlimited telephone support or online support for a period of one (1) year from the completion of the training course. During this period, the student may contact the Contractor's instructors for refresher assistance and answers to related course curriculum questions.

6. PRICE FOR TRAINING

The price that the ordering activity will be charged will be the ordering activity training price in effect at the time of order placement, or the ordering activity price in effect at the time the training course is conducted, whichever is less.

7. INVOICES AND PAYMENT

Invoices for training shall be submitted by the Contractor after ordering activity completion of the training course. Charges for training must be paid in arrears (31 U.S.C. 3324). PROMPT PAYMENT DISCOUNT, IF APPLICABLE, SHALL BE SHOWN ON THE INVOICE.

8. FORMAT AND CONTENT OF TRAINING

See GSA Price List for Details

9. "NO CHARGE" TRAINING

Merlin does not offer any no charge training.