PointStream

POINTSTREAM, Inc.

12600 Hill Country Blvd., R275, Bee Cave, TX 78738
1 (512) 463-1643 www.point-stream.com contracts@point-stream.com

Authorized Federal Supply Service (FSS) Information Technology Schedule Pricelist

General Services Administration (GSA) Federal Acquisition Service (FAS) Information Technology (IT) Schedule 70

Contract Number: GS-35F-394GA
Contract Period: 25 April 2017 through 24 April 2022
Highly Adaptive Cybersecurity Services (HACS)
Special Item Number: 132-45A
Special Item Number: 132-45B
Special Item Number: 132-45C
Special Item Number: 132-45D
Cloud Computing Services
Special Item Number: 132-40

Updated: *August 10, 2017*

Contents

1. Customer Information 3
1.1 Schedule Title 3
1.2 Special Item Numbers 3
1.3 Contact Information 3
1.4 Special Notice to Agencies: Small Business Participation 3
1.5 Geographic Scope of Contract (Delivery Area) 3
1.6 Government Purchase Cards 3
1.7 Liability for Injury or Damage 3
1.8 Statistical Data for Government Ordering Office Completion of SF-279 4
1.9 Commercial and Government Entity (CAGE) Code 4
1.10 Central Contractor Registration (CCR) Database 4
1.11 FOB Points 4
1.12 Time of Delivery 4
1.13 Urgent Requirements 4
1.14 Discounts 4
1.15 Trade Agreements Act of 1979, as Amended 5
1.16 Statement Concerning Availability of Export Packing 5
1.17 Minimum and Maximum Order 5
1.18 Ordering Procedures for Federal Supply Schedule Contracts 5
1.19 Contractor Tasks / Special Requirements (C-FSS-370) (NOV 2003) 5
1.20 Contract Administration for Ordering Activities 6
1.21 GSA Advantage!™ 6
1.22 Purchase of Open Market Items 7
1.23 Contractor Commitments, Warranties, and Representations 7
1.24 Overseas Activities 7
1.25 Blanket Purchase Agreements (BPAs) 7
1.26 Contractor Team Arrangements 7
1.27 Installation, Deinstallation, Reinstallation 8
1.28 Section 508 Compliance 8
1.29 Prime Contractor Ordering From Federal Supply Schedules 8
1.30 Insurance – Work on a Government Installation (JAN 1997) (FAR 52.228-5) 8
1.31 Software Interoperability 9
1.32 Advance Payments 9
2. Terms and Conditions Applicable to Cloud Computing Services, Special Item Number 132-40 9
2.1 Scope 9
2.2 Description of Cloud Computing Services and Pricing 10
2.3 Responsibilities of the Contractor 11
2.4 Responsibilities of the Ordering Activity 12
2.5 Guidance for Contractors 15
2.6 Factors for Evaluation for IT Schedule 70 Cloud Computing Services SIN 22
2.7 GSA Cloud Computing Software as a Service (SaaS) Price List 23
3. Terms and Conditions Applicable to Highly Adaptive Cybersecurity Services (Special Item Numbers 132-45A, 132-45B, 132-45C and 132-45B) 24
3.1 Scope 25
3.2 Order 25
3.3 Performance of Services 25
3.4 Inspection of Services 25
3.5 Responsibilities of the Contractor 25
3.6 Independent Contractor 26
3.7 Invoices 26
3.8 Resumes 26
3.9 Approval of Subcontracts 26
3.10 Description of Highly Adaptive Cybersecurity Services and Pricing 26
3.11 Labor Category Descriptions 29
3.12 Pricing 34
4. PointStream, Inc. Commitment to Promote Small Business Participation 35
5. Best Value Blanket Purchase Agreement Federal Supply Schedule 36
Appendix A, GSA-Negotiated Cybernance Cloud Service Agreement 39

1. Customer Information

1.1 Schedule Title

General Services Administration (GSA) Information Technology (IT) Schedule 70
Cloud Computing Services
Highly Adaptive Cybersecurity Services (HACS)

1.2 Special Item Numbers

Special Item Number: 132-40 – Cloud Computing Services

Special Item Number: 132-45A – Penetration Testing
Special Item Number: 132-45B – Incident Response
Special Item Number: 132-45C – Cyber Hunt
Special Item Number: 132-45D – Risk and Vulnerability Assessment

1.3 Contact Information

PointStream, Inc.
12600 Hill Country Blvd., Suite R275
Bee Cave, TX 78730

Phone: 1 (512) 463-1643

Fax: 1 (866) 245-6696
Website: www.point-stream.com
Email: contracts@point-stream.com

1.4 Special Notice to Agencies: Small Business Participation

SBA strongly supports the participation of small business concerns in the Federal Acquisition Service. To enhance Small Business Participation SBA policy allows agencies to include in their procurement base and goals, the dollar value of orders expected to be placed against the Federal Supply Schedules, and to report accomplishments against these goals.

For orders exceeding the micro-purchase threshold, FAR 8.404 requires agencies to consider the catalogs/pricelists of at least three schedule contractors or consider reasonably available information by using the GSA Advantage!™ on- line shopping service (www.gsaadvantage.gov). The catalogs/pricelists, GSA Advantage!™ and the Federal Acquisition Service Home Page (www.gsa.gov/fas) contain information on a broad array of products and services offered by small business concerns.

This information should be used as a tool to assist ordering activities in meeting or exceeding established small business goals. It should also be used as a tool to assist in including small, small disadvantaged, and women-owned small businesses among those considered when selecting pricelists for a best value determination.

For orders exceeding the micro-purchase threshold, customers are to give preference to small business concerns when two or more items at the same delivered price will satisfy their requirement.

1.5 Geographic Scope of Contract (Delivery Area)

Worldwide.

1.6 Government Purchase Cards

Government purchase cards are accepted for orders equal to or less than the micro-purchase threshold for oral or written orders under this contract.

1.7 Liability for Injury or Damage

The Contractor shall not be liable for any injury to ordering activity personnel or damage to ordering activity property arising from the use of equipment maintained by the Contractor, unless such injury

or damage is due to the fault or negligence of the Contractor.

1.8 Statistical Data for Government Ordering Office Completion of SF-279

Block 9: ***G. Order/Modification Under Federal Schedule Contract***
Block 16: Data Universal Numbering System (DUNS) Number: ***080296633***
Block 30: Type of Contractor: ***B. Other Small Business***
Block 31: Woman-Owned Small Business: ***No***
Block 37: Contractor's Taxpayer Identification Number (TIN): ***81-1354374***
Block 40: Veteran Owned Small Business (VOSB): ***No***

1.9 Commercial and Government Entity (CAGE) Code

7NGW7

1.10 Central Contractor Registration (CCR) Database

PointStream, Inc. has registered with the CCR Database/System for Award Management (SAM).

1.11 FOB Points

SIN 132-40	
SIN 132-45A	Destination.
SIN 132-45B	
SIN 132-45C	
SIN 132-45D	

1.12 Time of Delivery

SIN 132-40	
SIN 132-45A	As negotiated between ordering activity and PointStream, Inc.
SIN 132-45B	
SIN 132-45C	
SIN 132-45D	

1.13 Urgent Requirements

When the Federal Supply Schedule contract delivery period does not meet the bona fide urgent delivery requirements of an ordering activity, ordering activities are encouraged, if time permits, to contact the Contractor for the purpose of obtaining accelerated delivery. The Contractor shall reply to the inquiry within 3 workdays after receipt. (Telephonic replies shall be confirmed by the Contractor in writing.) If the Contractor offers an accelerated delivery time acceptable to the ordering activity, any order(s) placed pursuant to the agreed upon accelerated delivery time frame-shall be delivered within this shorter delivery time and in accordance with all other terms and conditions of the contract.

1.14 Discounts

SIN 132-40	Prices shown are NET prices; basic discounts have been deducted. Prompt Payment: *Not applicable* Quantity: *Not applicable* Dollar Volume: *Not applicable* Government Education Institutions: *Not applicable* Other: *Not applicable*
SIN 132-45A	
SIN 132-45B	
SIN 132-45C	
SIN 132-45D	

1.15 Trade Agreements Act of 1979, as Amended

All items are U.S. made end products or designated country end products.

1.16 Statement Concerning Availability of Export Packing

Not applicable.

1.17 Minimum and Maximum Order

The minimum dollar of orders to be issued is $100.00.

The maximum dollar of orders to be issued is $500,000.

1.18 Ordering Procedures for Federal Supply Schedule Contracts

Ordering activities shall use the ordering procedures of Federal Acquisition Regulation (FAR) 8.405 when placing an order or establishing a BPA for supplies or services. These procedures apply to all schedules.

a. FAR 8.405-1 Ordering procedures for supplies, and services not requiring a statement of work.

b. FAR 8.405-2 Ordering procedures for services requiring a statement of work.

Federal Information Technology / Telecommunications Standards Requirements

Ordering activities acquiring products from this Schedule must comply with the provisions of the Federal Standards Program, as appropriate (reference: NIST Federal Standards Index). Inquiries to determine whether or not specific products listed herein comply with Federal Information Processing Standards (FIPS) or Federal Telecommunication Standards (FED-STDS), which are cited by ordering activities, shall be responded to promptly by the Contractor.

Federal Information Processing Standards Publications (FIPS PUBS)

Information Technology products under this Schedule that do not conform to Federal Information Processing Standards (FIPS) should not be acquired unless a waiver has been granted in accordance with the applicable "FIPS Publication." Federal Information Processing Standards Publications (FIPS PUBS) are issued by the U.S. Department of Commerce, National Institute of Standards and Technology (NIST), pursuant to National Security Act. Information concerning their availability and applicability should be obtained from the National Technical Information Service (NTIS), 5301 Shawnee Road, Alexandria, Virginia 22312. FIPS PUBS include voluntary standards when these are adopted for Federal use. Individual orders for FIPS PUBS should be referred to the NTIS Sales Desk, telephone number 1(800) 553-6847, or email at info@ntis.gov. Orders for subscription service should be referred to the NTIS Subscription Officer at the above address, telephone number 1(800) 363-2068.

Federal Telecommunication Standards (FED-STDS)

Telecommunication products under this Schedule that do not conform to Federal Telecommunication Standards (FED-STDS) should not be acquired unless a waiver has been granted in accordance with the applicable "FED-STD." Federal Telecommunication Standards are issued by the U.S. Department of Commerce, NIST, pursuant to National Security Act. Ordering information and information concerning the availability of FED-STDS should be obtained from the GSA, Federal Acquisition Service, Specification Section, 470 East L'Enfant Plaza, Suite 8100, SW, Washington, DC 20407, telephone number (202)619-8925. Please include a self- addressed mailing label when requesting information by mail. Information concerning their applicability can be obtained by writing or calling the U.S. Department of Commerce, NIST, Gaithersburg, MD 20899, telephone number (301) 975-2833.

1.19 Contractor Tasks / Special Requirements (C-FSS-370) (NOV 2003)

a. *Security Clearances:* The Contractor may be required to obtain/possess varying levels of security clearances in the performance of orders issued under this contract. All costs associated with obtaining/possessing such security clearances should be factored into the price offered under the Multiple Award Schedule.

b. *Travel:* The Contractor may be required to travel in performance of orders issued under this contract. Allowable travel and per diem charges are governed by Pub .L. 99-234 and FAR Part 31, and are reimbursable by the ordering agency or can be priced as a fixed price item on orders placed under the Multiple Award Schedule. Travel in performance of a task order will only be reimbursable to the extent authorized by the ordering agency. The Industrial Funding Fee does NOT apply to travel and per diem charges.

c. *Certifications, Licenses and Accreditations:* As a commercial practice, the Contractor may be required to obtain/possess any variety of certifications, licenses and accreditations for specific FSC/service code classifications offered. All costs associated with obtaining/ possessing such certifications, licenses and accreditations should be factored into the price offered under the Multiple Award Schedule program.

d. *Insurance:* As a commercial practice, the Contractor may be required to obtain/possess insurance coverage for specific FSC/service code classifications offered. All costs associated with obtaining/possessing such insurance should be factored into the price offered under the Multiple Award Schedule program.

e. *Personnel:* The Contractor may be required to provide key personnel, resumes or skill category descriptions in the performance of orders issued under this contract. Ordering activities may require agency approval of additions or replacements to key personnel.

f. *Organizational Conflicts of Interest:* Where there may be an organizational conflict of interest as determined by the ordering agency, the Contractor's participation in such order may be restricted in accordance with FAR Part 9.5.

g. *Documentation/Standards:* The Contractor may be requested to provide products or services in accordance wit*h rules, regulations, OMB orders, standards and documentation as specified by the agency's order.*

h. *Data/Deliverable Requirements:* Any required data/deliverables at the ordering level will be as specified or negotiated in the agency's order.

i. *Government-Furnished Property:* As specified by the agency's order, the Government may provide property, equipment, materials or resources as necessary.

j. *Availability of Funds:* Many Government agencies' operating funds are appropriated for a specific fiscal year. Funds may not be presently available for any orders placed under the contract or any option year. The Government's obligation on orders placed under this contract is contingent upon the availability of appropriated funds from which payment for ordering purposes can be made. No legal liability on the part of the Government for any payment may arise until funds are available to the ordering Contracting Officer.

k. *Overtime:* For professional services, the labor rates in the Schedule should not vary by virtue of the Contractor having worked overtime. For services applicable to the Service Contract Act (as identified in the Schedule), the labor rates in the Schedule will vary as governed by labor laws (usually assessed a time and a half of the labor rate).

1.20 Contract Administration for Ordering Activities

Any ordering activity, with respect to any one or more delivery orders placed by it under this contract, may exercise the same rights of termination as might the GSA Contracting Officer under provisions of FAR 52.212 -4, paragraphs (1) Termination for the ordering activity's convenience, and (m) Termination for Cause (See 52.212-4).

1.21 GSA Advantage!™

GSA Advantage!™ is an on-line, interactive electronic information and ordering system that provides on-line access to vendors' schedule prices with ordering information, which may be found at https://www.gsaadvantage.gov.

1.22 Purchase of Open Market Items

NOTE: Open Market Items are also known as incidental items, noncontract items, non-Schedule items, and items not on a Federal Supply Schedule contract. Ordering Activities procuring open market items must follow FAR 8.402(f).

For administrative convenience, an ordering activity contracting officer may add items not on the Federal Supply Multiple Award Schedule (MAS) -- referred to as open market items -- to a Federal Supply Schedule blanket purchase agreement (BPA) or an individual task or delivery order, only if-

(1) All applicable acquisition regulations pertaining to the purchase of the items not on the Federal Supply Schedule have been followed (e.g., publicizing (Part 5), competition requirements (Part 6), acquisition of commercial items (Part 12), contracting methods (Parts 13, 14, and 15), and small business programs (Part 19));

(2) The ordering activity contracting officer has determined the price for the items not on the Federal Supply Schedule is fair and reasonable;

(3) The items are clearly labeled on the order as items not on the Federal Supply Schedule; and

(4) All clauses applicable to items not on the Federal Supply Schedule are included in the order.

1.23 Contractor Commitments, Warranties, and Representations

a. For the purpose of this contract, commitments, warranties and representations include, in addition to those agreed to for the entire schedule contract:

   (1) Time of delivery/installation quotations for individual orders;

   (2) Technical representations and/or warranties of products concerning performance, total system performance and/or configuration, physical, design and/or functional characteristics and capabilities of a product/equipment/ service/software package submitted in response to requirements which result in orders under this schedule contract.

   (3) Any representations and/or warranties concerning the products made in any literature, description, drawings and/or specifications furnished by the Contractor.

b. The above is not intended to encompass items not currently covered by the GSA Schedule contract.

1.24 Overseas Activities

The terms and conditions of this contract shall apply to all orders for installation, maintenance and repair of equipment in areas listed in the pricelist outside the 48 contiguous states and the District of Columbia, except as indicated below:

None.

Upon request of the Contractor, the ordering activity may provide the Contractor with logistics support, as available, in accordance with all applicable ordering activity regulations. Such ordering activity support will be provided on a reimbursable basis, and will only be provided to the Contractor's technical personnel whose services are exclusively required for the fulfillment of the terms and conditions of this contract.

1.25 Blanket Purchase Agreements (BPAs)

The use of BPAs under any schedule contract to fill repetitive needs for supplies or services is allowable. BPAs may be established with one or more schedule contractors. The number of BPAs to be established is within the discretion of the ordering activity establishing the BPA and should be based on a strategy that is expected to maximize the effectiveness of the BPA(s). Ordering activities shall follow FAR 8.405-3 when creating and implementing BPA(s).

1.26 Contractor Team Arrangements

Contractors participating in contractor team arrangements must abide by all terms and conditions of their respective contracts. This includes compliance with Clauses 552.238-74, Industrial Funding Fee and Sales Reporting, i.e., each contractor (team member) must report sales and remit the IFF for all products and services provided under its individual contract.

1.27 Installation, Deinstallation, Reinstallation

The Davis-Bacon Act (40 U.S.C. 276a-276a-7) provides that contracts in excess of $2,000 to which the United States or the District of Columbia is a party for construction, alteration, or repair (including painting and decorating) of public buildings or public works with the United States, shall contain a clause that no laborer or mechanic employed directly upon the site of the work shall receive less than the prevailing wage rates as determined by the Secretary of Labor. The requirements of the Davis-Bacon Act do not apply if the construction work is incidental to the furnishing of supplies, equipment, or services. For example, the requirements do not apply to simple installation or alteration of a public building or public work that is incidental to furnishing supplies or equipment under a supply contract. However, if the construction, alteration or repair is segregable and exceeds $2,000, then the requirements of the Davis-Bacon Act applies.

The ordering activity issuing the task order against this contract will be responsible for proper administration and enforcement of the federal labor standards covered by the Davis-Bacon Act. The proper Davis-Bacon wage determination will be issued by the ordering activity at the time a request for quotations is made for applicable construction classified installation, deinstallation, and reinstallation services under SIN 132 -8 or 132-9.

1.28 Section 508 Compliance

If applicable, Section 508 compliance information on the supplies and services in this contract are available in Electronic and Information Technology (EIT) at the following website:

www.point-stream.com

The EIT standard can be found at: www.Section508.gov.

1.29 Prime Contractor Ordering From Federal Supply Schedules

Prime Contractors (on cost reimbursement contracts) placing orders under Federal Supply Schedules, on behalf of an ordering activity, shall follow the terms of the applicable schedule and authorization and include with each order –

a. A copy of the authorization from the ordering activity with whom the contractor has the prime contract (unless a copy was previously furnished to the Federal Supply Schedule contractor); and
b. The following statement:

"This order is placed under written authorization from_____dated_____. In the event of any inconsistency between the terms and conditions of this order and those of your Federal Supply Schedule contract, the latter will govern."

1.30 Insurance – Work on a Government Installation (JAN 1997) (FAR 52.228-5)

a. The Contractor shall, at its own expense, provide and maintain during the entire performance of this contract, at least the kinds and minimum amounts of insurance required in the Schedule or elsewhere in the contract.
b. Before commencing work under this contract, the Contractor shall notify the Contracting Officer in writing that the required insurance has been obtained. The policies evidencing required insurance shall contain an endorsement to the effect that any cancellation or any material change adversely affecting the Government's interest shall not be effective—

(1) For such period as the laws of the State in which this contract is to be performed prescribe;

or,

(2) Until 30 days after the insurer or the Contractor gives written notice to the Contracting Officer, whichever period is longer.

c. The Contractor shall insert the substance of this clause, including this paragraph (c), in subcontracts under this contract that require work on a Government installation and shall require subcontractors to provide and maintain the insurance required in the Schedule or elsewhere in the contract. The Contractor shall maintain a copy of all subcontractors' proofs of required insurance, and shall make copies available to the Contracting Officer upon request.

1.31 Software Interoperability

Offerors are encouraged to identify within their software items any component interfaces that support open standard interoperability. An item's interface may be identified as interoperable on the basis of participation in a Government agency-sponsored program or in an independent organization program. Interfaces may be identified by reference to an interface registered in the component registry located at http://www.core.gov.

1.32 Advance Payments

A payment under this contract to provide a service or deliver an article for the United States Government may not be more than the value of the service already provided or the article already delivered. Advance or pre-payment is not authorized or allowed under this contract. (31 U.S.C. 3324).

2. Terms and Conditions Applicable to Cloud Computing Services, Special Item Number 132-40

2.1 Scope

The prices, terms and conditions stated under Special Item Number (SIN) 132 -40 Cloud Computing Services apply exclusively to Cloud Computing Services within the scope of this Information Technology Schedule.

This SIN provides ordering activities with access to technical services that run in cloud environments and meet the NIST Definition of Cloud Computing Essential Characteristics. Services relating to or impinging on cloud environments 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 service. Hardware, software and other artifacts 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 build on-premise cloud functionality, through combining different services on other IT Schedule 70 SINs (e.g. 132-51).

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 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.

See Table 1 for a representation of the scope and sub-categories.

Table 1: Cloud Computing Services SIN

SIN Description	Sub-Categories
• Commercially available cloud computing services • Meets the National Institute for Standards and Technology (NIST) definition of Cloud Computing essential characteristics • Open to all deployment models (private, public, community or hybrid), vendors specify deployment models	1. **Software as a Service (SaaS):** Consumer uses provider's applications on cloud infrastructure. Does not manage/control platform or infrastructure. Limited application level configuration may be available. 2. **Platform as a Service (PaaS):** Consumer deploys applications onto cloud platform service using provider-supplied tools. Has control over deployed applications and some limited platform configuration but does not manage the platform or infrastructure. 3. **Infrastructure as a Service (IaaS):** Consumer provisions computing resources. Has control over OS, storage, platform, deployed applications and some limited

2.2 Description of Cloud Computing Services and Pricing

a. Service Description Requirements for Listing Contractors

The description requirements below are in addition to the overall Schedule 70 evaluation criteria described in SCP -FSS-001, SCP-FSS-004 and other relevant publications.

Refer to overall Schedule 70 requirements for timelines related to description and other schedule updates, including but not limited to clauses 552.238-81 – section E and clause I-FSS-600.

Table 2 summarizes the additional Contractor-provided description requirements for services proposed under the Cloud Computing Services SIN. All mandatory description requirements must be complete, and adequate according to evaluation criteria.

In addition, there is one "Optional" reporting description which exists to provide convenient service selection by relevant criteria. Where provided, optional description requirements must be complete and adequate according to evaluation criteria:

- The NIST Service Model provides sub-categories for the Cloud SIN and is strongly encouraged, but not required. The Service Model-based sub-categories provide this SIN with a structure to assist ordering activities in locating and comparing services of interest. Contractors may optionally select the single service model most closely corresponding to the specific se vice offering.
- If a sub-category is selected it will be evaluated with respect to the NIST Service Model definitions and guidelines in "Guidance for Contractors".

Table 2: Cloud Service Description Requirements

#	Description Requirement	Reporting	Instructions
1	Provide a brief written description of how the proposed cloud computing services satisfies each individual essential NIST Characteristic	Mandatory	The cloud service must be capable of satisfying each of the five NIST essential characteristics as outlined in NIST Special Publication 800-145. See "GUIDANCE FOR CONTRACTORS: NIST Essential Characteristics" below in this document for detailed overall direction, as well as guidance on inheriting essential characteristics.

2	Select NIST deployment models for the cloud computing service proposed.	Mandatory	Contractors must select at least one NIST deployment model as outlined in NIST Special Publication 800-145 describing how the proposed cloud computing service is deployed. Select multiple deployment models if the service is offered in more than one deployment model. See "GUIDANCE FOR CONTRACTORS: NIST Deployment Model" below in this document for detailed direction on how to best categorize a service for the NIST deployment models.
3	Optionally select the most appropriate NIST service model that will be the designated sub-category, or may select no sub-category.	Optional	Contractor may select a single NIST Service model to sub-categorize the service as outlined in NIST Special Publication 800-145. Sub-category selection is optional but recommended. See "GUIDANCE FOR CONTRACTORS: NIST Service Model" below in this document for detailed direction on how to best categorize a service for the NIST IaaS, PaaS, and SaaS service models.

b. Pricing of Cloud Computing Services

All current pricing requirements for Schedule 70, including provision SCP-FSS-001 (Section III Price Proposal), SCP-FSS-004 (Section III Price Proposal), and clause I-FSS-600 Contract Price Lists, apply. At the current time there is no provision for reducing or eliminating standard pricelist posting requirements to accommodate rapid cloud price fluctuations.

In addition to standard pricing requirements, all pricing models must have the core capability to meet the NIST Essential Cloud Characteristics, particularly with respect to on-demand self-service, while allowing alternate variations at the task order level at agency discretion, pursuant to the guidance on NIST Essential Characteristics.

2.3 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 solution. Any additional substantial and ongoing professional services related to the offering such as integration, migration, and other cloud professional services are out of scope for this SIN.

e. Performance of Cloud Computing Services

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 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.

2.4 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 Schedule 70 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

i. 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.

ii. The Ordering Activity shall assign a required impact level for confidentiality, integrity and availability (CIA) prior to issuing the initial statement of work. 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 CIA assessment area.

iii. 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.

iv. 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.

v. 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. For example, a requirement could be requiring assurance that the service is capable of safeguarding Personally Identifiable Information (PII), in accordance with NIST SP 800 -122 and OMB memos M-06-16 and M-07-16. An Ordering Activity will determine what data elements constitute PII according to OMB Policy, NIST Guidance and Ordering Activity policy.

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 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 Schedule 70 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. Example cases that might require clarification include status and mode of delivery for:

- Configuration information created by the government and affecting the government's use of the cloud provider's service.
- Virtual machine configurations created by the government but operating on the cloud provider's service.
- Profile, configuration and other metadata used to configure SaaS application services or PaaS platform services.

The key is to determine in advance the ownership of classes of data and the means by which Government owned data can be returned to the Government.

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:

- 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.
- 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, genera l regions where service locations are available, etc.

l. Related Professional Services

Ordering activities should engage with Contractors to discuss the availability of limited assistance with initial setup, training and access to the services that may be available through this SIN.

Any additional substantial and ongoing professional services related to the offering such as integration, migration, and other cloud professional services are out of scope for this SIN. Ordering activities should consult the appropriate GSA professional services schedule.

2.5 Guidance for Contractors

This section offers guidance for interpreting the Contractor Description Requirements in Table 2, including the NIST essential cloud characteristics, service models and deployment models. This section is not a list of requirements.

Contractor-specific definitions of cloud computing characteristics and models or significant variances from the NIST Essential Characteristics or models are discouraged and will **not** be considered in the scope of this SIN or accepted in response to Factors for Evaluation. The only applicable cloud characteristics, service model/subcategories and deployment models for this SIN will be drawn from the NIST 800-145 special publication. Services qualifying for listing as cloud computing services under this SIN must substantially satisfy the essential characteristics of cloud computing as documented in the NIST Definition of Cloud Computing SP800-145.

Contractors must select deployment models corresponding to each way the service can be deployed. Multiple deployment model designations for a single cloud service are permitted but at least one deployment model must be selected.

In addition, contractors submitting services for listing under this SIN are encouraged to select a sub-category for each service proposed under this SIN with respect to a single principal NIST cloud service model that most aptly characterizes the service. Service model categorization is optional.

Both service and deployment model designations must accord with NIST definitions. Guidance is offered in this document on making the most appropriate selection.

a. NIST Essential Characteristics

General Guidance
NIST's Essential cloud Characteristics provide a consistent metric for whether a service is eligible for inclusion in this SI N. It is understood that due to legislative, funding and other constraints government entities cannot always leverage cloud service to the extent that all NIST Essential Characteristics are commercially available. For the purposes of the Cloud SIN, meeting the NIST Essential Characteristics is determined by whether each essential capability of the commercial service is available for the service, whether or not the Ordering Activity actually requests or implements the capability. The guidance in Table 3 offers examples of how services might or might not be included based on the essential characteristics, and how the Contractor should interpret the characteristics in light of current government contracting processes.

Table 3: Guidance on Meeting NIST Essential Characteristics

Characteristic	Capability	Guidance
On-demand Self-Service	• Ordering activities can directly provision services without requiring Contractor intervention. • This characteristic is typically implemented via a service console or programming interface for provisioning.	Government procurement guidance varies on how to implement on- demand provisioning at this time. Ordering activities may approach on-demand in a variety of ways, including "not-to-exceed" limits, or imposing monthly or annual payments on what are essentially on demand services. Services under this SIN must be capable of true on-demand self-service, and ordering activities and Contractors must negotiate how they implement on demand capabilities in practice at the task order level: • Ordering activities must specify their procurement approach and requirements for on-demand service. • Contractors must propose how they intend to meet the approach. • Contractors must certify that on-demand self-service is technically available for their service should procurement guidance become available.
Broad Network Access	• Ordering activities are able to access services over standard agency networks. • Service can be accessed and consumed using standard devices such as browsers, tablets and mobile phones.	• Broad network access must be available without significant qualification and in relation to the deployment model and security domain of the service. • Contractors must specify any ancillary activities, services or equipment required to access cloud services or integrate cloud with other cloud or non-cloud networks and services. For example, a private cloud might require an Ordering Activity to purchaser provide a dedicated router, etc. which is acceptable but should be indicated by the Contractor.
Resource Pooling	• Pooling distinguishes cloud services from offsite hosting. • Ordering activities draw resources from a common pool maintained by the Contractor. • Resources may have general characteristics such as regional location.	• The cloud service must draw from a pool of resources and provide an automated means for the Ordering Activity to dynamically allocate them. • Manual allocation, e.g. manual operations at a physical server farm where Contractor staff configure servers in response to Ordering Activity requests, does not meet this requirement. • Similar concerns apply to software and platform models; automated provisioning from a pool is required. • Ordering activities may request dedicated physical hardware, software or platform resources to access a private cloud deployment service. However, the provisioned cloud resources must be drawn from a common pool and automatically allocated on request.

Rapid Elasticity	• Rapid provisioning and de-provisioning commensurate with demand	• Rapid elasticity is a specific demand-driven case of self-service • Procurement guidance for on-demand self-service applies to rapid elasticity as well, i.e. rapid elasticity must be technically available but ordering activities and Contractors may mutually negotiate other contractual arrangements for procurement and payment. • 'Rapid' should be understood as measured in minutes and hours, not days or weeks. • Elastic capabilities by manual request, e.g., via a console operation or programming interface call, are required. • Automated elasticity which is driven dynamically by system load, etc. is optional. Contractors must specify whether automated, demand-driven elasticity is available and the general mechanisms that drive the capability.
Measured Service	• Measured service should be understood as a reporting requirement that enables an Ordering Activity to control their use in cooperation with self-service.	• Procurement guidance for on-demand self-service applies to measured services as well, i.e. rapid elasticity must be technically available but ordering activities and Contractors may mutually designate other contractual arrangements. • Regardless of specific contractual arrangements, reporting must indicate actual usage, be continuously available to the Ordering Activity, and provide meaningful metrics appropriate to the service measured. • Contractors must specify that measured service is available and the general sort of metrics and mechanisms available.

Inheriting Essential Characteristics

Cloud services may depend on other cloud services, and cloud service models such as PaaS and SaaS are able to inherit essential characteristics from other cloud services that support them. For example, a PaaS platform service can inherit the broad network access made available by the IaaS service it runs on, and in such a situation would be fully compliant with the broad network access essential characteristic. Services inheriting essential characteristics must make the inherited characteristic fully available at their level of delivery to claim the relevant characteristic by inheritance.

Inheriting characteristics does not require the inheriting provider to directly bundler integrate the inherited service, but it does require a reasonable measure of support and identification. For example, the Ordering Activity may acquire an IaaS service from "Provider A" and a PaaS service from "Provider B". The PaaS service may inherit broad network access from "Provider A" but must identify and support the inherited service as an acceptable IaaS provider.

Assessing Broad Network Access

Typically broad network access for public deployment models implies high bandwidth access from the public internet for authorized users. In a private cloud deployment internet access might be considered broad access, as might be access through a dedicated shared high bandwidth network connection from the Ordering Activity, in accord with the private nature of the deployment model.

Resource Pooling and Private Cloud

All cloud resource pools are finite, and only give the appearance of infinite resources when sufficiently large, as is sometimes the case with a public cloud. The resource pool supporting a private cloud is typically smaller with more visible limits. A finite pool of resources purchased as a private cloud service qualifies as resource pooling so long as the resources within the pool can be

Dynamically allocated to the ultimate users of the resource, even though the pool itself appears finite to the Ordering Activity that procures access to the pool as a source of dynamic service allocation.

b. NIST Service Model

The Contractor may optionally document the service model of cloud computing (e.g. IaaS, PaaS, SaaS, or a combination thereof, that most closely describes their offering, using the definitions in The NIST Definition of Cloud Computing SP 800-145. The following guidance is offered for the proper selection of service models.

NIST's service models provide this SIN with a set of consistent sub-categories to assist ordering activities in locating and comparing services of interest. Service model is primarily concerned with the nature of the service offered and the staff and activities most likely to interact with the service. Contractors should select a single service model most closely corresponding to their proposed service based on the guidance below. It is understood that cloud services can technically incorporate multiple service models and the intent is to provide the single best categorization of the service.

Contractors should take care to select the NIST service model most closely corresponding to each service offered. Contractors should not invent, proliferate or select multiple cloud service model sub-categories to distinguish their offerings, because ad-hoc categorization prevents consumers from comparing similar offerings. Instead vendors should make full use of the existing NIST categories to the fullest extent possible.

For example, in this SIN an offering commercially marketed by a Contractor as "Storage as a Service" would be properly characterized as Infrastructure as a Service (IaaS), storage being a subset of infrastructure. Services commercially marketed as "LAMP as a Service" or "Database as a Service" would be properly characterized under this SIN as Platform as a Service (PaaS), as they deliver two kinds of platform services. Services commercially marketed as "Travel Facilitation as a Service" or "Email as a Service" would be properly characterized as species of Software as a Service (SaaS) for this SIN. However, Contractors can and should include appropriate descriptions (include commercial marketing terms) of the service in the full descriptions of the service's capabilities.

When choosing between equally plausible service model sub-categories, Contractors should consider several factors:

1) Visibility to the Ordering Activity. Service model sub-categories in this SIN exist to help Ordering Activities match their requirements with service characteristics. Contractors should select the most intuitive and appropriate service model from the point of view of an Ordering Activity.
2) Primary Focus of the Service. Services may offer a mix of capabilities that span service models in the strict technical sense.

   For example, a service may offer both IaaS capabilities for processing and storage, along with some

PaaS capabilities for application deployment, and SaaS capabilities for specific applications. In a service mix situation the Contractor should select the service model that is their primary focus. Alternatively contractors may choose to submit multiple service offerings for the SIN, each optionally and separately subcategorized.

3) Ordering Activity Role. Contractors should consider the operational role of the Ordering Activity's primary actual consumer or operator of the service. For example services most often consumed by system managers are likely to fit best as IaaS; services most often consumed by application deplorers or developers as PaaS, and services most often consumed by business users as SaaS.
4) Lowest Level of Configurability. Contractors can consider IaaS, PaaS and SaaS as an ascending hierarchy of complexity, and select the model with the lowest level of available Ordering Activity interaction. As an example, virtual machines are an IaaS service often bundled with a range of operating systems, which are PaaS services. The Ordering Activity usually has access to configure the lower level IaaS service, and the overall service should be considered IaaS. In cases where the Ordering Activity cannot configure the speed, memory, network configuration, or any other aspect of the IaaS component, consider categorizing as a PaaS service.

Cloud management and cloud broker services should be categorized based on their own characteristics and not those of the other cloud services that are their targets. Management and broker services typically fit the SaaS service model, regardless of whether the services they manage are SaaS, PaaS or IaaS. Use Table 3 to determine which service model is appropriate for the cloud management or cloud broker services, or, alternately choose not to select a service model for the service.

The guidance in Table 4 offers examples of how services might be properly mapped to NIST service models and how a Contractor should interpret the service model sub-categories.

Table 4: Guidance on Mapping to NIST Service Models

Service Model	Guidance
Infrastructure as a Service (IaaS)	Select an IaaS model for service based equivalents of hardware appliances such as virtual machines, storage devices, routers and other physical devices. • IaaS services are typically consumed by system or device managers who would configure physical hardware in a non-cloud setting. • The principal customer interaction with an IaaS service is provisioning then configuration, equivalent to procuring and then configuring a physical device. Examples of IaaS services include virtual machines, object storage, disk block storage, network routers and firewalls, software defined networks. Gray areas include services that emulate or act as dedicated appliances and are directly used by applications, such as search appliances, security appliances, etc. To the extent that these services or their emulated devices provide direct capability to an application they might be better classified as Platform services (PaaS). To the extent that they resemble raw hardware and are consumed by other platform services they are better classified as IaaS.

Platform as a Service (PaaS)	Select a PaaS model for service based equivalents of complete or partial software platforms. For the purposes of this classification, consider a platform as a set of software services capable of deploying all or part of an application. • A complete platform can deploy an entire application. Complete platforms can be proprietary or open source. • Partial platforms can deploy a component of an application which combined with other components make up the entire deployment. • PaaS services are typically consumed by application deployment staff whose responsibility is to take a completed agency application and cause it to run on the designated complete or partial platform service. • The principal customer interaction with a PaaS service is deployment, equivalent to deploying an application or portion of an application on a software platform service. • A limited range of configuration options for the platform service may be available. Examples of complete PaaS services include: • A Linux/Apache/MySQL/PHP (LAMP) platform ready to deploy a customer PHP application, • A Windows .Net platform ready to deploy a .Net application, • A custom complete platform ready to develop and deploy an customer application in a proprietary language, and, • A multiple capability platform ready to deploy an arbitrary customer application on a range of underlying software services. The essential characteristic of a complete PaaS is defined by the customer's ability to deploy a complete custom application directly on the platform.
	PaaS includes partial services as well as complete platform services. Illustrative examples of individual platform enablers or components include: • A database service ready to deploy a customer's tables, views and procedures, • A queuing service ready to deploy a customer's message definitions, and, • A security service ready to deploy a customer's constraints and target applications for continuous monitoring. The essential characteristic of an individual PaaS component is the customer's ability to deploy their unique structures and/or data onto the component for a partial platform function. Note that both the partial and complete PaaS examples all have two things in common: • They are software services, which offer significant core functionality out of the box. • They must be configured with customer data and structures to deliver results. As noted in IaaS, operating systems represent a grey area in that OS is definitely a platform service, but is typically bundled with IaaS infrastructure. If your service provides an OS but allows for interaction with infrastructure, please sub-categorize it as IaaS. If your service "hides" underlying infrastructure, consider it as PaaS.

Software as a Service (SaaS)	Select a SaaS model for service based equivalents of software applications. • SaaS services are typically consumed by business or subject-matter staff who would interact directly with the application in a non-cloud setting • The principal customer interaction with a SaaS service is actual operation and consumption of the application services the SaaS service provides. Some minor configuration may be available, but the scope of the configuration is limited to the scope and then the permissions of the configuring user. For example, an agency manager might be able to configure some aspects of the application for their agency but not all agencies. An agency user might be able to configure some aspects for themselves but not everyone in their agency. Typically only the Contractor would be permitted to configure aspects of the software for all users. Examples of SaaS services include email systems, business systems of all sorts such as travel systems, inventory systems, etc., wiki's, websites or content management systems, management applications that allow a customer to manage other cloud or non-cloud services, and in general any system where customers interact directly for a business purpose. Gray areas include services that customers use to configure other cloud services, such as cloud management software, cloud brokers, etc. In general these sorts of systems should be considered SaaS, per guidance in this document.

c. Deployment Model

Deployment models (e.g., private, public, community, or hybrid) are not restricted at the SIN level and any specifications for a deployment model are the responsibility of the Ordering Activity.

Multiple deployment model selection is permitted, but at least one model must be selected. The guidance in Table 4 offers examples of how services might be properly mapped to NIST deployment models and how the Contractor should interpret the deployment model characteristics. Contractors should take care to select the range of NIST deployment models most closely corresponding to each service offered.

Note that the scope of this SIN does not include hardware or software components used to construct a cloud, only cloud capabilities delivered as a service, as noted in the Scope section.

Table 5: Guidance for Selecting a Deployment Model

Deployment Model	Guidance
Private Cloud	The service is provided exclusively for the benefit of a definable organization and its components; access from outside the organization is prohibited. The actual services may be provided by third parties, and may be physically located as required, but access is strictly defined by membership in the owning organization.
Public Cloud	The service is provided for general public use and can be accessed by any entity or organization willing to contract for it.

Community Cloud	The service is provided for the exclusive use of a community with a definable shared boundary such as a mission or interest. As with private cloud, the service may be in any suitable location and administered by a community member or a third party.
Hybrid Cloud	The service is composed of one or more of the other models. Typically hybrid models include some aspect of transition between the models that make them up, for example a private and public cloud might be designed as a hybrid cloud where events like increased load permit certain specified services in the private cloud to run in a public cloud for extra capacity, e.g. bursting.

2.6 Factors for Evaluation for IT Schedule 70 Cloud Computing Services SIN

The following technical evaluation factor applies in addition to the standard Schedule 70 evaluation factors outlined in CI -FSS-152 ADDITIONAL EVALUATION FACTORS and related documents and applies solely to the Cloud Computing Services SIN. A template will be provided at the time of solicitation refresh to complete the requested documentation.

FACTOR - Cloud Computing Services Adherence to Essential Cloud Characteristics

Within a two page limitation for each cloud service submitted, provide description of how the cloud computing service meets each of the five essential cloud computing characteristics as defined in National Institute of Standards and Technology (NIST) Special Publication 800-145 and subsequent versions of this publication. This standard specifies the definition of cloud computing for the use by Federal agencies. The cloud service must be capable of satisfying each of the five NIST Essential Characteristics as follows:

- On-demand self-service
- Broad network access
- Resource Pooling
- Rapid Elasticity
- Measured Service

Refer to the 'Guidance for Contractors' section of the Terms & Conditions for the Cloud Computing Services SIN for guidance on meeting the NIST characteristics. For the purposes of the Cloud Computing Services SIN, meeting the NIST essential characteristics is concerned primarily with whether the underlying capability of the commercial service is available, whether or not an Ordering Activity actually requests or implements the capability.

FACTOR – Cloud Computing Services Deployment Model

For each cloud service submitted, provide a written description of how the proposed service meets the NIST definition of a particular deployment model (Public, Private, Community, or Hybrid), within a one half (1/2) page limitation for each designated deployment model of each cloud service submitted. Multiple deployment model selection is permitted, but at least one model must be indicated.

Refer to the 'Guidance for Contractors' section of the Terms & Conditions for the Cloud Computing Services SIN for guidance on identifying the appropriate deployment model according to the NIST service model definitions.

FACTOR - Cloud Computing Services Service Model

For each cloud computing service proposed to be categorized under a specific sub-category (IaaS, PaaS or SaaS), provide a written description of how the proposed service meets the NIST definition of that service model, within a half (1/2) page limitation for each cloud service submitted.

Refer to the 'Guidance for Contractors' section of the Terms & Conditions for the Cloud Computing Services SIN for guidance on categorizing the service into a sub-category according to the NIST service model definitions.

Note that it is not mandatory to select a sub-category, and therefore this factor for evaluation applies ONLY to cloud services proposed to fall under a specific sub-category. If no sub-category is selected, this factor does not need to be addressed. The two other factors ('Adherence to Essential Cloud Characteristics' and 'Cloud Computing Services Deployment Model') apply to all cloud services.

2.7 GSA Cloud Computing Software as a Service (SaaS) Price List

NOTE: The GSA-negotiated Cybernance Cloud Service Agreement is included in Appendix A.

Cybernance Corporation
GSA Commercial Price List
July 25, 2017
The Cybernance Platform, Product/Version 100-Fed01

General

The Cybernance Platform is a SaaS solution.
Pricing is determined by multiplying the number of employees that use the organization's network by the price per employee.
Pricing is paid as an Annual Premium.

Base price/employee/month:	$0.90
Basic price/employee/year:	$10.80
Minimum Annual Premium:	no minimum

Pricing Matrix (example Annual Premiums):

Employees	Annual Premium ($)
1,000	10,800
1,667	18,004
2,000	21,600
2,500	27,000
3,000	32,400
4,000	43,200
5,000	54,000
6,000	64,800
7,000	75,600
8,000	86,400
9,000	97,200
10,000	108,000
20,000	216,000
30,000	324,000
40,000	432,000
50,000	540,000
100,000	1,080,000

3. Terms and Conditions Applicable to Highly Adaptive Cybersecurity Services (Special Item Numbers 132-45A, 132-45B, 132-45C and 132-45B)

Vendor suitability for offering services through the Highly Adaptive Cybersecurity Services (HACS) SINs must be in accordance with the following laws and standards when applicable to the specific task orders, including but not limited to:

- Federal Acquisition Regulation (FAR) Part 52.204-21
- OMB Memorandum M-06-19 - Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments
- OMB Memorandum M -07-16 - Safeguarding Against and Responding to the Breach of Personally Identifiable Information
- OMB Memorandum M-16-03 - Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements
- OMB Memorandum M-16-04 – Cybersecurity Implementation Plan (CSIP) for Federal Civilian Government
- The Cybersecurity National Action Plan (CNAP)
- NIST SP 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems
- NIST SP 800-27A - Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
- NIST SP 800-30 - Guide for Conducting Risk Assessments
- NIST SP 800-35 - Guide to Information Technology Security Services
- NIST SP 800-37 - Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- NIST SP 800-39 - Managing Information Security Risk: Organization, Mission, and Information System View
- NIST SP 800-44 - Guidelines on Securing Public Web Servers
- NIST SP 800-48 - Guide to Securing Legacy IEEE 802.11 Wireless Networks
- NIST SP 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-61 - Computer Security Incident Handling Guide
- NIST SP 800-64 - Security Considerations in the System Development Life Cycle
- NIST SP 800-82 - Guide to Industrial Control Systems (ICS) Security
- NIST SP 800-86 - Guide to Integrating Forensic Techniques into Incident Response
- NIST SP 800-115 - Technical Guide to Information Security Testing and Assessment
- NIST SP 800-128 - Guide for Security-Focused Configuration Management of Information Systems
- NIST SP 800-137 - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- NIST SP 800-153 - Guidelines for Securing Wireless Local Area Networks (WLANs)
- NIST SP 800-171 - Protecting Controlled Unclassified Information in non- federal Information Systems and Organizations

3.1 Scope

a. The labor categories, prices, terms and conditions stated under Special Item Numbers 132-45A, 132-45B, 132-45C and 132-45D High Adaptive Cybersecurity Services apply exclusively to High Adaptive Cybersecurity Services within the scope of this Information Technology Schedule.

b. Services under these SINs are limited to Highly Adaptive Cybersecurity Services only. Software and hardware products are under different Special Item Numbers on IT Schedule 70 (e.g. 132-32, 132-33, 132-8), and may be quoted along with services to provide a total solution.

c. These SINs provide ordering activities with access to Highly Adaptive Cybersecurity services only.

d. Highly Adaptive Cybersecurity Services provided under these SINs shall comply with all Cybersecurity certifications and industry standards as applicable pertaining to the type of services as specified by ordering agency.

e. 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.

3.2 Order

a. Agencies may use written orders, Electronic Data Interchange (EDI) orders, Blanket Purchase Agreements, individual purchase orders, or task orders for ordering services under this contract. Blanket Purchase Agreements shall not extend beyond the end of the contract period; all services and delivery shall be made and the contract terms and conditions shall continue in effect until the completion of the order. Orders for tasks which extend beyond the fiscal year for which funds are available shall include FAR 52.232-19 (Deviation – May 2003) Availability of Funds for the Next Fiscal Year. The purchase order shall specify the availability of funds and the period for which funds are available.

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

3.3 Performance of Services

a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity. All Contracts will be fully funded.

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 for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner.

d. Any Contractor travel required in the performance of Highly Adaptive Cybersecurity Services 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.

3.4 Inspection of Services

Inspection of services is in accordance with 552.212-4 - CONTRACT TERMS AND CONDITIONS – COMMERCIAL ITEMS (MAY 2015) (ALTERNATE II – JUL 2009) (FAR DEVIATION – JUL 2015) (TAILORED) for Firm-Fixed Price and Time-and-Materials and Labor-Hour Contracts orders placed under this contract.

3.5 Responsibilities of the Contractor

Subject to the ordering activity's security regulations, the ordering activity shall permit Contractor

access to all facilities necessary to perform the requisite Highly Adaptive Cybersecurity Services.

3.6 Independent Contractor

a. Definitions.

"Contractor" means the person, firm, unincorporated association, joint venture, partnership, or corporation that is a party to this contract.

"Contractor and its affiliates" and "Contractor or its affiliates" refers to the Contractor, its chief executives, directors, officers, subsidiaries, affiliates, subcontractors at any tier, and consultants and any joint venture involving the Contractor, any entity into or with which the Contractor subsequently merges or affiliates, or any other successor or assignee of the Contractor.

An "Organizational conflict of interest" exists when the nature of the work to be performed under a proposed ordering activity contract, without some restriction on ordering activities by the Contractor and its affiliates, may either (i) result in an unfair competitive advantage to the Contractor or its affiliates or (ii) impair the Contractor's or its affiliates' objectivity in performing contract work.

b. To avoid an organizational or financial conflict of interest and to avoid prejudicing the best interests of the ordering activity, ordering activities may place restrictions on the Contractors, its affiliates, chief executives, directors, subsidiaries and subcontractors at any tier when placing orders against schedule contracts. Such restrictions shall be consistent with FAR 9.505 and shall be designed to avoid, neutralize, or mitigate organizational conflicts of interest that might otherwise exist in situations related to individual orders placed against the schedule contract. Examples of situations, which may require restrictions, are provided at FAR 9.508.

3.7 Invoices

The Contractor, upon completion of the work ordered, shall submit invoices for Highly Adaptive Cybersecurity Services. 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.

3.8 Resumes

Resumes shall be provided to the GSA Contracting Officer or the user ordering activity upon request.

3.9 Approval of Subcontracts

The ordering activity may require that the Contractor receive, from the ordering activity's Contracting Officer, written consent before placing any subcontract for furnishing any of the work called for in a task order.

3.10 Description of Highly Adaptive Cybersecurity Services and Pricing

a. The Contractor shall provide a description of each type of Highly Adaptive Cybersecurity Service offered under Special Item Numbers 132-45A, 132-45B, 132-45C and 132-45D for Highly Adaptive Cybersecurity Services and it should be presented in the same manner as the Contractor sells to its commercial and other ordering activity customers. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles (labor categories) for those individuals who will perform the service should be provided.

b. Pricing for all Highly Adaptive Cybersecurity Services shall be in accordance with the Contractor's customary commercial practices; e.g., hourly rates, minimum general experience and minimum education.

The following is an example of the manner in which the description of a commercial job title should be presented (see SCP FSS 004).

EXAMPLE

Commercial Job Title: Computer Network Defense Analysis

Description: Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

Professionals involved in this specialty perform the following tasks:

- Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities
- Provide daily summary reports of network events and activity relevant to Computer Network Defense practices
- Monitor external data sources (e.g., Computer Network Defense vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of Computer Network Defense threat condition and determine which security issues may have an impact on the enterprise.

Knowledge, Skills and Abilities: Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws, etc.), statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed

Minimum Experience: 5 Years

Minimum Education Requirements: a bachelor's of science degree with a concentration in computer science, cybersecurity services, management information systems (MIS), engineering or information science is essential.

Highly Desirable: Offensive Security Certified Professional (OSCP) or commercial Cybersecurity advanced certification(s).

Special Item Number 132-45A – Penetration Testing – Subject to Cooperative Purchasing

Penetration testing is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network. Related Job Titles include but are not limited to: Blue Team Technician, Penetration Tester, Red Team Technician, and Ethical Hacker.

Tasks include but are not limited to:

- Conducting and/or supporting authorized penetration testing on enterprise network assets.
- Analyzing site/enterprise Computer Network Defense policies and configurations and evaluating compliance with regulations and enterprise directives.

- Assisting with the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems, and processes).

Special Item Number 132-45B – Incident Response – Subject to Cooperative Purchasing

Incident response services help organizations impacted by a Cybersecurity compromise determine the extent of the incident, remove the adversary from their systems, and restore their networks to a more secure state.

Related Job Titles include: but are not limited to: Incident Response Analyst, Computer Crime Investigator, and Intrusion Analyst.

Tasks include but are not limited to:

- Collect intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise.
- Perform command and control functions in response to incidents.
- Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.

Special Item Number 132-45C – Cyber Hunt – Subject to Cooperative Purchasing

Cyber hunt activities are responses to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. 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. Responders use information and threat intelligence specifically focused on the proximate incident to identify undiscovered attacks, and investigate and analyze all relevant response activities.

Related Job Titles include but are not limited to: Computer Crime Investigator, Incident Handler, Incident Responder, Incident Response Analyst, Incident Response Coordinator and Intrusion Analyst.

Tasks include but are not limited to:

- 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.
- Correlating incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.

Special Item Number 132-45D – Risk and Vulnerability Assessments (RVA) – Subject to Cooperative Purchasing

Risk and vulnerability assessors conduct assessments of threats and vulnerabilities, determine deviations from acceptable configurations, enterprise or local policy, assess the level of risk, and develop and/or recommend appropriate mitigation countermeasures in operational and non-operational situations. At a minimum, offerors who would like to be considered for this SIN must offer the following services: Network Mapping, Vulnerability Scanning, Phishing Assessment, Wireless Assessment, Web Application Assessment, Operating System Security Assessment (OSSA), and Database Assessment.

Related Job Titles include but are not limited to: Risk/Vulnerability Analyst, Vulnerability Manager, Ethical Hacker, Computer Network Defense (CND) Auditor, Compliance Manager, and Information Security Engineer.

At a minimum, offerors who would like to be considered for this SIN must offer the following services:

- Network Mapping - consists of identifying assets on an agreed upon IP address space or network range(s).
- Vulnerability Scanning - comprehensively identifies IT vulnerabilities associated with agency systems that are potentially exploitable by attackers.
- Phishing Assessment - includes activities to evaluate the level of awareness of the agency workforce with regard to digital form of social engineering that uses authentic looking, but bogus, emails to request information from users or direct them to a fake Website that requests information. Phishing assessments can include scanning, testing, or both and can be conducted as a one-time event or as part of a larger campaign to be conducted over several months.
- Wireless Assessment - includes wireless access point (WAP) detection, penetration testing or both and is performed while onsite at a customer s facility.
- Web Application Assessment - includes scanning, testing or both of outward facing web applications for defects in Web service implementation that may lead to exploitable vulnerabilities. Provides report on how to implement Web services securely and ensure that traditional network security tools and techniques are used to limit access to the Web Service to only those networks and systems that should have legitimate access.
- Operating System Security Assessment (OSSA) - assesses the configuration of select host operating systems (OS) against standardized configuration baselines.
- Database Assessment - assesses the configuration of selected databases against configuration baselines in order to identify potential misconfigurations and/or database vulnerabilities.

3.11 Labor Category Descriptions

NOTE: Any labor category below may be applied to any of the HACS SINs: 132-45A, 132-45B, 132-45C and 132-45D.

Labor Category	Subject Matter Expert (SME)
Functional Responsibilities	**Areas supported include Penetration Testing, Incident Response, Cyber Hunt and Risk and Vulnerability Assessment.** SME IV - Generally recognized as a leader in the industry in their area of expertise; sought out by others in the area of expertise for advice and guidance - Provides expert support, analysis, strategy. Policy, research, and advice into exceptionally complex problems, and processes relating to cybersecurity or other functional area SME III - Serves as technical expert on project teams, providing technical direction, interpretation and alternatives. Expertise is in Cybersecurity or other functional area. - Performs highly specialized and technical tasks associated with the most current and cutting-edge technologies including research and development SME II - Performs technical tasks in his area of expertise with minimal oversight. SME I - Provides technical support in his area of expertise.

Minimum Qualifications and Experience	Qualifications and experience will be determined on a case-by-case basis. Generally, the labor category requires the following minimum qualifications and experience for each corresponding level.	
	Level	**Education/Experience**
	SME IV	BS/BA or, more than 10 years of experience, including demonstrable skills in Cybersecurity, Computer Engineering or Software Development.
	SME III	BS/BA or, 10 years of experience, including demonstrable skills in Cybersecurity, Computer Engineering or Software Development.
	SME II	BS/BA or, 7 years of experience, including demonstrable skills in Cybersecurity, Computer Engineering or Software Development.
	SME I	BS/BA or, 3 years of experience, including demonstrable skills in Cybersecurity, Computer Engineering or Software Development.

Labor Category	**Cyber Team Project Manager**	
Functional Responsibilities	- Manages complex and/or high risk programs. - Directs daily staff and task activities to meet client and corporate work objectives. - Supervises assigned technical and administrative staff, including subordinate managers. - Assures quality of task products, services, and deliverables, including participating in reviews, audits, and site visits. - Serves as a liaison with clients to coordinate activities, negotiate tasks, and solve problems. - Responsible for coordinating and monitoring subcontractor activities.	
Minimum Qualifications and Experience	Qualifications and experience will be determined on a case-by-case basis. Generally, the labor category requires the following minimum qualifications and experience for each corresponding level.	
	Level	**Education / Experience**
	Project Manager	BS/BA or, more than 10 years of Cyber experience, including demonstrable program management skills in Cybersecurity, Computer Engineering or Software Development.

Labor Category	Cyber Team Operations Manager
Functional Responsibilities	- Monitors each task, and keeps the Program Manager abreast of all problems and accomplishments. - Anticipates problems, and works to mitigate occurrence. - As a team or project leader, provides technical direction for the complete systems development effort. - May serve as a technical authority for a design area. - As a staff specialist or consultant, resolves unique and unyielding systems problems using new technology. - Can complete tasks within estimated time frames and budget constraints. - Schedules and assigns duties to subordinates. Interacts with government management personnel.
Minimum Qualifications and Experience	Qualifications and experience will be determined on a case-by-case basis. Generally, the labor category requires the following minimum qualifications and experience for each corresponding level.

Level	Education / Experience
Operations Manager	BS/BA or, more than 8 years of Cyber experience, including demonstrated operations management skills in Cybersecurity, Computer Engineering or Software Development.

Labor Category	Cyber Researcher
Functional Responsibilities	Cyber Research III - Initiates and executes advanced cyber research and/or developments within a cybersecurity environment. - Analyzes problems and develops experimental or theoretical methods, techniques tactics or customized software to complete assigned tasks. - Carries out development and testing of advanced programs on systems, components and materials concurrent with design or testing to better evaluate and minimize future problems. - Develops alternative solutions to existing problems; uses specialized techniques and ingenuity to select and evaluate approaches to unforeseen or unique problems. - Performs or delegates all detail work necessary to determine optimum solutions. - Evaluates proposals and makes recommendations based on

	- Prepares cost and schedule estimates and technical documents on proposed projects in assigned area. - Demonstrates creative ability through patent disclosures, problem solving, reports or technical papers and articles; participates in special projects as required. Cyber Researcher II - Executes advanced cyber research and/or developments within a cybersecurity environment. - Analyzes problems and develops methods, techniques, tactics or customized software to complete assigned tasks. - Carries out development and testing of advanced programs on systems and components. Cyber Researcher I - Supports advanced cyber research and/or development within a cybersecurity environment.	
Minimum Qualifications and Experience	Qualifications and experience will be determined on a case-by-case basis. Generally, the labor category requires the following minimum qualifications and experience for each corresponding level.	
	Level	**Education / Experience**
	CR III	BS/BA or, more than 10 years of experience in Cybersecurity, Computer Engineering or Software Development.
	CR II	BS/BA or, more than 7 years of experience, including demonstrated leadership skills in Cybersecurity, Computer Engineering or Software Development.
	CR I	BS/BA or, more than 3 years of experience, including demonstrated leadership skills in Cybersecurity, Computer Engineering or Software Development.

Labor Category	**Cyber Research Team Leader**	
Functional Responsibilities	- Leads and mentors the Cyber Research Team. - Coordinates all cyber research and development. - Establishes standards for Cyber Research Team performance and monitors conformance with those standards.	
Minimum Qualifications and Experience	Qualifications and experience will be determined on a case-by-case basis. Generally, the labor category requires the following minimum qualifications and experience for each corresponding level.	
	Level	**Education / Experience**
	Cyber Team Leader	BS/BA or, more than 10 years of experience, including demonstrated leadership skills in Cybersecurity, Computer Engineering or Software Development, in addition to demonstrable leadership skills.

Labor Category	Cyber Research Manager	
Functional Responsibilities	- Responsible for managing very complex and/or high risk programs. - Directs daily staff and task activities to meet client and corporate work objectives. - Supervises assigned technical and administrative staff, including subordinate managers. - Assures quality of task products, services, and deliverables, including participating in reviews, audits, and site visits. - Serves as a liaison with clients to coordinate activities, negotiate tasks, and solve problems. - Responsible for coordinating and monitoring	
Minimum Qualifications and Experience	Qualifications and experience will be determined on a case-by-case basis. Generally, the labor category requires the following minimum qualifications and experience for each corresponding level.	
	Level	**Education / Experience**
	Cyber Team Leader	BS/BA or 15 experience, with advanced, demonstrable skills, and 5 years management experience.

Labor Category	PTSSA SAFEScreen Instructor	
Functional Responsibilities	- Schedules, manages and conducts Investigation / Interrogation training in conjunction with the PTSSA SAFEScreen technology.	
Minimum Qualifications and Experience	Qualifications and experience will be determined on a case-by-case basis. Generally, the labor category requires the following minimum qualifications and experience for each corresponding level.	
	Level	**Education / Experience**
	PTSSA Instructor	BS/BA in Law Enforcement or Psychology, or Demonstrable investigation / interrogation experience. Instructor experience in investigation or interrogation.

Labor Category	PTSSA SAFEScreen Examiner	
Functional Responsibilities	- Conducts PTSSA SAFEScreen Investigations / Interrogation of personnel per the contract. - Collects data from the PTSSA device(s). - Writes report. - Submits reports to the proper level of management.	
Minimum Qualifications and Experience	Qualifications and experience will be determined on a case-by-case basis. Generally, the labor category requires the following minimum qualifications and experience for each corresponding level.	
	Level	**Education / Experience**
	PTSSA Examiner	BS/BA or Equivalent, in Law Enforcement or Psychology, or demonstrable investigation / interrogation experience.

Labor Category	Environmental Consultant	
Functional Responsibilities	- The services include, but are not limited to consultation in the areas of: - Planning and documentation services for the development, planning, facilitation, coordination of risk management, and vulnerability assessments and analyses. - Collects and delivers relevant data to the proper level of authority.	
Minimum Qualifications and Experience	Qualifications and experience will be determined on a case-by-case basis. Generally, the labor category requires the following minimum qualifications and experience for each corresponding level.	
	Level	**Education / Experience**
	Environmental Consultant	BS/BA or 3 years relevant, demonstrable experience.

3.12 Pricing

NOTE: Any of the labor rates listed below may be used in support of the following SINs:
132-45A
132-45B
132-45C
132-45D

HACS Labor Category Title	2017 Rate
Subject Matter Expert IV	$ 259.94
Subject Matter Expert III	$ 216.61
Subject Matter Expert II	$ 187.40
Subject Matter Expert I	$ 168.66
Cyber Team Program Manager	$ 259.94
Cyber Team Operations Manager	$ 238.27
Cyber Researcher III	$ 259.94
Cyber Researcher II	$ 242.61
Cyber Researcher I	$ 229.61
Cyber Research Manager	$ 392.93
Cyber Research Team Leader	$ 329.25
PTSSA Instructor	$ 187.40
PTSSA Examiner	$ 149.92
Environmental Consultant	$ 238.27

4. PointStream, Inc. Commitment to Promote Small Business Participation

PREAMBLE

PointStream, Inc. provides commercial products and services to ordering activities. We are committed to promoting participation of small, small disadvantaged and women-owned small businesses in our contracts. We pledge to provide opportunities to the small business community through reselling opportunities, mentor-protégé programs, joint ventures, teaming arrangements, and subcontracting.

COMMITMENT

To actively seek and partner with small businesses.

To identify, qualify, mentor and develop small, small disadvantaged and women-owned small businesses by purchasing from these businesses whenever practical.

To develop and promote company policy initiatives that demonstrate our support for awarding contracts and subcontracts to small business concerns.

To undertake significant efforts to determine the potential of small, small disadvantaged and women-owned small business to supply products and services to our company.

To insure procurement opportunities are designed to permit the maximum possible participation of small, small disadvantaged, and women-owned small businesses.

To attend business opportunity workshops, minority business enterprise seminars, trade fairs, procurement conferences, etc., to identify and increase small businesses with whom to partner.

To publicize in our marketing publications our interest in meeting small businesses that may be interested in subcontracting opportunities.

We signify our commitment to work in partnership with small, small disadvantaged and women-owned small businesses to promote and increase their participation in ordering activity contracts. To accelerate potential opportunities please contact PointStream, Inc., Ronda Foster at 1 (512) 463-1643 or email contracts@point-stream.com.

5. Best Value Blanket Purchase Agreement Federal Supply Schedule

(Insert Customer Name)

In the spirit of the Federal Acquisition Streamlining Act (ordering activity) and (Contractor) enter into a cooperative agreement to further reduce the administrative costs of acquiring commercial items from the General Services Administration (GSA) Federal Supply Schedule Contract(s)_____ _____.

Federal Supply Schedule contract BPAs eliminate contracting and open market costs such as: search for sources; the development of technical documents, solicitations and the evaluation of offers. Teaming Arrangements are permitted with Federal Supply Schedule Contractors in accordance with Federal Acquisition Regulation (FAR) 9.6.

This BPA will further decrease costs, reduce paperwork, and save time by eliminating the need for repetitive, individual purchases from the schedule contract. The end result is to create a purchasing mechanism for the ordering activity that works better and costs less.

Signatures

_____		_____	
Ordering Activity	Date	Contractor	Date

BPA Number _____

(Customer Name) Blanket Purchase Agreement

Pursuant to GSA Federal Supply Schedule Contract Number(s)_____, Blanket Purchase Agreements, the Contractor agrees to the following terms of a Blanket Purchase Agreement (BPA) EXCLUSIVELY WITH (ordering activity):

(1) The following contract items can be ordered under this BPA. All orders placed against this BPA are subject to the terms and conditions of the contract, except as noted below:

Model Number / Part Number	*Special BPA Discount/Price

(2) Delivery

Destination	Delivery Schedules / Dates

(3) The ordering activity estimates, but does not guarantee that, the volume of purchases through this agreement will be_____.

(4) This BPA does not obligate any funds.

(5) This BPA expires on_____or at the end of the contract period, whichever is earlier.

(6) The following office(s) is hereby authorized to place orders under this BPA: Office Point of Contact

(7) Orders will be placed against this BPA via Electronic Data Interchange (EDI), FAX, or paper.

(8) Unless otherwise agreed to, all deliveries under this BPA must be accompanied by delivery tickets or sales slips that must contain the following information as a minimum:

(a) Name of Contractor;
(b) Contract Number;
(c) BPA Number;
(d) Model Number or National Stock Number (NSN);
(e) Purchase Order Number;
(f) Date of Purchase;
(g) Quantity, Unit Price, and Extension of Each Item (unit prices and extensions need not be shown when incompatible with the use of automated systems; provided, that the invoice is itemized to show the information); and
(h) Date of Shipment.

(9) The requirements of a proper invoice are specified in the Federal Supply Schedule contract. Invoices will be submitted to the address specified within the purchase order transmission issued against this BPA.

(10) The terms and conditions included in this BPA apply to all purchases made pursuant to it. In the event of an inconsistency between the provisions of this BPA and the Contractor's invoice, the provisions of this BPA will take precedence.

APPENDIX A

GSA-NEGOTIATED CYBERNANCE CLOUD SERVICES AGREEMENT

BACKGROUND

Cybernance and Customer (also referred to herein as “Party” in the singular and “Parties” in the plural) desire to define the terms and conditions applicable to Customer’s use of Cybernance’s services.

Cybernance has developed a service consisting of a software platform (“Cybernance Platform”) that it makes available to subscribers via the internet for the purpose of supporting cybersecurity governance. Customer wishes to use the Cybernance Platform and associated services in its business operations. Cybernance has agreed to provide and Customer has agreed to use and pay for Cybernance's service subject to the terms and conditions of this agreement. This agreement creates a "software as a service" (SaaS) arrangement, providing for the secure delivery of services to the user's terminal over a network (typically the internet) from processors hosted remotely by Cybernance and its contractors, as distinct from the more traditional "software as a license" which is normally installed on Customers' servers.

1. DEFINITIONS

1.1 The definitions and rules of interpretation in this clause 1 apply in and to this entire document.

Agreement: the entirety of this document.

Authorized Users: those employees, agents, and independent contractors of Customer who are authorized by the Customer to use the Services and the Documentation.

Business Day: any day that is not a Saturday, Sunday, or public holiday in the U.S.

Change of Control: the direct or indirect acquisition of either, the majority of the voting stock, or of all, or substantially all, of the assets, of a party by another entity in a single transaction or a series of transactions.

Confidential Information: information that is proprietary or confidential and is either (a) clearly labeled as such, (b) identified as Confidential Information in clause 4 or 9.5, or, (c) is otherwise generally considered confidential information.

Customer Data: the data inputted by Customer, Authorized Users, or Cybernance on Customer's behalf for the purpose of using the Services or facilitating Customer’s use of the Services, and the output from using the Services.

Documentation: the document made available to Customer by Cybernance online via console.cybernance.com or such other web address as notified by Cybernance to Customer from time to time that sets out a description of the Services and the user instructions for the Services.

Effective Date: the date of this Agreement.

Initial Subscription Term: the initial term of this Agreement as set out in Exhibit A.

Normal Business Hours: 9:00 am to 6:00 pm CDT on each Business Day.

Party: Each of Cybernance and Customer are a Party to this agreement. The term “**Parties**” refers to both Cybernance and Customer.

Renewal Period: the period described in clause 12.2.

Reseller: the company authorized by Cybernance to offer its service for purchase on the GSA Schedule on behalf of Cybernance.

Security Breach: any act or omission that materially compromises either the security, confidentiality, or integrity of Confidential Information or the physical, technical, administrative, or organizational safeguards put in place by Cybernance that relate to the protection of the security, confidentiality, or integrity of Confidential Information.

Services: the subscription services provided by Cybernance to Customer under this Agreement via console.cybernance.com (a/k/a the "Cybernance Platform") or any other website as notified to Customer by Cybernance from time to time, and, as more particularly described in the Documentation.

Software: the online software applications provided by Cybernance as part of the Services.

Subscription Fees: the subscription fees payable by Customer to Cybernance for usage of its Software and Services.

Subscription Term: has the meaning given in clause 12.1.

Support Services Policy: Cybernance's policy for providing support in relation to the Services as made available at console.cybernance.com or such other website address as may be notified to Customer from time to time and attached as Exhibit C.

Virus: any thing or device (including any software, code, file, or program) that may: prevent, impair or otherwise adversely affect the operation of any computer software, hardware, or network, any telecommunications service, equipment, or network, or any other service or device; prevent, impair, or otherwise adversely affect access to or the operation of any program or data, including the reliability of any program or data (whether by re-arranging, altering, or erasing the program or data in whole or part or otherwise); or, adversely affect the user experience, including worms, Trojan horses, viruses, and other similar things or devices.

1.2 Clause, schedule, and paragraph headings shall not affect the interpretation of this Agreement.

1.3 A person includes an individual, corporate, or unincorporated body (whether or not having separate legal personality) and that person's legal and personal representatives, successors or permitted assigns.

1.4 A reference to a company shall include any company, corporation, or other body corporate, wherever and however incorporated or established.

1.5 Words in the singular shall include the plural and vice versa.

1.6 A reference to one gender shall include a reference to the other genders.

1.7 A reference to a statute or statutory provision is a reference to it as it is in force for the time being, taking account of any amendment, extension, or re-enactment and includes any subordinate legislation for the time being in force made under it.

1.8 A reference to writing or written includes faxes but not e-mail.

1.9 References to clauses and schedules are to the clauses and schedules of this Agreement; references to paragraphs are to paragraphs of the relevant schedule to this Agreement.

2. SOFTWARE USAGE

2.1 Subject to the restrictions set out in this clause 2 and the other terms and conditions of this Agreement, Cybernance hereby grants to Customer a non-exclusive, non-transferable right to permit Authorized Users to use the Services and to use, download, display, and make a reasonable number of copies of the Documentation during the Subscription Term solely for Customer's internal business operations.

2.2 In relation to the Authorized Users, Customer undertakes that:

(a) each Authorized User shall keep a secure password for his use of the Services and Documentation, that such password shall be changed no less frequently than every 90 days, and that each Authorized User shall keep his password confidential;

(b) it shall permit Cybernance to audit the Services to establish the name and password of each Authorized User. Such audit may be conducted no more than once per year, at Cybernance's expense, and this right shall be exercised with reasonable prior notice, in such a manner as not to substantially interfere with Customer's normal conduct of business, and shall be subject to applicable Government security requirements;

(c) if any of the audits referred to in clause 2.2(b) reveal that any password has been provided to any individual who is not an Authorized User, then without prejudice to Cybernance's other rights, Customer shall promptly disable such passwords and Cybernance shall not issue any new passwords to any such individual.

2.3 Customer shall not knowingly access, store, distribute or transmit any Viruses, or any material during its use of the Services that:

(a) is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing, or racially or ethnically offensive;

(b) facilitates illegal activity;

(c) depicts sexually explicit images;

(d) promotes unlawful violence;

(e) is discriminatory based on race, gender, color, religious belief, sexual orientation, disability, or any other illegal activity; or

(f) causes damage or injury to any person or property;

(g) and Cybernance reserves the right, without liability to Customer, to disable Customer’s access to any material that breaches the provisions of this clause 2.3.

2.4 Except as may be allowed by any applicable law that is incapable of exclusion by agreement between the parties, and except to the extent expressly permitted under this Agreement, Customer shall not:

(a) attempt to copy, modify, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute all or any portion of the

Software and/or Documentation (as applicable) in any form or media or by any means; or

(b) attempt to reverse compile, disassemble, reverse engineer, or otherwise reduce to human-perceivable form all or any part of the Software; or

(c) access all or any part of the Services and Documentation to build a product or service which competes with the Services and/or the Documentation; or

(d) use the Services and/or Documentation to provide services to unaffiliated third parties; or

(e) subject to clause 16.1, license, sell, rent, lease, transfer, assign, distribute, display, disclose, or otherwise commercially exploit or otherwise make the Services and/or Documentation available to any third party except the Authorized Users, or

(f) attempt to obtain, or assist third parties in obtaining, access to the Services and/or Documentation, other than as provided under this clause 2.

2.5 Customer shall use all reasonable commercial efforts to prevent any unauthorized access to, or use of, the Services and/or the Documentation as specified in clause 2.2 above, and in the event of any such unauthorized access or use, shall promptly notify Cybernance.

2.6 The rights provided under this clause 2 are granted to Customer only and shall not be considered granted to any subsidiary or holding company of Customer.

3. SERVICE AVAILABILITY

3.1 Cybernance shall, during the Subscription Term, provide the Services and make available the Documentation to Customer on and subject to the terms of this Agreement.

3.2 Cybernance shall use commercially reasonable efforts to make the Services available and operating as intended in accordance with the Documentation and without material degradation of service and accessible by Customer 24 hours a day, seven days a week, except for:

(a) planned maintenance carried out during the maintenance window of midnight to 6:00 am U.S. CST; and

(b) unscheduled maintenance performed outside Normal Business Hours, provided that Cybernance has used reasonable efforts to give Customer at least 4 Normal Business Hours written notice in advance.

3.3 Cybernance will, as part of the Services and at no additional cost to Customer, provide Customer with Cybernance’s standard Customer support services in accordance with Cybernance's Support Services Policy in effect at the time that the Services are provided (see Exhibit C for policy in effect at time of signing). Cybernance may amend the Support Services Policy in its sole and absolute discretion from time to time, but may not amend the policy in any way that negatively affects the support provided to Customer, and Cybernance will get changes approved in writing by a duly warranted contracting officer as specified under FAR 43.102 and consistent with FAR 1.601(a). Customer may purchase enhanced support services separately at Cybernance’s then-current rates.

4. CUSTOMER DATA

4.1 Customer shall own all rights, title and interest in and to all of Customer Data and shall have sole responsibility for the legality, reliability, integrity, accuracy and quality of Customer Data as of the time it is entered into the Cybernance Platform, provided, however, that Cybernance will be responsible for the integrity of Customer Data stored in the Cybernance Platform.

4.2 Customer hereby grants Cybernance the right in perpetuity to archive and aggregate a copy of all de-identified Customer Data to combine it with other data to analyze and create data analytics for its commercial use. Cybernance is responsible for keeping Customer's individual data anonymous. Cybernance will delete identifiable Customer Data upon termination of this Agreement in accordance with clause 12.4.

4.3 Cybernance shall follow its archiving procedures for Customer Data as set out in its Backup Policy available at www.cybernance.com/backup-policy/, or such other website address as may be notified to Customer from time to time. The Backup Policy, attached as Exhibit E, may be amended by Cybernance in its sole discretion from time to time, provided, however, that such Backup Policy must comply at all times with the terms and conditions contained in this Agreement and that changes are approved in advance in writing by a duly warranted contracting officer as specified under FAR 43.102 and consistent with FAR 1.601(a). In the event of any loss or damage to Customer Data, Customer's sole and exclusive remedy shall be for Cybernance to use reasonable commercial efforts to restore the lost or damaged Customer Data from the latest backup of such Customer Data maintained by Cybernance in accordance with the archiving procedure described in its Backup Policy. Cybernance shall be responsible for any loss, destruction, alteration, or disclosure of Customer Data caused by third parties subcontracted by Cybernance to perform services related to Customer Data hosting, maintenance, and backup.

4.4 Cybernance shall, in providing the Services, comply with its Privacy and Security Policy relating to the privacy and security of Customer Data available at console.cybernance.com or such other website address as may be notified to Customer from time to time and attached as Exhibit D. Such document may be amended from time to time by Cybernance in its sole discretion, but Cybernance may not amend the policy so as to reduce the level of privacy and security measures currently detailed in Exhibit D and will get changes approved in writing in advance by a duly warranted contracting officer as specified under FAR 43.102 and consistent with FAR 1.601(a).

4.5 The transmitting, processing and storage of Customer Data by Cybernance will be performed only in the United States. Cybernance will provide Customer 90 days' written notice before it changes a third-party service provider or subcontractor that has access to Customer Data. Cybernance must perform due diligence on any third-party service providers to verify that such entities are able to adequately protect the confidentiality and integrity of the Customer Data in accordance with the security controls detailed in this Agreement before permitting access to any such Customer Data.

5. CYBERNANCE'S OBLIGATIONS

5.1 Cybernance warrants that (i) the Services will be performed substantially in accordance with the Documentation, (ii) the Services, including configuration services, and support will be performed with reasonable skill and care and in a workmanlike manner, and (iii) the Documentation is complete and accurate. Cybernance further represents and warrants that its collection, access, use, storage, disposal and disclosure of Confidential Information does and will comply with all applicable federal and state privacy and data protection laws, as well as all other applicable regulations and directives.

5.2 The warranty at clause 5.1 shall not apply to the extent of any non-conformance that is caused by use of the Services contrary to Cybernance's Documentation and this Agreement. If the Services do not conform with the foregoing warranty, Cybernance will, at its expense, use all reasonable commercial efforts to correct any such non-conformance promptly, or provide Customer with a reasonable alternative means of accomplishing the desired performance; and if unable to provide such resolution, allow Customer to terminate this Agreement and receive a pro-rated refund of the fees paid to Cybernance Such correction or substitution (or termination) constitutes Customer's sole and exclusive remedy for any breach of the undertaking set out in clause 5.1. Notwithstanding the foregoing, Cybernance:

(a) does not warrant that Customer's use of the Services will be uninterrupted or error-free; nor that the Services, Documentation, and/or the information obtained by Customer through the Services will meet Customer's requirements; and

(b) is not responsible for any delays, delivery failures, or any other loss or damage resulting from the transfer of data over communications networks and facilities, including the internet, to the extent outside of Cybernance’s control, and Customer acknowledges that the Services and Documentation may be subject to limitations, delays, and other problems inherent in the use of such communications facilities. Note, when the Customer is a Federal Government Agency, excusable delays shall be governed by FAR 52.212-4(f).

5.3 Without limiting Cybernance’s obligations under clause 5.1 above, Cybernance shall implement administrative, physical, and technical safeguards to protect Confidential Information that are no less rigorous than accepted industry practices, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework or other applicable industry standards for information security, and shall ensure that all such safeguards, including the manner in which Confidential Information is collected, accessed, used, stored, processed, disposed of, and disclosed, comply with applicable data protection and privacy laws as well as the terms and conditions of this Agreement.

5.4 At a minimum, Cybernance’s safeguards for the protection of Confidential Information shall include: (i) limiting access to Confidential Information in accordance with clause 9 hereof; (ii) securing business facilities, data centers, paper files, servers, backup systems, and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (iii) implementing network, device application, database, and platform security; (iv)

securing information transmission, storage, and disposal;
(v) implementing authentication and access controls within media, applications, operating systems, and equipment; (vi) strictly segregating Confidential Information from information of Cybernance or its other customers so that Confidential Information is not commingled with any other types of information; (vii) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (viii) providing appropriate privacy and information security training to Cybernance's employees.

5.5 Cybernance shall: (i) provide Customer with the name and contact information for an employee of Cybernance who shall serve as Customer's primary security contact and shall be available as a contact in resolving obligations associated with a Security Breach; (ii) notify Customer of a Security Breach as soon as practicable, but no later than twenty-four (24) hours after Cybernance becomes aware of it; and (iii) notify Customer of any Security Breaches by e-mailing with a read receipt to Cybernance's primary business contact within Customer with a read receipt. Immediately following Cybernance's notification to Customer of a Security Breach, the parties shall coordinate with each other to investigate the Security Breach, and in such event, Cybernance agrees to: (i) assist with any investigation; (ii) provide Customer with physical access to Cybernance's facilities and operations affected; (iii) facilitate interviews with Cybernance's employees and others involved in the matter; and (iv) make available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law, regulation, industry standards, or as otherwise reasonably required by Customer. Cybernance shall take reasonable steps to immediately remedy any Security Breach and prevent any further Security Breach at Cybernance's expense in accordance with applicable privacy rights, laws, regulations, and standards.

5.6 This Agreement shall not prevent Cybernance from entering into similar agreements with third parties, or from independently developing, using, selling or licensing documentation, products, and/or services that are similar to those provided under this Agreement.

5.7 Cybernance warrants that it has and will maintain all necessary licenses, consents, and permissions necessary for the performance of its obligations under this Agreement.

5.8 Cybernance warrants that the Services are and will continue to be free of Viruses and destructible code that may, or may be used to, access, alter, delete, damage, or disable the Services, Customer Data, or other Confidential Information.

5.9 Cybernance will provide the initial setup and configuration of the Services for Customer at Customer's site.

5.10 Cybernance will comply with all applicable laws and regulations with respect to its provision of Services and other obligations under this Agreement.

6. CUSTOMER'S OBLIGATIONS

6.1 Customer shall:

(a) provide Cybernance with:

(i) all necessary co-operation in relation to this Agreement; and

(ii) all necessary access to such information as may be reasonably required by Cybernance to perform the Services;

(iii) security access information and configuration services required to render the Services, including but not limited to Customer Data;

(b) comply with all applicable laws and regulations with respect to its activities under this Agreement;

(c) carry out all other Customer responsibilities set out in this Agreement in a timely and efficient manner. In the event of any delays in Customer's provision of such assistance as agreed by the parties, Cybernance may adjust any agreed timetable or delivery schedule as reasonably necessary;

(d) ensure that the Authorized Users use the Services and the Documentation in accordance with the terms and conditions of this Agreement. In the event of a breach, Cybernance will submit a claim in a manner consistent with the procedure contained in FAR 52.233-1 and consistent with FAR 12. 302(b);

(e) obtain and maintain all necessary licenses, consents, and permissions necessary for Customer to use the Services under this Agreement;

(f) ensure that its network and systems comply with the relevant specifications provided by Cybernance from time to time, provided that Cybernance provides Customer will no less than 90 days advance written notice of any changes; and

(g) be solely responsible for procuring and maintaining its network connections and telecommunications links from its systems to Cybernance's data centers, and all problems, conditions, delays, delivery failures, and all other loss or damage solely caused by Customer's network connections or telecommunications links or caused by Customer's internet provider services.

7. CHARGES AND PAYMENT

7.1 Any and all Subscription Fees and other payments will be defined in Exhibit B.

7.2 The Reseller shall invoice Customer in accordance with this clause 7 and 21.1.

7.3 Customer shall on the Effective Date provide to Reseller its approved purchase order information, and Reseller shall invoice Customer:

(a) on the Effective Date for the Subscription Fees payable in respect of the Initial Subscription Term; and

(b) Customer shall pay each invoice within 30 days after receipt of such invoice for undisputed amounts.

7.4 When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be made as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, Cybernance shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

7.5 All amounts and fees stated or referred to in this Agreement:

(a) shall be payable in U. S. dollars;

(b) are, subject to clause 11.4(b), non-cancellable and non-refundable, except as otherwise provided in this Agreement;

(c) Reseller shall state separately on invoices taxes excluded from the fees, and the Customer agrees either to pay the amount of the taxes (based on the current value of the equipment) or provide evidence necessary to sustain an exemption, in accordance with FAR 52.229-1 and FAR 52.229-3.

7.6 Each Party acknowledges that its name and its logo have value. The Parties mutually agree to allow the other Party to use its name and logo in advertising Customer relationship, while promising to guard Customer's Confidential Information as specified in clause 9, upon the prior written approval of the other Party.

8. PROPRIETARY RIGHTS

8.1 Customer acknowledges and agrees that Cybernance and/or its licensors own all intellectual property rights in the Services and the Documentation. Except as expressly stated herein, this Agreement does not grant Customer any rights to, or in, patents, copyrights, database rights, trade secrets, trade names, trade marks (whether registered or unregistered), or any other rights or licenses in respect of the Services or the Documentation.

8.2 Cybernance confirms that it has all the rights in relation to the Services and the Documentation that are necessary to grant all the rights it purports to grant under, and in accordance with, the terms of this Agreement.

9. CONFIDENTIALITY

9.1 Each party may be given access to confidential and/or proprietary business information (collectively, "Confidential Information") from the other party that is necessary to perform its obligations under this Agreement. A party's Confidential Information shall not be deemed to include information that:

(a) is or becomes publicly known other than through any act or omission of the receiving party;

(b) was in the other party's lawful possession before the disclosure;

(c) is lawfully disclosed to the receiving party by a third party without restriction on disclosure;

(d) is independently developed by the receiving party, which independent development can be shown by written evidence; or

(e) is required to be disclosed by law, by any court of competent jurisdiction or by any regulatory or administrative body.

9.2 Each party shall hold the other's Confidential Information in strict confidence and, unless required by law, shall not make the other's Confidential Information available to any third party or use the other's Confidential Information for any purpose other than the implementation of this Agreement.

9.3 Each party shall use its best efforts to protect the secrecy of, and avoid the unauthorized disclosure or use of, Confidential Information. Each party will only disclose Confidential Information to which it has access to employees who have a need to know and will not otherwise disclose or distribute such information without the express written permission of the disclosing party.

9.4 Customer acknowledges that details of the Services, and the results of any performance tests of the Services, constitute Cybernance's Confidential Information.

9.5 Cybernance acknowledges that Customer Data, together with the results from the Cybernance Platform assessment, constitute Confidential Information of Customer, which, in Customer's sole discretion, Customer may disclose to its employees, clients, and/or insurance underwriters and brokers.

9.6 Each party will promptly notify the other party in writing if it becomes aware of a loss, suspected misuse, or unauthorized access or disclosure of the other party's Confidential Information.

9.7 Except as required by law or regulation or court order and subject to clause 4.2 herein, upon termination of the Agreement, or at such earlier time as either party may request in writing, a party receiving Confidential Information of the requesting party shall promptly return to such requesting party all copies, whether in written, electronic or other form or media, of Confidential Information in its possession or securely dispose of all such copies, and certify in writing to the requesting party that such Confidential Information has been returned or disposed of securely.

9.8 Cybernance recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which requires that certain information be released, despite being characterized as "confidential" by the vendor.

9.9 This clause 9 shall survive termination of this Agreement, however arising.

10. INDEMNITY

10.1 Cybernance shall, subject to clause 11.4, defend Customer, its officers, directors and employees against any claim, actions, proceedings, losses, damages, expenses, and costs (including without limitation court costs and reasonable legal fees) (i) that the Services or Documentation infringes any United States patent, copyright, trademark, database right, or other intellectual property right or violation of right of confidentiality, and, (ii) to the extent arising out of Cybernance's or its subcontractor's breach of this Agreement, negligence, willful misconduct, or violation of law, and shall indemnify Customer for any amounts awarded against Customer in judgment or settlement of such claims, provided that:

(a) Cybernance is given prompt notice of any such claim;

(b) Customer provides reasonable cooperation to Cybernance in the defense and settlement of such claim, at Cybernance's sole expense; and

(c) Cybernance is given authority to defend or settle the claim.

10.2 In the defense or settlement of any claim under subpart (i) of clause 10.2, Cybernance may procure the right for Customer to continue using the Services, replace or modify the Services so that they become non-infringing without materially reducing the

functionality or, if such remedies are not reasonably available, terminate this Agreement within five (5) Business Days' notice to Customer and promptly provide a pro-rated refund of prepaid fees. For the avoidance of doubt, this clause does not limit Cybernance's indemnity obligations under clause 10.2.

10.3 In no event shall Cybernance, its employees, agents and subcontractors be liable to Customer to the extent that the alleged infringement is based on:

(a) Customer's use of the Services or Documentation in a manner contrary to the Documentation given to Customer by Cybernance; or

(b) Customer's use of the Services or Documentation after written notice of the alleged or actual infringement from Cybernance or any appropriate authority.

10.4 The foregoing states Customer's sole and exclusive rights and remedies, and Cybernance's (including Cybernance's employees', agents; and subcontractors') entire obligations and liability, for infringement of any patent, copyright, trademark, database right, or right of confidentiality.

10.5 Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516.

10.6 This clause 10 shall survive termination of this Agreement, however arising.

11. LIMITATION OF LIABILITY

11.1 Subject to the provisions of clause 10, this clause 11 sets out the entire financial liability of a party, including any liability for the acts or omissions of its employees, agents, and subcontractors, to the other party in respect of:

(a) any breach of this Agreement;

(b) any use made by Customer of the Services and Documentation or any part of them; and

(c) any representation, statement, or tortious act or omission (including negligence) arising under or in connection with this Agreement.

11.2 Except as expressly and specifically provided in this Agreement:

(a) Customer assumes sole responsibility for results obtained from the use of the Services and the Documentation by Customer, and for conclusions drawn from such use. Cybernance shall have no liability for any damage caused by errors or omissions in any information, instructions, or scripts provided to Cybernance by Customer in connection with the Services, or any actions taken by Cybernance at Customer's direction; and

(b) all warranties, representations, conditions and all other terms of any kind whatsoever implied by statute or common law are, to the fullest extent permitted by applicable law, excluded from this Agreement.

11.3 THIS AGREEMENT SHALL NOT IMPAIR THE U.S. GOVERNMENT'S RIGHT TO RECOVER FOR FRAUD OR CRIMES ARISING OUT OF OR RELATED TO THIS CONTRACT UNDER ANY FEDERAL FRAUD STATUTE, INCLUDING THE FALSE CLAIMS ACT, 31 U.S.C. 3729-3733. FURTHERMORE, THIS

CLAUSE SHALL NOT IMPAIR NOR PREJUDICE THE U.S. GOVERNMENT'S RIGHT TO EXPRESS REMEDIES PROVIDED IN THE GSA SCHEDULE CONTRACT (E.G., CLAUSE 552.238-75 – PRICE REDUCTIONS, CLAUSE 52.212-4(H) – PATENT INDEMNIFICATION, AND GSAR 552.215-72 – PRICE ADJUSTMENT – FAILURE TO PROVIDE ACCURATE INFORMATION).

11.4 Subject to clause 11.2 and clause 11.3, and except for a party's indemnity obligations under clause 10, negligence, or willful misconduct:

(a) Neither party shall be liable, whether in tort (including for negligence or breach of statutory duty), contract, misrepresentation, restitution, or otherwise, for any loss of profits, loss of business, depletion of goodwill and/or similar losses, or pure economic loss, or for any special (except to the extent damages from breach of confidentiality provisions constitute special damages), indirect or consequential loss, costs, damages, charges, or expenses however arising under this Agreement; and

(b) Each party's total aggregate liability in contract, tort (including negligence or breach of statutory duty), misrepresentation, restitution or otherwise, arising in connection with the performance or contemplated performance of this Agreement shall be limited to the total Subscription Fees paid during the twelve (12) months immediately preceding the date on which the claim arose.

11.5 This clause 11 shall survive termination of this Agreement, however arising.

12. TERM AND TERMINATION

12.1 This Agreement shall, unless otherwise terminated as provided in this clause 12, commence on the Effective Date and shall continue for the Initial Subscription Term as defined in Exhibit A.

12.2 When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be made as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, Cybernance shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

12.3 Upon termination of this Agreement for any reason:

(a) all licenses granted under this Agreement shall immediately terminate;

(b) each party shall return or destroy and make no further use of any equipment, property, Documentation, and other items (and all non-archival copies of them) belonging to the other party;

(c) Cybernance will destroy or otherwise dispose of any of Customer Data in its possession, except as noted in clause 4.2, unless Cybernance receives, no later than 30 days after the effective date of the termination of this Agreement, a written request for the delivery to Customer of the then most recent backup of Customer Data. Cybernance shall use reasonable commercial efforts to deliver the backup to

Customer within 30 days of its receipt of such a written request. Customer shall pay all reasonable expenses incurred by Cybernance in returning Customer Data, and after providing Customer such backup of Customer Data, will promptly and securely destroy all of Customer Data in its possession in accordance with clause 9.7 herein; and

(d) the accrued rights of the parties as at termination, or the continuation after termination of any provision expressly stated to survive or implicitly surviving termination, shall not be affected or prejudiced.

(e) This clause 12.4 shall survive termination of this Agreement, however arising.

13. FORCE MAJEURE

13.1 Excusable delays shall be governed by FAR 52.212-4(f).

14. WAIVER

14.1 A waiver of any right under this Agreement is only effective if it is in writing and it applies only to the party to whom the waiver is addressed and to the circumstances for which it is given.

14.2 Unless specifically provided otherwise, rights arising under this Agreement are cumulative and do not exclude rights provided by law.

15. ENTIRE AGREEMENT

15.1 This Agreement, together with the underlying GSA Schedule Contract, Schedule Pricelist and Purchase Order(s), and any documents referred to in it, constitute the whole agreement between the parties and supersede any previous arrangement, understanding, or agreement between them relating to the subject matter they cover.

15.2 Absent fraud or misrepresentation by a party, each of the parties acknowledges and agrees that in entering into this Agreement, it does not rely on any undertaking, promise, assurance, statement, representation, warranty, or understanding (whether in writing or not) of any person (whether party to this Agreement or not) relating to the subject matter of this Agreement, other than as expressly set out in this Agreement.

16. ASSIGNMENT

16.1 Neither party shall, without the prior written consent of the other party, assign, transfer, charge, or deal in any other similar manner with all or any of its rights or obligations under this Agreement.

16.2 Subject to clause 4.5, Cybernance may at any time subcontract its obligations under this Agreement, however it will remain liable to Customer for the acts or omissions of the subcontractor.

17. NO PARTNERSHIP OR AGENCY

17.1 Nothing in this Agreement is intended to or shall operate to create a partnership between the parties, or authorize either party to act as agent for the other, and neither party shall have the authority to act in the name or on behalf of or otherwise to bind the other in any way, including, but not limited to, the making of any representation or warranty, the assumption of any obligation or liability and the exercise of any right or power.

18. THIRD PARTY RIGHTS

18.1 This Agreement does not confer any rights on any person or party other than the parties to this Agreement and, where applicable, their successors and permitted assigns.

19. NOTICES

19.1 Any notice required to be given under this Agreement shall be in writing and shall be delivered by hand or sent by prepaid first class post or recorded delivery post to the other party at its address set out in this Agreement, or such other address as may have been notified by that party for such purposes, or sent by fax to the other party's fax number as set out in this Agreement.

19.2 A notice delivered by hand shall be deemed to have been received when delivered, or if delivery is not in business hours, at 9:00 am on the first Business Day following delivery. A correctly addressed notice sent by prepaid first class post or recorded delivery post shall be deemed to have been received upon actual receipt. A notice sent by fax shall be deemed to have been received at the time of successful transmission (as shown by the timed printout obtained and retained by the sender).

20. [RESERVED]

21. GENERAL PROVISIONS

21.1 Governing Law; Consent to Personal Jurisdiction. This Agreement will be governed by and construed according to the Federal laws of the United States. This clause survives termination of the Agreement.

21.2 Waiver. No waiver by either Party of any breach of this Agreement shall be a waiver of any preceding or succeeding breach. No waiver by either Party of any right under this Agreement shall be construed as a waiver of any other right.

21.3 If any provision or part of a provision of this Agreement is found by any court or administrative body of competent jurisdiction to be invalid, unenforceable, or illegal, the other provisions shall remain in force.

21.4 If any invalid, unenforceable, or illegal provision would be valid, enforceable, or legal if some part of it were deleted, the provision shall apply with whatever modification is necessary to give effect to the commercial intention of the parties.

21.5 Insurance. Cybernance will carry the following types and amounts of insurance for the duration of the Agreement. Cybernance will provide Customer with a certificate of insurance evidencing this coverage within five days after the execution of the Agreement and thereafter as requested by Customer:

(a) Commercial General Liability insurance with minimum limits of $1,000,000 per occurrence and $2,000,000 general aggregate;

(b) Professional Liability or Errors or Omissions insurance for liability stemming from rendering or failing to render any professional service for which Cybernance has been contracted. The limits of insurance will be $2,000,000 per occurrence and a $2,000,000 aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as undertaken by Cybernance in this Agreement and shall include, but not be limited to, claims involving infringement of intellectual

property, including but not limited to infringement of copyright, trademark, trade dress, information theft, damage to or destruction of electronic information, release of confidential information, alteration of electronic information, extortion, and network security; and

(c) Audit. Customer (or, upon Customer's election, a third party on Customer's behalf) has the right to reasonable access to all of the Cybernance's (including any subcontractors) premises, personnel, operations, books, and records relating to its duties and obligations under this Agreement, including Cybernance's physical and/or technical security controls in relation to all Confidential Information being handled and/or services being provided to Customer pursuant to this Agreement, as well as compliance with any applicable laws, regulations, and industry standards. Such audit may be conducted no more than once per year, at Customer's expense, and this right shall be exercised with reasonable prior notice, in such a manner as not to substantially interfere with Cybernance's normal conduct of business. Cybernance and its subcontractors shall fully cooperate with such assessment by providing access to knowledgeable personnel, physical premises, documentation, infrastructure, and application software that processes, stores, or transports Confidential Information for Customer pursuant to this Agreement. In addition, upon Customer's written request, Cybernance shall provide Customer with the results of any audit by or on behalf of Cybernance performed that assesses the effectiveness of Cybernance's information security program as relevant to the security and confidentiality of Confidential Information shared during the course of this Agreement.

Exhibit A: Initial Subscription Term

The term will be specified in the applicable Government Purchase Order.

Exhibit B: Application, Subscription, and Payments

This information will appear in the Reseller's GSA Schedule Pricelist.

Exhibit C: Support Services Policy

- Telephone support is available during Normal Business Hours.
- Email support is available any time. Responses will occur within 2 hours of request during Normal Business Hours.
- Online support manuals will be made available and regularly updated.
- Enhanced support may be purchased through the execution of a separate Government Purchase Order, for additional fees.

Exhibit D: Privacy and Security Policy

Privacy Policy – Government Contracts

Cybernance Corporation

Sponsoring Office: Product Management
Effective Date: August 9, 2017
Last Reviewed: August 9, 2017
Next Scheduled Review: January 1, 2019

1 PRIVACY POLICY
2 INFORMATION COLLECTION AND USE
3 LOG DATA
4 COOKIES
5 SECURITY
6 SECURITY PRACTICES
7 TRANSIT & STORAGE OF SENSITIVE DATA
8 3RD-PARTY PARTNER PRIVACY & SECURITY
9 CHANGES TO THIS PRIVACY POLICY
10 PRIVACY COMPLAINT PROCEDURE

Cybernance Corporation

Subject: **Cybernance License Agreement | Exhibit D | Privacy and Security Policy**
Privacy Complaints Procedure

1. PRIVACY POLICY

Cybernance Corporation ("us", "we", or "our") operates at

http://www.cybernance.com/ (the "Site"). This page informs you of our policies regarding the collection, use and disclosure of Personal Information we receive from users of the Site.

We use your Personal Information only for providing and improving the Site. By using the Site, you agree to the collection and use of information in accordance with this policy.

2. INFORMATION COLLECTION AND USE

While using our Site, we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you. Personally identifiable information may include, but is not limited to your name ("Personal Information").

3. LOG DATA

Like many site operators, we collect information that your browser sends whenever you visit our Site ("Log Data"). This Log Data may include information such as your computer's Internet Protocol ("IP") address, browser type, browser version, the pages of our Site that you visit, the time and date of your visit, the time spent on those pages and other statistics.

4. COOKIES

Cookies are files with small amount of data, which may include an anonymous unique identifier. Cookies are sent to your browser from a web site and stored on your computer's hard drive.

Like many sites, we use "cookies" to collect information. You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some portions of our Site.

5. SECURITY

The security of your Personal Information is important to us, but remember that no method of transmission over the Internet, or method of electronic storage, is 100% secure. While we strive to use industry leading means to protect your Personal Information, we cannot guarantee its absolute security.

6. SECURITY PRACTICES

Cybernance Security Practices align with the standards put forth in The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). Cybernance uses its own platform to manage

cybersecurity and conducts compliance assessments to our cybersecurity policies & procedures on a quarterly basis.

7. Transit & Storage of Sensitive Data

Cybernance takes special precautions with Customer data related to their use of our software. Such data is encrypted at all times in transit and in storage. When necessary, records of Customer software usage will be transmitted to authorized legal counsel and will be done so using private connections.

8. 3rd-Party Partner Privacy & Security

Cybernance uses a number of service providers whose Privacy & Security Policies are available upon request. Cybernance also uses its own platform to assess 3rd parties for cybersecurity measures before use of any Cybernance systems or data.

9. Changes to This Privacy Policy

Cybernance Corporation may update this Privacy Policy from time to time. Before implementing any policy change, we will notify you of any changes and seek your written concurrence in accordance with the changes clause in the contract.

10. Procedure for Alleged Privacy Breaches

1. A written complaint must be forwarded to Cybernance Security Officer as quickly as possible, but no later than two (2) weeks after the time the government first became aware of the alleged privacy breach. The complaint must specify details of the alleged breach.
2. The Cybernance Security Officer must make a determination on the complaint within forty-five (45) days of receipt of the complaint, and advise the government in writing.
3. If the Cybernance Security Officer determines that there has been a breach of the Privacy Principles, upon notification of the determination to the complainant, he or she will advise Cybernance Executives in writing of any action required in order to remedy the breach. If the breach is capable of being rectified and is not rectified within thirty (30) days of the advice from the Cybernance Security Officer, the Cybernance Security Officer must inform Cybernance Executives of the projected completion date.
4. The Cybernance Security Officer will keep a record of all complaints. This will comprise a register and file records that will be securely stored.
5. Consequences if the Privacy Policy is breached: Disciplinary action may be taken against any person who breaches this policy, including dismissal in the event of what Cybernance considers to be a serious breach by a staff member.

Backup Policy

Cybernance Corporation

Sponsoring Office: Product Management
Effective Date: January 27, 2017
Last Reviewed: January 27, 2017
Next Scheduled Review: January 1, 2018

Exhibit E: Backup Policy

1 POLICY STATEMENT

2 DATABASE SERVER

3 APPLICATION SERVERS

4 UPON TERMINATION

Cybernance Corporation

Subject: **Cybernance Backup Policy and Procedures**

1. POLICY STATEMENT

Cybernance employs daily offsite backups, continuous replication, and point-in-time recovery.

Cybernance utilizes Amazon Web Service as their hosting platform. Amazon's service is best in class, and guarantees the "five 9's" of uptime (99.999%), triple-redundant backups daily, and a multitude of security audit certifications for their data centers.

All Cybernance Platform code is stored in GitHub in a minimum of three redundant server farms, with at least one of them in a different physical location than the other two. It would take a catastrophe of epic

proportions to destroy all three sites simultaneously (in which case, our local backups would be used to recover).

The Cybernance Platform runs on a database server, three application servers, two redistribution ("redis") servers, and load balancers. The servers are designed to replicate data or fail over to a secondary database to enable uninterrupted service in the event of a technical or other issue.

An Amazon service called RDS with synchronous replication enabled is used. This means that every piece of data written to the database is synchronously replicated to another data center. In the event that the primary database, or even the entire data center that holds the primary database, fails in some way, the secondary database will pick up and respond to queries without manual intervention.

In the event that both the primary and secondary databases, or the data centers that hold them, fail in some way, Cybernance can make use of backups and the point-in-time restore capabilities of those backups. These backups are up-to-date within 5 minutes.

The Cybernance Platform application servers are stateless, meaning that no information other than the code of the application is stored on the servers. If a server goes down, the load balancers will automatically redirect requests to the remaining application servers in other data centers, and users will not even be logged out or know that anything has occurred. Currently, three data centers are used. In the event that all three data centers fail, a new server with the code can be provisioned, since distributed backups of both the servers themselves, the code, and the deployment mechanisms have been continuously maintained. The two RDS servers are managed by Amazon and are set up in a failover configuration that holds information about background asynchronous jobs (e.g., generating reports, emails, and so on). If one fails, the other one will take the load as they are provisioned to be large enough for that possibility. If both fail, then some reports and emails will not go out until they have been restored to service by Amazon.

2. DATABASE SERVERS

An Amazon service called RDS with synchronous replication enabled is used. This means that every piece of data written to the database is synchronously replicated to another data center. Should the primary database, or even the entire data center that holds the primary database, fail in some way, the secondary database will pick up and respond to queries without any manual intervention. If both the primary and secondary databases, or the data centers that hold them, fail in some way, Cybernance can make use of backups, and the point-in-time restore capabilities of those backups. These backups are generally up to date within 5 minutes.

3. APPLICATION SERVERS

Application servers are stateless, meaning that no information other than the code of the application is stored on the servers. If a server goes down, the load balancers will automatically redirect requests to the

remaining application servers in other data centers, and users will not even be logged out or know that anything has gone wrong. Currently, three data centers are used. If all three data centers fail, a new server with the code can be provisioned, since distributed backups of both the servers themselves, the code, and the deployment mechanisms have been continuously maintained.

4. UPON TERMINATION

A customer who elects to terminate a paid license, either through cancelation or expiration of the license term, may request a data file containing the most current information associated with their accounts.