IT-CNP, INC.

ADVANCED GOVERNMENT ORIENTED CLOUD HOSTING SOLUTIONS AND MANAGED SERVICES

GSA MULTIPLE AWARD SCHEDULE (MAS) PRICE LIST

FISMA CLOUD

SECURITY COMPLIANCE

DISASTER RECOVERY

APPLICATION SUPPORT

GSA MAS Contract Number GS-35F-099BA

FedRAMP

FEDRAMP HIGH IMPACT CERTIFIED CLOUD

IT-CNP Inc.

GSA MULTIPLE AWARD SCHEDULE (MAS) PRICELIST

Special Item Number 54151S (legacy 54151S) - Information Technology Professional Services

Special Item Number 54151ECOM (legacy 54151ECOM) - Electronic Commerce and Subscription Services

Special Item Number 518210C (legacy 518210C) - Cloud and Cloud-Related IT Professional Services

OLM – Order Level Material

IT-CNP, INC.

9160 Red Branch Road, Columbia, Maryland 21045

(410) 884-1004 | (800) 967-1004

www.it-cnp.com | www.govdatahosting.com

Contract Number: GS-35F-099BA

Period Covered by Contract: 12/1/2018 - 11/30/2023

Pricelist current through Modification # A824, dated 8/19/2020.

Products and ordering information in this Authorized Federal Supply Schedule Pricelist are also available on the GSA Advantage! System (http://www.gsaadvantage.gov).

TABLE OF CONTENTS

1. Information For Ordering Activities Applicable To All Special Item Numbers

1.1 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 micropurchase 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 micropurchase threshold, customers are to give preference to small business concerns when two or more items at the same delivered price will satisfy their requirement.

1.2 GEOGRAPHIC SCOPE OF CONTRACT:

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

Overseas delivery is delivery to points outside of the 48 contiguous states, Washington, DC, Alaska, Hawaii, Puerto Rico, and U.S. Territories.

Offerors are requested to check one of the following boxes:

[**X**] **The Geographic Scope of Contract will be domestic and overseas delivery.**
[ ] The Geographic Scope of Contract will be overseas delivery only.
[ ] The Geographic Scope of Contract will be domestic delivery only.

1.3 CONTRACTOR'S ORDERING ADDRESS AND PAYMENT INFORMATION:

Ordering Address:

IT-CNP, Inc.
8775 Centre Park Drive, Suite153
Columbia, MD 21045-2104
Telephone: 410-884-1004
Facsimile: 410-884-0412
Email: contracts@it-cnp.com

Payment/Remittance Information

IT-CNP, Inc.
8775 Centre Park Drive, Suite153
Columbia, MD 21045-2104
Attn: Accounts Receivable

Contractor must accept the credit card for payments equal to or less than the micro-purchase for oral or written orders under this contract. The Contractor and the ordering agency may agree to use the credit card for dollar amounts over the micro-purchase threshold (See GSAR 552.232-79 Payment by Credit Card). In addition, bank account information for wire transfer payments will be shown on the invoice.

The following telephone number(s) and email address can be used by ordering activities to obtain technical and/or ordering assistance: **Telephone: (410) 884-1004 | contracts@it-cnp.com**

1.4 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.

1.5 STATISTICAL DATA FOR GOVERNMENT ORDERING OFFICE COMPLETION OF STANDARD FORM 279:

Block 9: G. Order/Modification Under Federal Schedule Contract
Block 16: Data Universal Numbering System (DUNS) Number: **04-548-6755**
Block 30: Type of Contractor: **A. Small Business**
Block 31: Woman-Owned Small Business - **No**
Block 37: Contractor's Taxpayer Identification Number (TIN): **52-235-4055**
Block 40: Veteran Owned Small Business (VOSB): **No**

4a. CAGE Code: **1XVF0**
4b. Contractor has registered with the Central Contractor Registration Database.

1.6 FOB DESTINATION - N/A

1.7 DELIVERY SCHEDULE

a. TIME OF DELIVERY: The Contractor shall deliver to destination within the number of calendar days after receipt of order (ARO), as set forth below:

SPECIAL ITEM NUMBER	DELIVERY TIME (Days ARO)
54151S	Delivery is 30 calendar days after receipt of a valid, acceptable order, or as negotiated and mutually agreed for each individual delivery/task order.
54151ECOM	Delivery is 30 calendar days after receipt of a valid, acceptable order, or as negotiated and mutually agreed for each individual delivery/task order.
518210C	Delivery is 30 calendar days after receipt of a valid, acceptable order, or as negotiated and mutually agreed for each individual delivery/task order.

b. 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.

1.8 DISCOUNTS: Prices shown are NET Prices; Basic Discounts have been deducted.

a. Prompt Payment: **None**

b. Quantity: **None**

c. Dollar Volume: **None**

d. Government Educational Institutions: **Government Educational Institutions are offered the same discounts as all other Government customers.**

d. Other: **Payment Terms - Net 30 Days**

1.9 TRADE AGREEMENTS ACT OF 1979, as amended:

All items are U.S. made end products, designated country end products, Caribbean Basin country end products, Canadian end products, or Mexican end products as defined in the Trade Agreements Act of 1979, as amended.

1.10 STATEMENT CONCERNING AVAILABILITY OF EXPORT PACKING: N/A

1.11 Small Requirements: The minimum dollar of orders to be issued is **$100.00**

1.12 MAXIMUM ORDER (All dollar amounts are exclusive of any discount for prompt payment.)

The Maximum Order for the following Special Item Numbers (SINs) is $500,000:

Special Item Number 54151S - Information Technology Professional Services
Special Item Number 54151ECOM - Electronic Commerce (EC) Services
Special Item Number 518210C – Cloud Computing Services

1.13 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.

1.14 FEDERAL INFORMATION TECHNOLOGY/TELECOMMUNICATION 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.

1.15 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), 5285 Port Royal Road, Springfield, Virginia 22161. FIPS PUBS include voluntary standards when these are adopted for Federal use. Individual orders for FIPS PUBS should be referred to the NTIS Sales Office, and orders for subscription service should be referred to the NTIS Subscription Officer, both at the above address, or telephone number (703) 487-4650.

1.16 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, National Institute of Standards and Technology (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, National Institute of Standards and Technology, Gaithersburg, MD 20899, telephone number (301)975-2833.

1.17 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 with 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).

1.18 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 (l) Termination for the ordering activity's convenience, and (m) Termination for Cause (See 52.212-4)

1.19 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. GSA Advantage! will allow the user to perform various searches across all contracts including, but not limited to:

(1) Manufacturer;
(2) Manufacturer's Part Number; and
(3) Product categories.

Agencies can browse GSA Advantage! by accessing the Internet World Wide Web utilizing a browser (ex.: NetScape). The Internet address is http://www.gsaadvantage.gov

1.20 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.

1.21 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.

c. The maintenance/repair service provided is the standard commercial terms and conditions for the type of products and/or services awarded.

1.22 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:

Services are only offered to U.S. Government customers overseas.

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.

1.23 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).

1.24 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.

1.25 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 received 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.

1.26 SECTION 508 COMPLIANCE.

I certify that in accordance with 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d), FAR 39.2, and the Architectural and Transportation Barriers Compliance Board Electronic and Information Technology (EIT) Accessibility Standards (36 CFR 1194) General Services Administration (GSA), that all IT hardware/software/services are 508 compliant:

Yes **X (where applicable)**

No _____

The offeror is required to submit with its offer a designated area on its website that outlines the Voluntary Product Accessibility Template (VPAT) or equivalent qualification, which ultimately becomes the Government Product Accessibility Template (GPAT). If applicable, Section 508 compliance information on the supplies and services in this contract are available at the following website address (URL): www.it-cnp.com

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

1.27 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.

1.28 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.

1.29 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.

1.30 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 Information Technology (IT) Professional Services (SIN 54151S)

2.1 SCOPE

a. The prices, terms and conditions stated under 54151S Information Technology Professional Services category apply exclusively to IT/IAM Professional Services within the scope of this Information Technology Schedule.

b. 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.

2.2 PERFORMANCE INCENTIVES I-FSS-60 Performance Incentives (April 2000)

a. Performance incentives may be agreed upon between the Contractor and the ordering activity on individual fixed price orders or Blanket Purchase Agreements under this contract.

b. The ordering activity must establish a maximum performance incentive price for these services and/or total solutions on individual orders or Blanket Purchase Agreements.

c. Incentives should be designed to relate results achieved by the contractor to specified targets. To the maximum extent practicable, ordering activities shall consider establishing incentives where performance is critical to the ordering activity's mission and incentives are likely to motivate the contractor. Incentives shall be based on objectively measurable tasks.

2.3 ORDER

a. Agencies may use written orders, 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.

2.4 PERFORMANCE OF SERVICES

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

b. The Contractor agrees to render services only 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 IT/IAM 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.

2.5 STOP-WORK ORDER (FAR 52.242-15) (AUG 1989)

(a) The Contracting Officer may, at any time, by written order to the Contractor, require the Contractor to stop all, or any part, of the work called for by this contract for a period of 90 days after the order is delivered to the Contractor, and for any further period to which the parties may agree. The order shall be specifically identified as a stop-work order issued under this clause. Upon receipt of the order, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the order during the period of work stoppage. Within a period of 90 days after a stop-work is delivered to the Contractor, or within any extension of that period to which the parties shall have agreed, the Contracting Officer shall either-

(1) Cancel the stop-work order; or

(2) Terminate the work covered by the order as provided in the Default, or the Termination for Convenience of the Government, clause of this contract.

(b) If a stop-work order issued under this clause is canceled or the period of the order or any extension thereof expires, the Contractor shall resume work. The Contracting Officer shall make an equitable adjustment in the delivery schedule or contract price, or both, and the contract shall be modified, in writing, accordingly, if-

(1) The stop-work order results in an increase in the time required for, or in the Contractor's cost properly allocable to, the performance of any part of this contract; and

(2) The Contractor asserts its right to the adjustment within 30 days after the end of the period of work stoppage; provided, that, if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon the claim submitted at any time before final payment under this contract.

(c) If a stop-work order is not canceled and the work covered by the order is terminated for the convenience of the Government, the Contracting Officer shall allow reasonable costs resulting from the stop-work order in arriving at the termination settlement.

(d) If a stop-work order is not canceled and the work covered by the order is terminated for default, the Contracting Officer shall allow, by equitable adjustment or otherwise, reasonable costs resulting from the stop-work order.

2.6 INSPECTION OF SERVICES

In accordance with FAR 52.212-4 CONTRACT TERMS AND CONDITIONS--COMMERCIAL ITEMS (MAR 2009) (DEVIATION I - FEB 2007) for Firm-Fixed Price orders and FAR 52.212-4 CONTRACT TERMS AND CONDITIONS COMMERCIAL ITEMS (MAR 2009) (ALTERNATE I OCT 2008) (DEVIATION I – FEB 2007) applies to Time-and-Materials and Labor-Hour Contracts orders placed under this contract.

2.7 RESPONSIBILITIES OF THE CONTRACTOR

The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character. If the end product of a task order is software, then FAR 52.227-14 (Dec 2007) Rights in Data – General, may apply.

2.8 RESPONSIBILITIES OF THE ORDERING ACTIVITY

Subject to security regulations, the ordering activity shall permit Contractor access to all facilities necessary to perform the requisite IT/IAM Professional Services.

2.9 INDEPENDENT CONTRACTOR

All IT/IAM Professional Services performed by the Contractor under the terms of this contract shall be as an independent Contractor, and not as an agent or employee of the ordering activity.

2.10 ORGANIZATIONAL CONFLICTS OF INTEREST

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.

2.11 INVOICES

The Contractor, upon completion of the work ordered, shall submit invoices for IT/IAM Professional 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.

2.12 PAYMENTS

For firm-fixed price orders the ordering activity shall pay the Contractor, upon submission of proper invoices or vouchers, the prices stipulated in this contract for service rendered and accepted. Progress payments shall be made only when authorized by the order. For time-and-materials orders, the Payments under Time-and-Materials and Labor-Hour Contracts at FAR 52.212-4 (MAR 2009) (ALTERNATE I – OCT 2008) (DEVIATION I – FEB 2007) applies to time-and-materials orders placed under this contract. For labor-hour orders, the Payment under Time-and-Materials and Labor-Hour Contracts at FAR 52.212-4 (MAR 2009) (ALTERNATE I – OCT 2008) (DEVIATION I – FEB 2007) applies to labor-hour orders placed under this contract. 52.216-31(Feb 2007) Time-and-Materials/Labor-Hour Proposal Requirements**—** Commercial Item Acquisition As prescribed in 16.601(e)(3), insert the following provision:

(a) The Government contemplates award of a Time-and-Materials or Labor-Hour type of contract resulting from this solicitation.

(b) The offeror must specify fixed hourly rates in its offer that include wages, overhead, general and administrative expenses, and profit. The offeror must specify whether the fixed hourly rate for each labor category applies to labor performed by—

(1) The offeror;

(2) Subcontractors; and/or

(3) Divisions, subsidiaries, or affiliates of the offeror under a common control.

2.13 RESUMES

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

2.14 INCIDENTAL SUPPORT COSTS

Incidental support costs are available outside the scope of this contract. The costs will be negotiated separately with the ordering activity in accordance with the guidelines set forth in the FAR.

2.15 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. Description of Information Technology (IT) Professional Services (SIN 54151S)

ProServices-1. Project Manager

Minimum/General Experience
Eight (8) years of demonstrated experience with five (5) years specialized experience in supervision and management of information systems projects involving fifty (50) or more people. Experienced with progressively difficult information systems management. Performs evaluation of current information system activities, plans and directs all phases of the work effort and ensures tasks are completed within negotiated time frames, budgets and technical specifications. Must be proficient in developing and presenting, both verbally and in writing, highly technical information and presentations to non-technical audiences at all levels of the organization.

Functional Responsibility
Demonstrated progressively difficult information systems management experience. Experienced in oral and written communications with all levels of management. Experience with multi-vendor environment.

Minimum Education
Bachelor's Degree in Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline. Substitutions of experience for education may be made when four years of specialized experience will be equivalent to a four-year degree.

ProServices-2. System Administrator

Minimum/General Experience
Three (3) or more years of progressively responsible experience on Windows/Linux/Unix server operations and maintenance. Two or more years of experience monitoring the operation of a system/network of servers, workstations, gateways, proxies, bridges and switches. Competent in the acquisition and management of communication hardware/software and operating and maintaining server and network related equipment. Running typical system backup, maintenance procedures, and providing assistance to internal stakeholders and end users. Operating environment: Solaris, UNIX, Linux, Windows Server 2003/2008/2012, Windows XP/7/8 and Windows based applications.

Functional Responsibility
Coordinates system/network requirements with users and sites. Optimizes network costs and performance, fault and security management. Provides technical leadership in the integration and testing of computer-integrated networks.

Minimum Education
Associate's Degree in Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline. Substitutions of experience for education may be made when two years of specialized experience will be equivalent to a two-year degree.

ProServices-3. Senior System Administrator

Minimum/General Experience
Six (6) or more years of progressively responsible experience on Windows/Linux/Unix server operations and maintenance. Three or more years of experience monitoring the operation of a system/network of servers, workstations, gateways, proxies, bridges and switches. Competent in the acquisition and management of communication hardware/software and operating and maintaining server and network related equipment. Responsible for advanced system administration tasks, running advanced system backup and recovery, and providing assistance to internal stakeholders and end users. Provides advanced level troubleshooting and analysis of system performance and on-going operations. Operating environment: Solaris, UNIX, Linux, Windows Server 2003/2008/2012, Windows XP/7/8 and Windows based applications.

Functional Responsibility
Coordinates advanced detailed system/network requirements with users and sites. Optimizes network costs and performance, fault and security management. Provides technical leadership in the integration and testing of computer-integrated networks.

Minimum Education
Associate's Degree in Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline. Substitutions of experience for education may be made when two years of specialized experience will be equivalent to a two-year degree.

ProServices-4. Database Administrator

Minimum/General Experience
Three (3) or more years experience with database management systems; knowledge of operating system commands in UNIX, Windows Server ecosystem; knowledge of SQL; Database normalization and RDBMS structures, commands and procedures.

Functional Responsibility
Assists in database operations, user connectivity to database, database security, backup and recovery, data integrity, database update and database reporting. Responsible for implementing data standards, designing and implementing security, and leading the effort to resolve data quality problems. Performs modeling of the data warehouse components, align the data warehouse information requirements with the data warehouse models, build and implement data and metadata into the data warehouse, and migrate data from the ODS to the data warehouse.

Minimum Education
Associate's Degree in Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline. Substitutions of experience for education may be made when two years of specialized experience will be equivalent to a two-year degree.

ProServices-5. Security Auditor

Minimum/General Experience
Three (3) or more years experience performing information and system security audits in accordance NIST, COBIT or ISO processes and standards. Thorough knowledge of vulnerability scanning tools (i.e., NESSUS, AppDetective, WebInspect and ISS). Knowledge of various operating platforms (i.e. UNIX, Solaris, Microsoft). Demonstrated familiarity with vulnerability management (POA&M) from creation to closure. Must be proficient in developing and presenting, both verbally and in writing, highly technical security information and presentations to non-technical audiences at all levels of the organization.

Functional Responsibility
Analyzes various types of systems and technologies and provides a gap analysis between security policies and existing configurations. Examines and evaluates information systems recommending controls to ensure system reliability and data integrity. Reviews and tests controls to ensure integrity and security of customer financial and operational data. Develops clear and concise audit/assessment and recommendation reports and be able to extract data from multiple data sources to produce real-time reports around audit results and metrics

Minimum Education
Bachelor's Degree in Information Systems Security, Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline. Substitutions of experience for education may be made when four years of specialized experience will be equivalent to a four-year degree.

ProServices-6. Programmer/Web Developer

Minimum/General Experience
Three (3) years of general experience within the software industry. Experience in design, programming and advanced programming languages. Possesses knowledge of computer equipment and the ability to develop software to satisfy design objectives. Requires competence in analysis and design of system applications. Possesses knowledge of system and database management concepts and the use of programming languages such as C, C++, Java, C#, PHP, Python, Ruby, FORTRAN or COBOL. Possesses knowledge of state-of-the-art software/database engineering methodologies, CASE tools, and design techniques, as well as applicable software/database standards.

Functional Responsibility
Develops block diagrams and logic flow charts. Translates detailed design into computer software. Supports testing, debugging and refining the computer software to produce the required product. Prepares program-level and user-level documentation. Enhances software to reduce operating time or improve efficiency.

Minimum Education
Associate's Degree in Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline. Substitutions of experience for education may be made when two years of specialized experience will be equivalent to a two-year degree.

ProServices-7. Senior Programmer/Web Developer

Minimum/General Experience
Six (6) years of general experience within the software industry. Experience in design, programming and advanced programming languages. Possesses knowledge of computer equipment and the ability to develop software to satisfy design objectives. Requires competence in analysis and design of system applications. Possesses knowledge of system and database management concepts and the use of programming languages such as C, C++, Java, C#, PHP, Python, Ruby, FORTRAN or COBOL. Possesses knowledge of state-of-the-art software/database engineering methodologies, CASE tools, and design techniques, as well as applicable software/database standards.

Functional Responsibility
Provides leadership for development of block diagrams and logic flow charts. Translates detailed design into computer software requirements. Supports testing, quality assurance oversight, debugging and refining the computer software to produce the required product. Prepares program-level and user-level documentation. Enhances software to reduce operating time or improve efficiency.

Minimum Education
Bachelor's Degree in Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline. Substitutions of experience for education may be made when four years of specialized experience will be equivalent to a four-year degree.

ProServices-8. Configuration Management Specialist

Minimum/General Experience
Three (3) or more years experience in general standards, concepts, practice and techniques related to the Configuration Management functions in order to accomplish assignments. Understanding of specific job requirements with requisite skills to perform assigned Configuration Management tasks with minimal supervision.

Functional Responsibility
Controls change and maintenance of the integrity of the project's artifacts. Identifies configuration items, restricts changes to those items, audits changes made to those items, and defines and manages configuration of those items throughout the software development or network design and support process. Uses applicable Configuration Management software to trace defects, requirements, specifications and

test cases. Creates builds and manages Development, QA or Production environments. Ensures that right versions of configuration items are selected for change or implementation. Enforcement of object check-in/check-out procedures.

Minimum Education
Associate's Degree in Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline. Substitutions of experience for education may be made when two years of specialized experience will be equivalent to a two-year degree.

ProServices-9. Quality Assurance Analyst

Minimum/General Experience
Four (4) or more years specialized experience in quality assurance concepts. Experience in analysis and design of business applications on complex systems, database management, use of programming languages, and/or RDBMS. Understanding and application of government documentation standards. Knowledge of current storage and retrieval methods and demonstrated ability to formulate specifications for computer programmers to use in coding, testing, and debugging of computer programs.

Functional Responsibility
Provides technical and administrative direction for personnel performing software development tasks, reviews products for correctness, adherence to the design concept and user standards, reviews program documentation to assure customer standards/requirements are adhered to, and for progress in accordance with schedules.

Minimum Education
Bachelor's Degree in Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline. Substitutions of experience for education may be made when four years of specialized experience will be equivalent to a four-year degree.

ProServices-10. Help Desk Support Professional

Minimum/General Experience
One (1) or more years experience operating a PC-based Help Desk, Call Center. One or more years experience working with Microsoft Office, Windows XP, 7, 8, Windows Server or comparable platforms and products. Experience with personnel computer communication products including network protocols and Internet browsers.

Functional Responsibility
Responds to telephone, faxed and email request for assistance

Minimum Education
Associate's Degree in Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline. Substitutions of experience for education may be made when two years of specialized experience will be equivalent to a two-year degree.

ProServices-11. SharePoint Farm Engineer

Minimum/General Experience
Four (4) or more years experience providing Microsoft SharePoint Farm engineering and administration support services. Experience performing SharePoint farm installation, patching and version upgrades. General experience with SharePoint native and related technology components (e.g. Microsoft Windows operating system, Active Directory, ADFS and SQL Server database application). Must be proficient in developing and presenting, both verbally and in writing, highly technical information and presentations to non-technical audiences at all levels of the organization.

Functional Responsibility
Adds/changes SharePoint infrastructure or features, troubleshoots errors, installs Microsoft SharePoint application update and security patches, performs restores of more than documents/files/pages (i.e. restoring a whole site), manages all settings in 'Central Admin' back-end interface including: 1) farm-wide search settings and search scope (adding URLs to search index); 2) adding web applications (new SharePoint URLs/hostnames); and 3) configures/changes authentication settings. Plans SharePoint backup and recovery strategy in accordance with recovery time and recovery point objectives.

Minimum Education
Bachelor's Degree in Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline. Substitutions of experience for education may be made when four years of specialized experience will be equivalent to a four-year degree.

ProServices-12. SharePoint Support Specialist

Minimum/General Experience
Two (2) or more years experience providing Microsoft SharePoint administration support services. Experience providing assistance in planning SharePoint farm installation, patching and version upgrades. General experience with SharePoint native and related technology components (e.g. Microsoft Windows operating system, Active Directory, ADFS and SQL Server database application).

Functional Responsibility
Performs all support actions that can be performed from the SharePoint Site Collection Administrator front-end interface such as creating new site collections, sites, sub sites, creating libraries, lists of other content areas, groups or permissions, bulk uploading of files, restoring items caught by the SharePoint recycle bin, installation of custom services, changes to individual web-app settings. Deployment of WSP and other requested changes between the environments (e.g. test to production). Assists in troubleshooting SharePoint Web Application issues. Performs SharePoint backups and tests recovery assuring compliance with recovery time and recovery point objectives.

Minimum Education
Associate's Degree in Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline. Substitutions of experience for education may be made when two years of specialized experience will be equivalent to a two-year degree.

ProServices-13. Business Analyst

Minimum/General Experience
Four (4) or more years specialized experience in process and functional analysis experience in the Information Technology field. Must possess superior process and functional knowledge of task order specific requirements and have experience in developing and analyzing process requirements for enterprise-wide information technology systems. Must be proficient in developing and presenting, both verbally and in writing, highly technical information and presentations to non-technical audiences at all levels of the organization.

Functional Responsibility
Analyzes and provides user needs to determine process and functional requirements as related to Information Technology. Performs process analysis and resource allocation to identify required tasks and their interrelationships. Identifies resources required for each task. Provides daily Information Technology process support and direction to customer executive staff. Analyzes Federal, State and Local Government Information Technology process requirements and makes enterprise level recommendations to key stake holders as required.

Minimum Education

Bachelor's Degree in Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline. Substitutions of experience for education may be made when four years of specialized experience will be equivalent to a four-year degree.

ProServices-14. Technical Writer

Minimum/General Experience
Three (3) or more years of demonstrated experience in editing administrative, configuration and technical documents. Experienced in collecting and organizing information required for preparation of user's manuals, training materials, installation guides, proposals, and other reports and deliverables. Demonstrated ability to work independently or under general direction.

Functional Responsibility
Prepares and edits system specifications, functional descriptions, special reports, user's manuals, configuration management documentation, and any other customer deliverables. Assists in preparation of user's manuals, training materials, installation guides, proposals, and reports. Documents system troubleshooting/installation procedures.

Minimum Education
Bachelor's Degree in English, Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline. Substitutions of experience for education may be made when four years of specialized experience will be equivalent to a four-year degree.

ProServices-15. Subject Matter Expert - Information Technology

Minimum/General Experience
Eight (8) years or more of progressive experience in the individual's field of study and specialization. Experienced in subject matter closely related to the work to be performed according to user specifications. Provides Expert advice, direction, guidance and insight into specific technologies and performs a variety of tasks where a specific subject matter expertise is necessary. Must be proficient in developing and presenting, both verbally and in writing, highly technical information and presentations to non-technical audiences at all levels of the organization.

Functional Responsibility
Provides high-level functional and subject matter analysis, design, integration, documentation and implementation problem solving and assistance which require a thorough knowledge of the related technical subject matter. Responsible for highly complex technical/engineering areas. Participates in all phases of project development. Designs and prepares complex technical reports and related documentation. Applies subject matter knowledge to high-level analysis, collection, assessment, design, development, modeling, simulation, integration, installation, documentation, and implementation. Resolves problems, which necessitates an intimate knowledge of the related technical subject matter.

Minimum Education
Bachelor's Degree in Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline. Substitutions of experience for education may be made when four years of specialized experience will be equivalent to a four-year degree.

ProServices-16. Subject Matter Expert - Information Security

Minimum/General Experience
Eight (8) or more years experience, of which 8 years must be specialized experience including INFOSEC technology, policy and procedure development and implementation on major industry and Government programs. Solid understanding of security policy advocated by the U.S. Federal, State and Local Government and appropriate civil agencies. Experienced in development of common user and special purpose information systems information security. Must be proficient in developing and presenting, both

verbally and in writing, highly technical information and presentations to non-technical audiences at all levels of the organization.

Functional Responsibility
Establishes and provides system-wide information security requirements based upon the analysis of user, policy, regulatory, and resource demands. Supports customers at the highest levels in the development and implementation of doctrine and policies. Provides leadership and guidance in the development, design and application of solutions implemented by more junior staff members. Applies expertise to common user information systems, as well as to dedicated special purpose systems requiring specialized security features and procedures. Applies subject matter knowledge to high-level analysis, collection, assessment, design, development, modeling, simulation, integration, installation, documentation, and implementation. Resolves problems, which necessitates an intimate knowledge of the related technical subject matter.

Minimum Education
Bachelor's Degree in Information Systems Security, Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline. Substitutions of experience for education may be made when four years of specialized experience will be equivalent to a four-year degree.

ProServices-17. Network Engineer

Minimum/General Experience
Four (4) years of technical experience which applies to analysis, design, and resolving complex network problems. Demonstrated experience with TCP/IP services, security, Ethernet, frame relay and LAN/WAN technology. Configure, tests and install infrastructure, services, desktop, and security technologies. Interfaces with users, assist users in system documentation and software support for information systems. Experience with routers/switches and related protocols and hubs.

Functional Responsibility
Interfaces with users. Assist users in system documentation and software support for information systems. Prepares test date for the information systems. Reviews work and installation progress for accuracy.

Minimum Education
Associate's Degree in Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline. Substitutions of experience for education may be made when two years of specialized experience will be equivalent to a two-year degree.

ProServices-18. Senior Network Engineer

Minimum/General Experience
Four (4) or more years of experience with LAN/WAN. Demonstrated experience with TCP/IP services, security, planning and enterprise databases. Installs, configures, implements and supports network infrastructure. Analyzes and evaluates network performance. Operating environment, DOS, UNIX, Windows Server, Windows XP/7/8 and Windows based applications, Ethernet, frame relay, routers/switches, and LAN/WAN technology. Experience with routers/switches and related protocols and hubs.

Functional Responsibility
Supervises and provides technical direction to lower level engineers. Reviews work and installation progress for accuracy, adherence to network design, and conformance to telecommunications standards. Evaluates equipment, network, and/or applications technologies and makes recommendations.

Minimum Education

Bachelor's Degree in Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline. Substitutions of experience for education may be made when four years of specialized experience will be equivalent to a four-year degree.

ProServices-19. Training Specialist

Minimum/General Experience
Two (2) or more years of experience developing and teaching training modules in complex and specialized areas. Experience in adhering to strict deadlines, moderate workloads and on-demand user service.

Functional Responsibility
Organize and conduct complex training and other educational programs for information systems, software and end user personnel. Maintain complete records of training activities, detailed user progress and overall program effectiveness. Competent in all phases of training.

Minimum Education
Associate's Degree in Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline. Substitutions of experience for education may be made when two years of specialized experience will be equivalent to a two-year degree.

ProServices-20. Systems Analyst

Minimum/General Experience
Five (5) years of technical experience analyzing, planning and supporting the design of computer systems. Analyzes and defines problems, develops network requirements and specifications. Evaluates existing information systems and recommends changes to them as they relate to networking. Confers with functional managers to determine requirements, and recommends alternative solutions. Computer Operating Systems: DOS, UNIX, Linux, Windows Server and Windows XP/7/8.

Functional Responsibility
Analyzes user interfaces, workload and computer usage, outside system interfaces, downtime, system modifications, upgrades, and information to be processed. Defines problems and develops system requirements.

Minimum Education
Associate's Degree in Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline. Substitutions of experience for education may be made when two years of specialized experience will be equivalent to a two-year degree.

ProServices-22. Professional Services - Disaster Recovery (As Defined by SOW)

Minimum/General Experience
Five (5) or more years experience in information technology system disaster recovery, planning and testing. Requires advanced knowledge of enterprise information technology architecture and applicable disaster recovery methodology and guidance. Must be proficient in developing and presenting, both verbally and in writing, highly technical information and presentations to non-technical audiences at all levels of the organization.

Functional Responsibility
Provides strategic support in the development of contingency, disaster recovery and business continuity planning. Reviews and develops integrated network and system related recovery strategies and documentation. Drafts disaster recovery policies and procedures. Communicates with disaster recovery team members during recovery test exercises and actual recovery events.

Minimum Education

Bachelor's Degree in Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline. Substitutions of experience for education may be made when four years of specialized experience will be equivalent to a four-year degree.

ProServices-23. Professional Services - Hosting (As Defined by SOW)

Minimum/General Experience
Five (5) or more years experience in information technology hosted system management, operations, disaster recovery planning, performance optimization, high availability and system troubleshooting. Requires advanced knowledge of hosted enterprise information technology architecture and applicable operational methodology.

Functional Responsibility
Provides strategic support in all aspects of hosted enterprise system infrastructure support including routers, switches, servers, SANs, virtualization, load balancing, monitoring, operational and security support infrastructure, operating system maintenance, anti-virus/malware operations and specific application related support.

Minimum Education
Bachelor's Degree in Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline. Substitutions of experience for education may be made when four years of specialized experience will be equivalent to a four-year degree.

ProServices-24. Professional Services - Incident Response (As Defined by SOW)

Minimum/General Experience
Four (4) or more years in demonstrated experience and aptitude with network architecture and design. Familiarity and knowledge of IT Security technologies to include but not limited to: host based intrusion detection, network based intrusion detection, firewalls, wireless intrusion detection, VPN, proxy servers, and anti-virus. Ability to perform triage on multiple incidents and prioritize as necessary.

Functional Responsibility
Provides strategic support in all aspects of incident response processes. Provides support to incident response planning, testing and execution. Serves as the initial point of contact for reported/suspected information technology security incidents. Orchestrates incident investigations among multiple external (i.e. external agencies) and internal stakeholders.
Tracks multiple incident reports from external organizations and responds with status.

Minimum Education
Bachelor's Degree in Information System Security, Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline. Substitutions of experience for education may be made when four years of specialized experience will be equivalent to a four-year degree.

ProServices-25. Professional Services - Security Compliance (As Defined by SOW)

Minimum/General Experience
Four (4) or more years in demonstrated experience and aptitude supporting Security Operations Center (SOC) in security compliance, vulnerability management, incident response assistance and all aspects of security compliance objectives. Familiar with information technology and data security compliance and risk mitigation strategies utilized in cyber security operations.

Functional Responsibility
Provides strategic support in all aspects of security compliance processes. Provides support of compliance management processes including system even log monitoring, vulnerability scanning, penetration testing, vulnerability report assessment, vulnerability remediation and transfer of remaining findings to Plan of

Actions and Milestones (POAM) report. Ensures the integrity of applicable operational, technical and management security controls in accordance with the established control baseline. Generates security documentation in accordance with applicable FISMA, NIST, OPM, FIPS and agency specific guidance. Provides support in all aspects of continuous monitoring process planning, operations and improvements.

Minimum Education
Bachelor's Degree in Information System Security, Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline. Substitutions of experience for education may be made when four years of specialized experience will be equivalent to a four-year degree.

ProServices-26. Professional Services - Custom System Administration (As Defined by SOW)

Minimum/General Experience
Four (4) or more years in demonstrated experience performing system administration support services. Must have familiarity with a wide range of enterprise technologies involved in routing, switching, high-availability, system integration, deployment methodology as well as system operational service excellence that results in improved customer satisfaction.

Functional Responsibility
Provides strategic support in all aspects of system management including infrastructure monitoring operations, helpdesk support operations, operating system management, middleware system management, Secure Socket Layer (SSL) management, SFTP management, encrypted remove connectivity management, 2-factor authentication management, Active Directory group policy management, load balancing, and patch management. Performs system hardening in accordance with government-wide and agency specific tailoring guidance. Responsible for oversight of system technology lifecycle, timely repair and issue resolution to ensure high performance and availability of information systems.

Minimum Education
Bachelor's Degree in Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline. Substitutions of experience for education may be made when four years of specialized experience will be equivalent to a four-year degree.

ProServices-27. Professional Services - Application Administration (As Defined by SOW)

Minimum/General Experience
Four (4) or more years in demonstrated experience performing application administration support services. Must have familiarity with a wide range of modern web application technologies (e.g. Microsoft, Oracle, Sun, Drupal, and other open source PHP, Java or .Net custom applications). Experienced in application installation, troubleshooting, security compliance, configuration management, upgrade cycle, on-going operations, optimization, disaster recovery, backup and decommission.

Functional Responsibility
Provides support in all aspects of application management lifecycle in accordance with defined requirements and objectives. Responsible for application installation planning and decommissioning, end user authentication setup, log setup, issue identification and subsequent troubleshooting, application hardening and SSL certificate installation, configuration management baseline establishment and updates, monthly and out of band application and security patching, application specific backup support, application performance optimization, and all aspects of application specific disaster recovery considerations and documentation detail.

Minimum Education
Bachelor's Degree in Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline. Substitutions of experience for education may be made when four years of specialized experience will be equivalent to a four-year degree.

4. IT Professional Services Pricing (SIN 54151S)

See Table 1 – 54151S IT Professional Servies Pricing.

Continued On The Next Page

TABLE 1 – SIN 54151S - IT PROFESSIONAL SERVICES PRICING

Item	Labor Category	GSA On-Site Rate	GSA Off-Site Rate
ProServices - 1	Project Manager	$126.05	$170.48
ProServices - 2	System Administrator	$78.89	$106.10
ProServices - 3	Senior System Administrator	$87.05	$116.98
ProServices - 4	Database Administrator	$88.87	$119.70
ProServices - 5	Security Auditor	$156.88	$211.28
ProServices - 6	Programmer/Web Developer	$74.36	$99.75
ProServices - 7	Senior Programmer/Web Developer	$88.87	$119.70
ProServices - 8	Configuration Management Specialist	$87.05	$116.98
ProServices - 9	Quality Assurance Analyst	$68.92	$92.49
ProServices - 10	Help Desk Support Professional	$49.87	$67.10
ProServices - 11	SharePoint Farm Engineer	$126.05	$170.48
ProServices - 12	SharePoint Support Specialist	$90.23	$122.42
ProServices - 13	Business Analyst	$78.89	$106.10
ProServices - 14	Technical Writer	$72.54	$97.93
ProServices - 15	Subject Matter Expert - Information Technology	$246.65	$333.70
ProServices - 16	Subject Matter Expert - Information Security	$287.46	$388.11
ProServices - 17	Network Engineer	$72.54	$97.93
ProServices - 18	Senior Network Engineer	$96.12	$129.67
ProServices - 19	Training Specialist	$86.15	$116.07
ProServices - 20	Systems Analyst	$72.54	$97.93
ProServices - 22	Professional Servces - Disaster Recovery (As defined by SOW)	-	$153.25
ProServices - 23	Professional Servces - Hosting (As defined by SOW)	-	$169.57
ProServices - 24	Professional Services - Incident Response (As defined by SOW)	-	$186.80
ProServices - 25	Professional Servides - Security Compliance (As defined by SOW)	-	$166.85
ProServices - 26	Professional Services - Custom System Administration (As defined by SOW)	-	$186.80
ProServices - 27	Professional Services - Application Administration (As defined by SOW)	-	$166.85

On-Site Rate - Government site hourly rate
Off-Site Rate - IT-CNP, Inc. (Contractor) site hourly rate
SOW - Customer's Statement of Work
All rates include GSA IFF fees

5. Terms And Conditions Applicable To Electronic Commerce And Subscription Services (SIN 54151ECOM)

5.1 SCOPE

a. The prices, terms and conditions stated under 54151ECOM Electronic Commerce (EC) Services category apply exclusively to EC Services within the scope of this Information Technology Schedule.

b. The Contractor shall provie services at the Contractor's facility and/or at the ordering activity location, as agreed to by the Contractor and the ordering activity.

5.2 ELECTRONIC COMMERCE CAPACITY AND COVERAGE

The Ordering Activity shall specify the capacity and coverage required as part of the initial requirement.

5.3 INFORMATION ASSURANCE

a. 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)

b. The Ordering Activity shall assign an impact level (per Federal Information Processing Standards Publication 199 & 200 (FIPS 199, *"Standards for Security Categorization of Federal Information and Information Systems"*) (FIPS 200, "*Minimum Security Requirements for Federal Information and Information Systems*") prior to issuing the initial statement of work. Evaluations shall consider the extent to which each proposed service accommodates the necessary security controls based upon the assigned impact level. The Contractor awarded 54151ECOM is capable of meeting at least the minimum security requirements assigned against a low-impact information system (per FIPS 200).

c. The Ordering Activity reserves the right to independently evaluate, audit, and verify the FISMA compliance for any proposed or awarded Electronic Commerce services. All FISMA certification, accreditation, and evaluation activities are the responsibility of the ordering activity.

5.4 DELIVERY SCHEDULE

Delivery schedule shall be specified by the ordering activity as part of the initial requirement.

5.5 INTEROPERABILITY

When an Ordering Activity requires interoperability, this requirement shall be included as part of the initial requirement. Interfaces may be identified as interoperable on the basis of participation in a sponsored program acceptable to the Ordering Activity. Any such access or interoperability with teleports/gateways and provisioning of enterprise service access will be defined in the individual requirement.

5.6 ORDER

a. Agencies may use written orders, EDI orders, blanket purchase agreements, individual purchase orders, or task orders for ordering electronic services under this contract. Blanket Purchase Agreements shall not extend beyond the end of the contract period; all electronic 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.

c. The ordering acrtivity should include criteria for satisfactory completion for each task in the requirement.

5.7 PERFORMANCE OF SERVICES

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

5.8 RESPONSIBILITIES OF THE CONTRACTOR

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

5.9 RESPONSIBILITIES OF THE ORDERING ACTIVITY

a. Issue a requirements document (Statement of Work or Delivery/TaskOrder) that contains technical requirements, performance requirements, delivery schedule, applicable compliance requirements and any additonal requirements or constraints necessary.

b. Permit the Contractor access to all facilities necessary to perform the requisite work, subject to applicable security regulations.

5.10 RIGHTS IN DATA

The Contractor shall comply FAR 52.227-14 RIGHTS IN DATA – GENERAL and with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character.

5.11 INDEPENDENT CONTRACTOR

All services performed by the Contractor under the terms of this contract shal lbe as an independant Contractor, and not as an agent or employee of the ordering activity.

5.12 INVOICES

The Contractor, upon completion of the work ordered, shall submit invoices for IT/IAM Professional 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.

5.13 PAYMENTS

For firm-fixed price orders the ordering activity shall pay the Contractor, upon submission of proper invoices or vouchers, the prices stipulated in this contract for service rendered and accepted. Progress payments shall be made only when authorized by the order. For time-and-materials orders, the Payments under Time-and-Materials and Labor-Hour Contracts at FAR 52.212-4 (MAR 2009) (ALTERNATE I – OCT 2008) (DEVIATION I – FEB 2007) applies to time-and-materials orders placed under this contract. For labor-hour orders, the Payment under Time-and-Materials and Labor-Hour Contracts at FAR 52.212-4 (MAR 2009) (ALTERNATE I – OCT 2008) (DEVIATION I – FEB 2007) applies to labor-hour orders placed under this contract. 52.216-31(Feb 2007) Time-and-Materials/Labor-Hour Proposal Requirements—Commercial Item Acquisition As prescribed in 16.601(e)(3), insert the following provision:

1. The Government contemplates award of a Time-and-Materials or Labor-Hour type of contract resulting from this solicitation.
2. The offeror must specify fixed hourly rates in its offer that include wages, overhead, general and administrative expenses, and profit. The offeror must specify whether the fixed hourly rate for each labor category applies to labor performed by—
    (i) The offeror;
    (ii) Subcontractors; and/or
    (iii) Divisions, subsidiaries, or affiliates of the offeror under a common control.

5.14 INCIDENTAL SUPPORT COSTS

Incidental support costs are available outside the scope of this contract. The costs will be negotiated separately with the ordering activity in accordance with the guidelines set forth in the FAR.

5.15 GSA MULTIPLE AWARD SCHEDULE SUPPLEMENTAL WEB HOSTING TERMS OF USE AGREEMENT

The ordering activity (Customer) agrees to abide by the following Standard Service Terms Of Use:

This GSA Multiple Award Schedule Supplemental Web Hosting Terms Of Use Agreement ("Agreement) is made by and between IT-CNP, Inc. (“IT-CNP”) and organizations eligible to place orders against IT-CNP's GSA Multiple Award Schedule contract to purchase web hosting and related IT professional services (“Customer”). This Agreement is effective as of the date referenced in each customer's individual task order (“Effective Date”).

1. SERVICE LEVELS. IT-CNP will provide the Services in accordance with the Service Level Agreement attached hereto as Exhibit A.

2. LICENSE GRANT. Subject to this Agreement, terms and conditions, IT-CNP hereby grants to Customer, (and to each Customer employee or authorized contractor who accesses the Services by means of Customer's account and an authorized password), subject to all of the terms and conditions, a non-exclusive, non-transferable, non-sublicensable license to access and use the Services via the Internet, solely for intended business purposes in accordance with any applicable end user documentation.

3. LICENSE RESTRICTIONS. Customer shall not, directly or indirectly, (i) reverse engineer, decompile, disassemble or otherwise attempt to discover the source code or underlying ideas or algorithms of the Services; (ii) modify, translate, or create derivative works based on the Services; (iii) rent, lease, distribute, sell, resell, assign, or otherwise transfer rights to the Services; (iv) use the Services for timesharing or service bureau purposes or otherwise for the benefit of a third party; (v) remove any proprietary notices from the Services; (vi) publish or disclose to third parties any evaluation of the Services without IT-CNP 's prior written consent.

4. PASSWORDS/SECURITY.

4.1 Passwords. IT-CNP may issue to Customer, or shall authorize a Customer administrator to issue, infrastructure access password for users authorized to use Customer's account. Customer and its users are responsible for maintaining the confidentiality of all passwords and for ensuring that each password is used only by the authorized user. Customer is entirely responsible for any and all activities that occur under the Customer's account and all charges incurred from use of the Services accessed with the Customer’s

passwords. Customer agrees to immediately notify IT-CNP of any unauthorized use of the Customer's account (including each password of each user accessing the Services by means of Customer's account) or any other breach of security known to Customer. IT-CNP shall have no liability for any loss or damage arising from Customer's failure to comply with these requirements.

4.2 Security. IT-CNP will implement commercially reasonable security precautions and industry's best practices to prevent unauthorized access to the Customer Data (as defined below). Customer acknowledges that, notwithstanding such security precautions, use of or connection to the Internet provides the opportunity for unauthorized third parties to circumvent such precautions and illegally gain access to the Services and Customer Data. Accordingly, IT-CNP cannot and does not guaranty the privacy, security or authenticity of any information so transmitted over or stored in any system connected to the Internet.

5. CUSTOMER DATA. As between IT-CNP and Customer, Customer shall own all data, information or material that Customer enters into the Services or has entered on its behalf ("Customer Data"). IT-CNP's authorized personnel may access Customer's account and Customer Data from time to time, as IT-CNP deems necessary, solely for purposes of information security monitoring, management and audit, technical support, administration and invoicing related to Customer's use of the Services. Except as permitted, IT-CNP will not edit, delete or disclose the contents of Customer Data unless authorized by the Customer or unless IT-CNP is required to do so by law or in the good faith belief that such action is necessary to: (1) conform with applicable laws or comply with legal process served on IT-CNP; (2) protect and defend the rights or property of IT-CNP; or (3) enforce these terms of use. Customer is solely responsible for the accuracy, quality, integrity, legality, reliability, appropriateness and copyright of all Customer Data and IT-CNP assumes no responsibility for the deletion, correction, destruction, loss, infringement or failure of the Services to store any Customer Data. IT-CNP reserves the right to establish a maximum amount of memory, storage, computing resources or maximum amount of Customer Data that Customer may store, post or transmit on or through the Services.

6. CUSTOMER OBLIGATIONS.

6.1 Conduct. Customer shall be solely responsible for its actions and the actions of its users while using the Services and the contents of its transmissions through the Services (including, without limitation, Customer Data). Customer agrees: (1) to abide by all local, state, national, and international laws and regulations applicable to Customer's use of the Services, including without limitation all laws regarding the transmission of technical data exported from the United States through the Services; (2) abide by all terms of applicable software licensing agreements used in conjunction with Services (3) not to intentionally or deliberately upload or distribute in any way files that contain viruses, corrupted files, or any other similar software or programs that may damage the operation of the Services or another's computer; (4) not to use the Services for illegal purposes; (5) not to interfere or disrupt networks connected to the Services; (6) not to post, promote or transmit through the Services any unlawful, harassing, libelous, abusive, threatening, harmful, vulgar, obscene, hateful, racially, ethnically or otherwise objectionable material of any kind or nature; (7) not to transmit or post any material that encourages conduct that could constitute a criminal offense or give rise to civil liability; (8) not to interfere with another customer's use and enjoyment of the Services or another entity's use and enjoyment of similar services; (9) not to intentionally or deliberately engage in contests, chain letters or post or transmit "junk mail," "spam," "chain letters," or unsolicited mass distribution of email; (10) not to install any unauthorized software including but not limited to network traffic sniffers/scanners, network monitoring or vulnerability scanners, network/server intrusion/penetration related software or any other software that may result in unauthorized capture or disclosure of traffic information or datacenter network components; and (11) to comply with all regulations, policies and procedures of networks connected to the Services. Customer acknowledges and agrees that IT-CNP neither endorses the contents of any customer communications or Customer Data nor assumes any responsibility for any threatening, libelous, obscene, harassing or offensive material contained therein, any infringement of third party intellectual property rights arising therefrom or any crime facilitated thereby. IT-CNP may remove any violating content posted on the Services or transmitted through the Services, without notice to Customer.

6.2 External Links/Resources. IT-CNP shall have no liability, obligation or responsibility whatsoever arising out of or in connection with any external website content, links to other web sites or resources. Customer acknowledges and agrees that IT-CNP is not responsible for the availability of such external sites or resources, and does not endorse and is not responsible or liable for any content, advertising, products, services or other materials on or available from such sites or resources. IT-CNP shall not be responsible or liable, directly or indirectly, to Customer or to any third party for any damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such content, goods or services available on such external sites or resources.

7. FEES AND TAXES.

7.1 Fees. Fees should be addressed in the schedule contract (price list) and negotiated at the task order level. Prices referenced in the price list include taxes and duties.

7.2 Payments. Payments terms are addressed in the schedule contract and negotiated at the task order level.

8. TERM. The contract duration should be stated in the task order. Termination will be effective at the end of the applicable term in which such notice is received. Customer shall be responsible for all Fees for the applicable term in which termination occurs, and IT-CNP shall not issue any refunds for such term.

9. TERMINATION.

9.1 Termination. Termination/cancellation terms are governed by the schedule contract and Federal Acquisition Regulations (FAR).

9.2 Effect of Termination. Upon the effective date of expiration or termination of service for any reason, whether by Customer or IT-CNP, Customer's right to use the Services shall immediately cease. Sections 5, 6, 9, 10, 11, 12, 13 and 14 of this Agreement shall survive its expiration or termination for any reason. IT-CNP shall retain Customer Data for a period of thirty (30) days after expiration or termination of service. Customer may request that IT-CNP conduct an export of Customer Data, and IT-CNP agrees to provide such services on a time and materials basis pursuant to a separate agreement. After thirty (30) days, IT-CNP may delete and destroy all Customer Data without notice or further liability to Customer.

10. PROPRIETARY RIGHTS. Customer acknowledges that the Services and all IT-CNP owned content contained therein where applicable, including but not limited to text, software, music, sound, photographs, video, graphics, and third party materials, excluding any Customer Data, (collectively, "Content") is proprietary to IT-CNP or such third parties, and IT-CNP or such third parties retain exclusive ownership of the same throughout the world, including all related copyrights, trademarks, service marks, patents, trade secrets or other proprietary rights thereto. Except as expressly stated herein, this Agreement do not transfer any right, title or interest in the Services or the Content to the Customer.

11. CONFIDENTIALITY.

11.1 Obligations. Each of the parties agrees to maintain in confidence any non-public information of the other party, whether written or otherwise, disclosed by the other party in the course of performance of this Agreement that a party knows or reasonably should know is considered confidential by the disclosing party ('Confidential Information'). The receiving party shall not disclose, use, transmit, inform or make available to any entity, person or body any of the Confidential Information, except as a necessary part of performing its obligations hereunder, and shall take all such actions as are reasonably necessary and appropriate to preserve and protect the Confidential Information and the parties' respective rights therein, at all times exercising at least a reasonable level of care. Each party agrees to restrict access to the Confidential Information of the other party to those employees or agents who require access in order to perform hereunder, and, except as otherwise provided, neither party shall make Confidential Information available to any other person or entity without the prior written consent of the other party.

11.2 Exclusions. Confidential Information shall not include any information that is (i) already known to the receiving party at the time of the disclosure; (ii) publicly known at the time of the disclosure or becomes publicly known through no wrongful act or failure of the receiving party; (iii) subsequently disclosed to the receiving party on a non-confidential basis by a third party not having a confidential relationship with the other party hereto that rightfully acquired such information; or (iv) communicated to a third party by the receiving party with the express written consent of the other party hereto. A disclosure of Confidential Information that is legally compelled to be disclosed pursuant to Freedom of Information Act (FOIA), subpoena, summons, order or other judicial or governmental process shall not be considered a breach of this Agreement; provided the receiving party provides prompt notice of any such subpoena, order, or the like to the other party so that such party will have the opportunity to obtain a protective order or otherwise oppose the disclosure.

11.3 Destruction or Return of Confidential Information. Upon expiration or termination of service for any reason, each party shall promptly return to the other party, or destroy, as the parties agree, all copies of the other party's Confidential Information. All copies, notes or other derivative material relating to the Confidential Information shall be promptly retrieved or destroyed, as agreed, and no such material shall be retained or used by the receiving party in any form or for any reason.

12. LIMITED WARRANTY AND WARRANTY DISCLAIMER.

12.1 Limited Warranty. IT-CNP warrants that the Services will perform substantially in accordance with the functions described in the documentation provided by IT-CNP under normal use and circumstances by authorized users of the Services.

12.2 Disclaimer. EXCEPT AS EXPRESSLY STATED IN SECTION 13.1, THERE ARE NO WARRANTIES OR CONDITIONS (WHETHER IMPLIED OR ARISING BY STATUTE OR OTHERWISE IN LAW OR FROM A COURSE OF DEALING OR USAGE OF TRADE) FOR THE SERVICES OR SUPPORT. IT-CNP DISCLAIMS ALL STATUTORY OR IMPLIED WARRANTIES AND CONDITIONS. IT-CNP DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SERVICES WILL MEET THE CUSTOMER'S REQUIREMENTS OR THAT THE OPERATION OF THE SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE. FURTHER, IT-CNP DOES NOT WARRANT THAT ALL ERRORS IN THE SERVICES CAN OR WILL BE CORRECTED. CUSTOMER UNDERSTANDS AND AGREES THAT ANY MATERIAL OR DATA DOWNLOADED OR OTHERWISE OBTAINED THROUGH THE SERVICES IS DONE AT CUSTOMER'S OWN DISCRETION AND RISK, AND THAT CUSTOMER WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO CUSTOMER'S COMPUTER SYSTEM OR LOSS OF DATA THAT RESULTS FROM THE DOWNLOAD OR USE OF SUCH MATERIAL OR DATA. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, SO SOME OF THE ABOVE EXCLUSIONS MAY NOT APPLY TO CUSTOMER.

13. LIMITATION OF LIABILITY.

13.1 Limitation on Direct Damages. IN NO EVENT SHALL IT-CNP'S AGGREGATE LIABILITY, IF ANY, ARISING OUT OF OR IN ANY WAY RELATED TO THIS DOCUMENT EXCEED THE FEES PAID BY CUSTOMER IN THE MONTHLY TERM IN WHICH THE ACTION AROSE, FOR THE SERVICES THAT DIRECTLY GAVE RISE TO THE DAMAGES CLAIMED, WITHOUT REGARD TO WHETHER SUCH CLAIM IS BASED IN CONTRACT OR TORT, INCLUDING NEGLIGENCE.

13.2 Disclaimer of Consequential Damages. IN NO EVENT SHALL IT-CNP OR ITS SUPPLIERS BE LIABLE (A) FOR ANY INDIRECT, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR (B) TO THIRD PARTIES CLAIMING THROUGH CUSTOMER; EVEN IF IT-CNP HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

13.3 Essential Purpose. The essential purpose of this Section 13 is to limit the potential liability of the parties arising under this document. The parties acknowledge that the limitations set forth in this Section 13 are intricate to the amount of consideration levied in connection with the license of the Services and that, were IT-CNP to assume any further liability, such consideration would out of necessity, been set much higher. This Section 13, Limitation of Liability, shall not impair the U.S. Government's right to recover for fraud or crimes arising out of or related to this Agreement under any federal fraud statute. Furthermore, this clause shall not impair nor prejudice the U.S. Government's right to express remedies provided in the schedule contract (i.e. Price Reductions, Patent Indemnification, Liability for Injury or Damage, Price Adjustment, Failure to Provide Accurate Information.)

14. GENERAL. All notices to a party shall be in writing and sent to the addresses specified and shall be deemed to have been duly given when received, if personally delivered; when receipt is electronically confirmed, if transmitted by facsimile or email; the day after it is sent, if sent for next day delivery by recognized overnight delivery service; and upon receipt, if sent by certified or registered mail, return receipt requested. Neither Service nor any Services license may be assigned or transferred by Customer, by merger, operation of law or otherwise, without IT-CNP' prior written consent. The terms of the schedule and the task order would take precedence over the terms of this agreement. This document may be amended or superseded only by a written instrument signed by both parties. This document shall be governed by the federal laws of the United States of America. The parties agree that the Uniform Computer Information Transactions Act (UCITA) is hereby excluded from application to this document. Any provision of this document held to be unenforceable shall not affect the enforceability of any other provisions of this document. In the event of any conflict between the terms of this document and the terms of any agreement, the terms of this document shall control. Neither party shall be in default if its failure to perform any obligation under this document is caused solely by supervening conditions beyond that party's reasonable control, including acts of God, civil commotion, war, strikes, labor disputes, third party Internet service interruptions or slowdowns, vandalism or "hacker" attacks, acts of terrorism or governmental demands or requirements. Customer agrees that IT-CNP may issue a press release identifying Customer as an IT-CNP customer, subject to customer's prior approval, which will not be unreasonably withheld or delayed. The parties agree that any press release or other public comments issued by either party relating to this document, any dispute of this document, or Customer's use of the Services, will be prepared jointly between IT-CNP and Customer and will be issued upon mutual agreement of the parties. Both parties agree that Customer maintains sole discretion over the use of its name or logo and requires IT-CNP to obtain Customer's approval through written consent prior to any use. Pre-printed terms and conditions on or attached to any Customer purchase order shall be of no force or effect.

EXHIBIT A - SERVICE LEVEL AGREEMENT

1. SERVICE AVAILABILITY. IT-CNP, Inc. will use commercially reasonable efforts to ensure that the Services will be available 24 hours per day, 7 days per week, excluding any Scheduled Downtime or Unscheduled Downtime events, each as defined below. The Service availability shall be measured as the total number of minutes in a month minus the total number of minutes in that month that comprise Schedule Downtime or Unscheduled Downtime events ("Scheduled Uptime").

2. SCHEDULED DOWNTIME. A minimum of (7) days advance notice will be provided for all scheduled downtime to perform system maintenance, backup and upgrade functions for the Services (the "Scheduled Downtime") if the Services will be unavailable due to the performance of system maintenance, backup and upgrade functions. Scheduled Downtime will not exceed eight (8) hours per month and will be scheduled in advance during off-peak hours (based on U.S. Eastern Standard Time). IT-CNP will notify the Customer administrator via email of any Scheduled Downtime that will exceed (2) hours. The duration of Scheduled Downtime is measured, in minutes, as the amount of elapsed time from when the Services are not available to perform operations to when the Services become available to perform operations. Daily system logs will be used to track Scheduled Downtime and any other Service outages.

3. UNSCHEDULED DOWNTIME. Unscheduled Downtime is defined as any time outside of the Scheduled Downtime when the Services are not available to perform operations, excluding any outages caused by the failure of any third party vendors, the Internet in general, or any emergency or force majeure event. The measurement is in minutes.

4. SERVICE LEVEL CREDITS. IT-CNP's goal is to achieve 100% Scheduled Uptime Availability for all customers. Subject to Sections 5 and 6 below, if IT-CNP does not meet the Scheduled Uptime levels set forth below, Customer will be entitled, upon written request, to a Service Level Credit to be calculated as follows, with the credit being calculated on the basis of the monthly service charge for the affected Services:

• If Scheduled Uptime is 100% of the month's minutes, no Service Level Credit is awarded.

• If Scheduled Uptime is 99.75% to 99.999% (inclusive) of the month's minutes, Customer will be eligible for a credit of 5% of a monthly fee paid to IT-CNP.

• If Scheduled Uptime is 99.50% to 99.74% (inclusive) of the month's minutes, Customer will be eligible for a credit of 7.5% of a monthly fee paid to IT-CNP.

• If Scheduled Uptime is less than 99.50% of the month's minutes, Customer will be eligible for a credit of 10.0% of a monthly fee paid to IT-CNP.

For annual paying Customers, the monthly fee for the purposes of calculating the Service Level Credit due shall be a monthly average fee derived from one-twelfth (1/12th) of the then-current annual fee paid to IT-CNP for the affected Services.

5. EXCEPTIONS. Customer shall not receive any credits under this SLA in connection with any failure or deficiency of system availability caused by or associated with: (a) circumstances beyond IT-CNP's reasonable control, including, without limitation, acts of any governmental body, war, insurrection, sabotage, armed conflict, embargo, fire, flood, strike or other labor disturbance, interruption of or delay in transportation, unavailability of or interruption or delay in telecommunications or third party services, virus attacks or hackers, failure of third party software (including, without limitation, e-commerce software, payment gateways, chat, statistics or free scripts) or inability to obtain raw materials, supplies, or power used in or equipment needed for provision of this SLA; (b) failure of access circuits to network, unless such failure is caused solely by IT-CNP; (c) scheduled maintenance and emergency maintenance and upgrades; (d) DNS issues outside the direct control of IT-CNP; (e) issues with FTP, POP, or SMTP access; (f) customer's acts or omissions (or acts or omissions of others engaged or authorized by customer), including, without limitation, custom scripting or coding (e.g., CGI, Perl, HTML, ASP, etc), any negligence, willful misconduct, or use of the Services in breach of Customer Conduct Obligations; (g) email delivery and transmission; (h) DNS (Domain Name Server) propagation; (i) outages elsewhere on the Internet that hinder access to your account. IT-CNP is not responsible for browser or DNS caching that may make your site appear inaccessible when others can still access it. IT-CNP will guarantee only those areas considered under the direct control of IT-CNP.

6. SERVICE LEVEL CREDIT REQUEST PROCEDURES. To receive a credit, the customer must make a request therefore by sending an e-mail message to accounting@it-cnp.com. The e-mail message MUST include the domain or system name of the customer's account in the "Subject" line. Each request in connection with this SLA must include the customer's account number (per IT-CNP 's invoice) and the dates and times of the unavailability of customer's system, and must be received by IT-CNP within ten (10) business days after the customer's system was not available. If the unavailability is confirmed by IT-CNP and is determined to be within the scope of IT-CNP's control, Service Level Credits will be applied within two billing cycles after IT-CNP 's receipt of the customer's credit request. Service Level Credits are not refundable

and can be used only towards future billing charges. Notwithstanding anything to the contrary herein, the total amount credited to customer in a particular month under this SLA shall not exceed the total hosting fee paid by customer for such month for the affected Services. Credits are exclusive of any applicable taxes charged to customer or collected by IT-CNP. Service Level Credits shall be Customer's sole and exclusive remedy in the event of any failure to meet the Service Levels.

6. Description Of Electronic Commerce (EC) Services

GovDataHosting.Com, a specialized FedRAMP certified hosting services division of IT-CNP, Inc. is a leading provider of FISMA compliant fully managed dedicated, virtual and cloud hosting services, providing high availability, reliable and compliant web hosting infrastructure and premier full scope system management and compliance services exclusively for U.S. Federal agencies. GovDataHosting.Com's solutions are designed for agencies seeking scalable, security compliant, highly available and enterprise-grade hosting solutions that can be expeditiously provisioned to meet unique ordering activity requirements. More information about GovDataHosting.Com service offerings is available at www.govdatahosting.com

6.1 GovDataHosting.Com offers the following managed IT infrastructure services:

- **FISMA Compliant Managed Hosting** - Offered exclusively to support U.S. Federal agency systems, GovDataHosting.Com provides a robust fully managed dedicated and virtual hosting infrastructure, compliant with applicable FISMA, HIPPA, NIST and DIACAP requirements. Features include a comprehensive set of enterprise infrastructure and server management services combined with complete security compliance and continuous monitoring services with associated documentation.

- **Public GovCloud** - Offered exclusively to support U.S. Federal agency systems, Public GovCloud offers fully managed FedRAMP JAB certified cloud Infrastructure as a Service (IaaS) in a multi-tenant U.S. agency environment from geographically dispersed and security compliant datacenters within the continental U.S. with rapid on demand allocation of scalable computing and processing resources. Features include fully managed rapid planning, provisioning and compliance documentation combined with cloud benefits of unit based pricing, resource utilization transparency and on-demand capacity scalability. Service is provided by IT-CNP's own network infrastructure zones across multiple states and national power grids.

- **Private GovCloud** - Offered exclusively to support U.S. Federal agency systems, Private GovCloud offers fully managed cloud Infrastructure as a Service (IaaS) dedicated to a single tenant environment. Available at multiple compliant datacenters within the U.S. with rapid on demand allocation of scalable computing and processing resources. Features include fully managed rapid planning, provisioning and compliance documentation combined with cloud benefits of unit based pricing, resource utilization transparency and on-demand scalability to meet capacity requirements. Service is provided by IT-CNP's own network infrastructure zones across multiple states and national power grids.

6.2 Optional Professional Services - available to supplement basic system management offerings beyond the operating system include:

- Database management (Microsoft SQL Server, Oracle, MySQL)
- Middleware management (Apache, Tomcat, IIS, WebSphere)
- Microsoft Exchange and Microsoft SharePoint management
- Custom application management (CMS, Drupal, Custom Applications)
- Initial security compliance documentation (C&A and A&A processes)
- On-going continuous monitoring/compliance management

- Web programming services (custom .Net, C#, PHP and Java)
- System development, integration and migration services
- High availability and disaster recovery planning services

6.3 FIPS 140-2 Encryption - FIPS 140-2 compliant encryption is utilized for all hosted infrastructure disk encryption. All data stored on GovDataHosting.Com FISMA Hosting and GovCloud infrastructure platforms is automatically encrypted utilizing robust hardware-based FIPS 140-2 compliant algorithms to provide continuous protection for customer data at rest.

6.4 Two-Factor Authentication - Optional Assurance Level 3 and Assurance Level 4 two-factor authentication infrastructure is available for all GovDataHosting.Com FISMA Hosting and GovCloud infrastructure platform customers.

6.5 Project Management - Project Management Institute (PMI) certified shared or dedicated project management is available for all GovDataHosting.Com FISMA Hosting and GovCloud infrastructure platform customers. All GovDataHosting.Com project managers are experienced with applicable requirements and nuances associated with FISMA compliance management requirements and methodology.

6.6 Clearances - All support activities are provided from continental U.S. locations by U.S. citizen personnel with a minimum of a criminal background check. GovDataHosting.Com can accommodate personnel clearance requirements ranging from Public Trust to Top Secret.

6.7 Assessment and Authorization (formerly Certification and Accreditation)

GovDataHosting.Com provides reasonable assurance to U.S. agency customers that all applicable system specific security controls are in place at a point in time prior to implementing the given IT application or system in a production environment. This process is achieved through a program of Assessment and Authorization (formerly called Certification and Accreditation) of the IT application or system which is accomplished by following NIST Special Publication 800-37.

- **DoD RMF Compliance** - All services provided by GovDataHosting.Com FISMA Hosting and GovCloud infrastructure platforms are compliant with DoD RMF and the latest edition of Department of Defense Cloud Computing Security Requirements Guide (SRG). GovDataHosting.Com is capable of hosting Level 2 categorized DoD owned information systems.

- **NIST Compliance** - All services provided by GovDataHosting.Com FISMA Hosting and GovCloud infrastructure platforms are compliant with NIST 800-53 Revision 4 guidance. GovDataHosting.Com is capable of hosting FIPS 199 High Risk, Moderate Risk and Low Risk categorized U.S. agency owned information systems.

- **NIST RMF Based/SOC2/Custom Compliance** - GovDataHosting.Com FISMA Hosting and GovCloud infrastructure platforms are also compliant with NIST Risk Management Framework (RMF) and other custom compliance models for agencies not subject to FISMA regulatory requirements.

6.8 Security Compliance Documentation and Continuous Monitoring

As part of its fully managed service offering, GovDataHosting.Com compiles all initial security compliance documentation (Certification Package) necessary to obtain a valid Approval to Operate (ATO) signed by the Federal government authorizing official before going into operation. As part of initial setup, the following documentation is established for every information system:

- System Security Plan (SSP)
- Configuration Management Plan (CMP)
- Risk Assessment (RA)
- Contingency & Recovery Plan (CRP)

- Incident Response Plan (IRP)
- Security Test and Evaluation Plan (ST&E)
- Vulnerability Scans
- Security Test and Evaluation Audit Report
- Initial Plan of Actions and Milestones (POAM)
- Interconnection Security Agreement (ISA)

Upon receipt of the security compliance documentation the respective Authorization Official for the system, in coordination with the system stakeholders such as Program Manager, Information System Security Manager (ISSM) and Information System Security Officer (ISSO) as applicable, will render an accreditation decision to authorize system operation with or without restrictions or limitations on its operations by issuing an Approval to Operate (ATO).

Once an applicable ATO is obtained, GovDataHosting.Com provides the following managed security compliance services to maintain the ATO through continuous monitoring of security controls and system operational environment.

6.9 Continuous Monitoring Highlights

- **Log Aggregation Services -** Managed service for historical and attack event correlation as well as addressing auditing and compliance requirements. This service provides necessary reporting to reconstruct suspected events as well as to satisfy FISMA, NIST, DIACAP, PCI, HIPAA, SOX and other compliance requirements.

- **Security Information and Event Monitoring (SIEM) -** Reporting tool to correlate events collected from all implemented security devices and services. This service leverages near real time event information across the network and server infrastructure to provide necessary alert and reporting services to Security Operations Center (SOC).

- **Intrusion Detection/Prevention Service (IDS/IPS) -** GovDataHosting.Com managed IDS/IPS service continuously monitors the network and server infrastructure to detect any suspected intrusion or malware distribution activity. IDS/IPS service is deployed on the network as well as on each server host (host based intrusion detection) to offer multiple layers of unwanted activity detection and prevention.

- **Managed Network Traffic Behavior Analysis (Netflow) -** Provides network visibility into traffic utilization capacity, patterns and activities. This service also performs application, service, port and resource utilization monitoring.

- **Managed Server Vulnerability Scanning -** On-going periodic server vulnerability scanning is performed on all dedicated and virtual servers to identify new vulnerabilities applicable to the operating system and installed applications.

- **Security Patch Implementation -** All published security patches for implemented operating systems are integrated into the infrastructure and customer implementations to ensure a consistent and current level of protection against resolved security threats.

- **Managed Application Scanning -** As an optional service for GovDataHosting.Com customers, periodic external vulnerability scanning is performed. External vulnerability scanning provides an early detection of newly introduced common application level vulnerabilities such as cross-site scripting and SQL injection.

- **Managed Backup and Recovery -** Continuous stream of incremental backups ensures integrity and availability of customer data, as well as provides for a number of safe recovery points in accordance with each customer's unique project requirements and information assurance mission.

- **Continuous Threat Assessment /Incident Response -** Trained security personnel continuously monitor and assess data feeds and reports from multiple sources to compile a live operational and security posture of each customer system to ensure that any suspicious activity is reviewed, analyzed and upon confirmation is escalated to the appropriate components based on standard operating procedures.

- **Periodic Mandatory NIST SP 800-53 Tasking -** On-going mandatory daily, weekly, monthly, quarterly and annual tasking referenced in NIST Special Publication 800-53 Revision 4 is performed and documented in accordance with IT-CNP, Inc. Enterprise Security Policy (ESP) that covers implementation and guidance of operational, technical and management controls that protect customer's data.

Continued On The Next Page

7. Pricing Of Electronic Commerce (EC) Services

7.1 FISMA Compliant Managed Hosting Platform Pricing (SIN 54151ECOM)

Item	Item Description	GSA MRC	GSA NRC
Managed FISMA Web Hosting Network and Server Infrastructure			
FISMA Hosting - 1	Managed Dedicated Windows/Linux Server (1 Proc/32GB RAM/600GB Disk), per server	$ 599.40	$ 2,208.97
FISMA Hosting - 2	Managed Dedicated Windows/Linux Server (2 Proc/64GB RAM/1000GB Disk), per server	$ 700.05	$ 2,413.00
FISMA Hosting - 3	Managed Dedicated Windows/Linux Server (2 Proc/128GB RAM/2000GB Disk), per server	$ 800.71	$ 2,615.21
FISMA Hosting - 4	Managed Windows Virtual Server (1 VP/2GB RAM/100GB Disk), per server	$ 184.08	$ 1,864.38
FISMA Hosting - 5	Managed Linux Virtual Server (1 VP/2GB RAM/100GB Disk), per server	$ 173.20	$ 1,864.38
FISMA Hosting - 6	Managed Unlicensed Virtual Server (1 VP/2GB RAM/100GB Disk), per server	$ 143.27	$ 1,864.38
FISMA Hosting - 7	Virtual RAM/Memory Add-On - 2 GB	$ 32.64	$ 186.80
FISMA Hosting - 8	Virtual Server Allocated Disk Add-On - Tier 1 FIPS 140-2 Encrypted Disk - 50 GB	$ 50.78	$ 186.80
FISMA Hosting - 9	Virtual Server Allocated Disk Add-On - Tier 2 FIPS 140-2 Encrypted Disk - 50 GB	$ 45.34	$ 176.83
FISMA Hosting - 10	Virtual Server Allocated Disk Add-On - Tier 3 FIPS 140-2 Encrypted Disk - 50 GB	$ 25.39	$ 124.23
FISMA Hosting - 11	Virtual Processor Add-On, per virtual processor	$ 47.15	$ 186.80
FISMA Hosting - 12	Unmetered In/Out Internet Bandwidth Utilization - Per Mbps	$ 96.12	$ 96.12
FISMA Hosting - 13	Public/Static IP Address, block of 5 IP addresses	$ 95.67	$ 96.12
FISMA Hosting - 14	Inherited Proxy/Load Balancing Service, per rule	$ 76.17	$ 196.78
FISMA Hosting - 15	Inherited Network Firewall Service, block of 10 rules	$ 186.80	$ 448.87
FISMA Hosting - 16	Resource Utilization Report, per report	$ 136.02	$ 287.46
FISMA Hosting - 17	Server Administration - FIPS 140-2 Encrypted Remote Access, per user	$ 18.14	$ 96.12
FISMA Hosting - 18	Server Administration - 2-Factor Authentication (Level 3 Assurance), per user	$ 29.02	$ 247.56
FISMA Hosting - 19	Server Administration - 2-Factor Authentication (Level 4 Assurance), per user	$ 34.46	$ 348.21
FISMA Hosting - 20	Firewall to Firewall VPN Service, per VPN	$ 317.38	$ 1,793.65
FISMA Hosting - 21	Application/Database Performance Monitoring, block of 5 monitors monitor	$ 196.78	$ 398.09
On-Site Data Backup and Data Archival			
FISMA Hosting - 22	4 Hour FIPS 140-2 Encrypted On-Site Backup - 10 Day Retention - Per 100 GB	$ 56.22	$ 196.78
FISMA Hosting - 23	Daily FIPS 140-2 Encrypted On-Site Backup - 10 Day Retention - Per 100 GB	$ 35.37	$ 176.83
FISMA Hosting - 24	Weekly FIPS 140-2 Encrypted On-Site Backup - 5 Week Retention - Per 100 GB	$ 25.39	$ 156.88
FISMA Hosting - 25	Monthly FIPS 140-2 Encrypted On-Site Data Archival - 12 Month Retention - Per 100 GB	$ 126.05	$ 146.90
Off-Site Disaster Recovery and Data Archival			
FISMA Hosting - 26	Managed FIPS 140-2 Encrypted Off-Site Data Storage and DR - 4 to 8 day RTO - Per 100 GB	$ 196.78	$ 196.78
FISMA Hosting - 27	Monthly FIPS 140-2 Encrypted Off-Site Data Archival - 12 Month Retention - Per 100GB	$ 145.99	$ 166.85
FISMA Hosting - 28	Disaster Recovery Testing Add-On - Full Test, one test per year	$ 418.94	$ -
FISMA Hosting - 29	Disaster Recovery Testing Add-On - Tabletop Exercise Test, one test per year	$ 186.80	$ -
Security Compliance			
FISMA Hosting - 30	NIST Compliance/Documentation/Continuouos Monitoring Service, per server	$ 653.80	$ 5,526.05
FISMA Hosting - 31	DIACAP Compliance/Documentation/Continuous Monitoring Service, per server	$ 754.46	$ 5,828.92
FISMA Hosting - 32	SSAE16 (SAS70)/Custom Compliance/Documentation/Continous Monitoring Service, per server	$ 629.32	$ 2,503.68
FISMA Hosting - 33	Database Security Management Service, per database	$ 327.36	$ 1,259.55
FISMA Hosting - 34	External Application Vulnerability Scanning, per URL scan	$ 252.09	$ 655.62

GSA MRC - GSA Multiple Award Schedule Monthly Recurring Charge
GSA NRC - GSA Multiple Award Schedule Non Recurring Charge
GB - Gigabyte | TB - Terabyte | Mbps - Megabits | VP - Virtual Processor | RAM - Memory
RTO - Recovery Time Objective | FIPS - Federal Information Processing Standard
All rates include GSA IFF fees

Continued On The Next Page

7.2 Public and Private GovCloud Platform Pricing (SIN 54151ECOM)

Item	Item Description	GSA MRC	GSA NRC
FISMA GovCloud - 1	Internet Bandwidth Out Transfer, per GB, per month	$ 0.12	$ 1,002.92
FISMA GovCloud - 2	Managed Licensed Windows Virtual Server (1 V. Proc / 2GB Memory), per hour	$ 0.22	$ 1,864.38
FISMA GovCloud - 3	Managed Linux Virtual Server (1 V. Proc / 2GB Memory), per hour	$ 0.20	$ 1,864.38
FISMA GovCloud - 4	Managed Unlicensed Virtual Server (1 V. Proc / 2GB Memory), per hour	$ 0.16	$ 1,864.38
FISMA GovCloud - 5	Add-On Virtual Server Memory, per GB per hour	$ 0.05	$ -
FISMA GovCloud - 6	Add-On Virtual Processor, per Virtual Processor per hour	$ 0.12	$ -
FISMA GovCloud - 7	Add-On FIPS 140-2 Encrypted Tier 1 Server Storage, per GB per month	$ 0.48	$ -
FISMA GovCloud - 8	Add-On FIPS 140-2 Encrypted Tier 2 Server Storage, per GB per month	$ 0.43	$ -
FISMA GovCloud - 9	Add-On FIPS 140-2 Encrypted Tier 3 Server Storage, per GB per month	$ 0.34	$ -
FISMA GovCloud -10	Managed On-Site FIPS 140-2 Encrypted Backup, per GB per month	$ 0.20	$ -
FISMA GovCloud -11	Managed Off-Site FIPS 140-2 Encrypted Data Storage, 4 - 8 day RTO, per GB per month	$ 2.47	$ -
FISMA GovCloud -12	Managed NIST Compliance/Documentation/Continuouos Monitoring, per server, per hour	$ 1.11	$ 5,526.05
FISMA GovCloud -13	Managed DIACAP Compliance/Documentation/Continuous Monitoring, per server, per hour	$ 1.16	$ 5,526.05
FISMA GovCloud -14	Managed SSAE16/Custom Compliance/Documentation/Continous Monitoring, per server, per hour	$ 1.02	$ 2,503.68

GSA MRC - GSA Multiple Award Schedule Monthly Recurring Charge
GSA NRC - GSA Multiple Award Schedule Non Recurring Charge
GB - Gigabyte | TB - Terabyte | Mbps - Megabits | VP - Virtual Processor | RAM - Memory
RTO - Recovery Time Objective | FIPS - Federal Information Processing Standard
All rates include GSA IFF fees

7.3 Microsoft Software -SPLA (SIN 54151ECOM)

All Microsoft software is available under the SPLA Licensing Agreement (monthly right to use) can ONLY be used on managed virtual or dedicated servers hosted at IT-CNP cloud datacenters and obtained under this schedule. The rights to use the software terminate when the dedicated, collocation, or managed services agreement terminates.

Microsoft sets the SPLA software pricing and licensing requirements and is subject to change. Please contact IT-CNP, Inc. for the current pricing and licensing requirements. Microsoft licenses are provided under Incidental Items as authorized in the FAR.

All Microsoft software is part of a bundled managed hosting service (sin 54151ECOM) for purchasing purposes. The exact number of licenses is based on the user requirements of the managed services being provided and pricing is Software Licensing Units (SLUs). The exact customer configuration determines the number of SLUs required to be purchased.

Item	Item Description	GSA MRC	GSA NRC
SOLU	Software Licensing Unit (per unit)	$ 1.01	$ -

GSA MRC - GSA Multiple Award Schedule Monthly Recurring Charge
GSA NRC - GSA Multiple Award Schedule Non Recurring Charge
All rates include GSA IFF fees

Continued On The Next Page

8. Terms and Conditions Applicable To Cloud and Cloud Related IT Professional Services (SIN 518210C)

These terms and conditions apply to IT-CNP's GovDataHosting Cloud Platform, a Federal Risk and Authorization Management Program (FedRAMP) High Impact authorized cloud Infrastructure-as-a-Service available for exclusive use of U.S. government agencies.

During the contract period, IT-CNP and the Government agree that these terms and conditions will apply to any order for GovDataHosting Cloud Platform cloud services.

The term "Government" shall mean all U.S. Federal agencies (United States Executive Branch), agencies of U.S. Legislative Branch, Agencies of U.S Judicial branch, U.S. state and local government agencies and the Government of the District of Columbia, all of which are hereinafter referred to as the Government.

The services under this Special Item will be available to the Government within the United States, the District of Columbia and Puerto Rico.

On a case-by-case basis IT-CNP, Inc. may choose to perform services to overseas U.S. Government locations which are maintained in support of national defense operations (including Embassies), and to locations which support the national interest of the United States.

8.1 SCOPE

The prices, terms and conditions stated under Special Item Number (SIN) 518210C Cloud Computing Services apply exclusively to Cloud Computing Services within the scope of this GSA 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 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 GSA IT Schedule 70 SINs (e.g. 54151S and 54151ECOM).

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

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,**	**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.** **Platform as a Service (PaaS): Consumer deploys applications onto cloud platform**

public, community or hybrid), vendors specify deployment models	**service using provider-supplied tools. Has control over deployed applications and some limited platform configuration but does not manage the platform or infrastructure.** **Infrastructure as a Service (IaaS): Consumer provisions computing resources. Has control over OS, storage, platform, deployed applications and some limited infrastructure configuration, but does not manage the infrastructure.**

Table 1: Cloud Computing Services SIN

8.2 DESCRIPTION OF CLOUD COMPUTING SERVICES

IT-CNP's GovDataHosting Cloud Platform offering under this SIN includes Infrastructure as a Service (IaaS).

IT-CNP's GovDataHosting Cloud Platform IaaS offering is provided to U.S. Government customers as a subscription service. It provides a basic cloud infrastructure capability for an agency to provision processing, storage, networking, communications, security and other fundamental resources upon which an agency can run an array of software, including operating systems, middleware and applications.

GovDataHosting Cloud Platform has 3 geographically separate cloud zones exclusively dedicated to supporting U.S. Government customers.

All GovDataHosting Cloud Platform cloud zones meet rigorous government security requirements up through and including FISMA High Impact and FedRAMP High Impact.

GovDataHosting Cloud Platform is FedRAMP Joint Authorization Board (JAB) High Impact Authorized for use by any U.S. Federal Government agency.

The JAB authorizing officials are Chief Information Officer of U.S. Department of Defense, Chief Information Officer of U.S. Department of Homeland Security and Chief Information Officer of U.S. General Services Administration.

NIST Essential Cloud Characteristics

NIST's essential cloud characteristics provide a consistent metric for whether a service is eligible for inclusion in this SIN. It is understood that due to legislative, funding and other constraints that government entities cannot always leverage a 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 2 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.

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 an 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 another cloud or non-cloud networks and services. For example a private cloud might require an Ordering Activity to purchase or 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. 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 and Ordering Activity to control their use in cooperation with self service	Procurement guidance for on-demand self-service applies to measured service 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

Table 2: Meeting NIST Essential Characteristics with GovDataHosting Cloud Platform

GovDataHosting Cloud Platform meets all cloud requirements as defined in the National Institute of Standards and Technology (NIST) Special Publication 800-145: The NIST Definition of Cloud Computing which defined cloud computing as a model for enabling ubiquitous, convenient, on-demand network

access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

On-Demand Self-Service – GovDataHosting Cloud Platform includes on on-demand self service capability available to customers through use of its tenant service portal. Administrative access for agencies to the tenant on-demand self-service portal is provided via a secure multi-factor authentication verified virtual private network (VPN) connection with role-based enforced user permissions levels.

There are multiple ways to interact with GovDataHosting Cloud Platform on-demand self-service tenant portal capability:

1) Login to self-service tenant portal directly to provision processing resources; or

2) Send service provisioning commands to the self-service tenant portal through a secure application programing interphase (API); or

3) Leverage GovDataHosting full-service management subscription service.

Broad Network Access - GovDataHosting Cloud Platform users can simply access all cloud resources through a certified web browser – such as Chrome, Safari, Firefox or Internet Explorer, and a functional Internet connection or a standard agency network. The service is accessible by any device running a certified browser. All administrative user connections to GovDataHosting Cloud Platform are encrypted utilizing FIPS 140-2 certified VPN encryption. Any computer workstation capable of running a certified browser and VPN can access GovDataHosting Cloud Platform services.

As an alternative to a public Internet connection, GovDataHosting Cloud Platform supports private U.S. Government agency-specific private network connectivity.

Authorized agency-provided networking, security or purpose-specific hardware is supported for deployment in any GovDataHosting Cloud Platform cloud zone.

Resource Pooling – GovDataHosting Cloud Platform is a virtualized multi-tenant environment that ensures common cloud resource pooling by providing aggregated storage, memory and CPU processing resources and presenting them to customers for virtual allocation and consumption through the cloud tenant portal thus ensuring common resource pooling.

To ensure security of virtual customer separation in the cloud resource pool, multiple layers of protection are implemented and annually audited by FedRAMP certified independent assessment organization.

Rapid Elasticity - GovDataHosting Cloud Platform is architected as vast national cloud infrastructure that allows agencies to quickly react to their cloud processing resources demand by rapidly increasing or decreasing their assigned clod processing resources utilizing our cloud tenant portal. Agencies can also configure auto-scaling features to execute automated adjustments to their processing resources to accommodate changes in workload demand.

Measured Service - GovDataHosting Cloud Platform infrastructure provides clear service metrics for agencies such as memory, storage, compute and bandwidth provisioned. These metrics are provided to customers via our cloud tenant portal where resource consumption, resource utilization, availability and cost are tracked.

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 bundle or 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 IT-CNP's GovDataHosting Cloud Platform and a PaaS service from another provider. The PaaS service from another provider may inherit broad network access from IT-CNP's GovDataHosting Cloud Platform 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.

8.4 CLOUD 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.

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.

Table 4: Guidance for Selecting a Deployment Model

IT-CNP's GovDataHosting Cloud Platform is offered in the following 2 cloud deployment models:

Community Cloud - GovDataHosting FISMA Community Cloud is a federal government-dedicated multi-tenant community cloud platform that enables agencies and government contractors to cost-effectively procure virtualized cloud server, network and security infrastructure resources available at a fixed or consumption-based price. Becoming a customer of our FISMA Community Cloud is the most cost-effective way of obtaining all necessary cloud, technology and security compliance resources while satisfying government-mandated security controls. Benefits of our FISMA Community Cloud include:

- Open only to U.S. agencies and government contractor customers
- Exclusive community of U.S. agency systems hosting government data
- FedRAMP-audited logical separation controls ensure complete tenant separation
- Managed by background U.S. citizens from U.S. locations only
- Eligible for low, moderate or high impact systems
- Public Internet and private agency connectivity options are available
- The fastest and most cost effective way to host a government system in a cloud

Private Cloud – GovDataHosting FISMA Private Cloud is a federal government-dedicated single-tenant enclave that enables agencies and government contractors to procure dedicated virtualized cloud server, network and security infrastructure resources to support highly intensive or sensitive data cloud workload. Becoming a customer of our FISMA Private Cloud is in the most efficient way of obtaining all necessary cloud, technology and security compliance resources while satisfying government-mandated security controls. Benefits of our FISMA Private Cloud include:

- Open only to U.S. agencies and government contractor customers
- Dedicated hypervisors, vCPU, memory and storage resources
- Physical separation controls ensure privacy through complete tenant isolation
- Managed by background U.S. citizens from U.S. locations only
- Eligible for low, moderate or high impact systems
- Public Internet and private agency connectivity options are available
- The most efficient way to host a sensitive government system in a cloud

8.5 CLOUD 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.

1) VisibilitytotheOrderingActivity.Servicemodelsub-categoriesinthisSINexisttohelp 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, or SaaS capabilities for specific applications.

In a service mix situation the Contractor should select the service model that is their primary focus. 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 3 offers examples of how services might be properly mapped to NIST service models and how a Contractor should interpret the service model sub-categories.

Characteristic	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 Service (PaaS) 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 • 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 • 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.

Table 3: Guidance on Mapping to NIST Service Models

IT-CNP's GovDataHosting Cloud Platform is offered to agencies as an Infrastructure-as-a-Service service model where customers interact with virtualized cloud resources via provisioning storage, memory, compute and other resources through the cloud tenant portal.

All GovDataHosting Cloud Platform cloud datacenters (cloud zones) are located within the continental United States and supported by trained U.S. citizen personnel with positively adjudicated criminal background checks and signed non-disclosure agreements upon hire.

GovDataHosting Cloud Platform leverages enterprise network and server hardware as foundation of the cloud physical layer infrastructure providing customers' virtual servers, processing and memory resources.

Disk infrastructure is provided by enterprise storage platform equipped with software and hardware based FIPS 140-2 certified encryption options providing secure and compliant storage for all government data.

Our cloud offers a variety of DISA STIG-hardened virtual server operating system templates for accelerated compliance with requisite NIST and agency-specific standards.

IT-CNP's GovDataHosting Cloud Platform has been FedRAMP JAB authorized as an Infrastructure-as-a-Service cloud option for government agencies since 2015, currently holding a FedRAMP High Impact authorization.

9. Pricing Of Cloud Computing Services

GovDataHosting Cloud Platform Authorized GSA Pricing (Includes GSA IFF)

MFR	SIN	Model Number	Description	GSA Price w/IFF	Unit	Production Point
GCP	518210C	GCP-COMMIT-1	GCP Commit - $1 in usage fees at GCP list price	$ 0.96	EA	USA
GCP	518210C	GCP-COMMIT-10	GCP Commit - $10 in usage fees at GCP list price	$ 9.57	EA	USA
GCP	518210C	GCP -COMMIT-100	GCP Commit - $100 in usage fees at GCP list price	$ 95.72	EA	USA
GCP	518210C	GCP -COMMIT-1000	GCP Commit - $1,000 in usage fees at GCP list price	$ 957.18	EA	USA
GCP	518210C	GCP -COMMIT-10000	GCP Commit - $10,000 in usage fees at GCP list price	$ 9,571.79	EA	USA
GCP	518210C	GCP -COMMIT-100000	GCP Commit - $100,000 in usage fees at GCP list price	$ 95,717.88	EA	USA

From the GovDataHosting Cloud Platform (GCP) cloud service catalog (https://www.govdatahosting.com/catalog) select the cloud service items required. The GCP cloud service catalog will show the available GCP service items with their associated list prices. Based on GCP items required for your cloud solution, purchase the appropriate amount of GCP commits from the pricing table above. IT-CNP's GovDataHosting will discount the list price by a minimum of 5% to arrive at the initial GSA pricing, followed by addition of required GSA Industrial Funding Fee (IFF) of 0.075%.

9.1 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 based on mutually agreed to and approved test procedures.

b. Training

Cloud related training, if requested shall be performed under this SIN 518210C.

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 cloud computing offering such as integration, migration, and other cloud professional services are available under this SIN 518210C.

e. Performance of Cloud Computing Services

The Contractor shall respond to Ordering Activity requirements at the Task Order level. Responses will be based on requirements outlined in the Request for Proposal. Contractors may include 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 at the Task Order level to address any reporting requirements and specify general reporting capabilities available for the Ordering Activity to verify performance, cost and availability.

9.2 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 per FIPS 199 and FIPS 200. The Contractor must be capable of meeting at least the minimum security requirements assigned against a low-impact information system in each CIA assessment area (per FIPS 200) and must detail the FISMA capabilities of the system in each of CIA assessment area.

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 (MEMORANDUM FOR CHIEF INFORMATION OFFICERS: Security Authorization of Information Systems in Cloud Computing Environments. December 8, 2011).

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 800-1224 and OMB memos M-06-165 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, general regions where service locations are available, etc.

l. Related Cloud Professional Services

Ordering activities should engage with Contractors to discuss the availability of assistance with cloud related professional services such as cloud migration, integration, initial setup, security hardening, information security continuous monitoring, training and access to the services that may be available through this SIN.

9.3 TERMS OF USE AGREEMENT – U.S. GOVERNMENT

IT-CNP, INC. GOVDATAHOSTING CLOUD PLATFORM

SUPPLEMENTAL CLOUD HOSTING TERMS OF USE AGREEMENT - U.S. GOVERNMENT

The ordering activity (Customer) agrees to abide by the following Cloud Hosting Terms Of Use:

This GSA Multiple Award Schedule Supplemental Cloud Hosting Terms Of Use Agreement ("Agreement) is made by and between IT-CNP, Inc. (“IT-CNP”) and organizations eligible to place orders against IT-CNP's GSA Schedule 70 contract to purchase web hosting and related IT professional services (“Customer”). This Agreement is effective as of the date referenced in each customer's individual task order (“Effective Date”).

1. SERVICE LEVELS. IT-CNP will provide the Services in accordance with the Service Level Agreement attached hereto as Exhibit A.

2. LICENSE GRANT. Subject to this Agreement, terms and conditions, IT-CNP hereby grants to Customer, (and to each Customer employee or authorized contractor who accesses the Services by means of Customer's account and an authorized password), subject to all of the terms and conditions, a non-exclusive, non-transferable, non-sublicensable license to access and use the Services via the Internet, solely for intended business purposes in accordance with any applicable end user documentation.

3. LICENSE RESTRICTIONS. Customer shall not, directly or indirectly, (i) reverse engineer, decompile, disassemble or otherwise attempt to discover the source code or underlying ideas or algorithms of the Services; (ii) modify, translate, or create derivative works based on the Services; (iii) rent, lease, distribute, sell, resell, assign, or otherwise transfer rights to the Services; (iv) use the Services for timesharing or service bureau purposes or otherwise for the benefit of a third party; (v) remove any proprietary notices from the Services; (vi) publish or disclose to third parties any evaluation of the Services without IT-CNP 's prior written consent.

4. PASSWORDS/SECURITY.

4.1 Passwords. IT-CNP may issue to Customer, or shall authorize a Customer administrator to issue, infrastructure access password for users authorized to use Customer's account. Customer and its users are responsible for maintaining the confidentiality of all passwords and for ensuring that each password is used only by the authorized user. Customer is entirely responsible for any and all activities that occur under the Customer's account and all charges incurred from use of the Services accessed with the Customer’s passwords. Customer agrees to immediately notify IT-CNP of any unauthorized use of the Customer's account (including each password of each user accessing the Services by means of Customer's account) or any other breach of security known to Customer. IT-CNP shall have no liability for any loss or damage arising from Customer's failure to comply with these requirements.

4.2 Security. IT-CNP will implement commercially reasonable security precautions and industry's best practices to prevent unauthorized access to the Customer Data (as defined below). Customer acknowledges that, notwithstanding such security precautions, use of or connection to the Internet provides the opportunity for unauthorized third parties to circumvent such precautions and illegally gain access to the Services and Customer Data. Accordingly, IT-CNP cannot and does not guaranty the privacy, security or authenticity of any information so transmitted over or stored in any system connected to the Internet.

5. CUSTOMER DATA. As between IT-CNP and Customer, Customer shall own all data, information or material that Customer enters into the Services or has entered on its behalf ("Customer Data"). IT-CNP's authorized personnel may access Customer's account and Customer Data from time to time, as IT-CNP deems necessary, solely for purposes of information security monitoring, management and audit, technical support, administration and invoicing related to Customer's use of the Services. Except as permitted, IT-CNP will not edit, delete or disclose the contents of Customer Data unless authorized by the Customer or unless IT-CNP is required to do so by law or in the good faith belief that such action is necessary to: (1) conform with applicable laws or comply with legal process served on IT-CNP; (2) protect and defend the rights or property of IT-CNP; or (3) enforce these terms of use. Customer is solely responsible for the accuracy, quality, integrity, legality, reliability, appropriateness and copyright of all Customer Data and IT-CNP assumes no responsibility for the deletion, correction, destruction, loss, infringement or failure of the Services to store any Customer Data. IT-CNP reserves the right to establish a maximum amount of memory, storage, computing resources or maximum amount of Customer Data that Customer may store, post or transmit on or through the Services.

6. CUSTOMER OBLIGATIONS.

6.1 Conduct. Customer shall be solely responsible for its actions and the actions of its users while using the Services and the contents of its transmissions through the Services (including, without limitation, Customer Data). Customer agrees: (1) to abide by all local, state, national, and international laws and regulations applicable to Customer's use of the Services, including without limitation all laws regarding the transmission of technical data exported from the United States through the Services; (2) abide by all terms of applicable software licensing agreements used in conjunction with Services (3) not to intentionally or deliberately upload or distribute in any way files that contain viruses, corrupted files, or any other similar software or programs that may damage the operation of the Services or another's computer; (4) not to use the Services for illegal purposes; (5) not to interfere or disrupt networks connected to the Services; (6) not to post, promote or transmit through the Services any unlawful, harassing, libelous, abusive, threatening, harmful, vulgar, obscene, hateful, racially, ethnically or otherwise objectionable material of any kind or nature; (7) not to transmit or post any material that encourages conduct that could constitute a criminal offense or give rise to civil liability; (8) not to interfere with another customer's use and enjoyment of the Services or another entity's use and enjoyment of similar services; (9) not to intentionally or deliberately engage in contests, chain letters or post or transmit "junk mail," "spam," "chain letters," or unsolicited mass distribution of email; (10) not to install any unauthorized software including but not limited to network traffic sniffers/scanners, network monitoring or vulnerability scanners, network/server intrusion/penetration related software or any other software that may result in unauthorized capture or disclosure of traffic information or datacenter network components; and (11) to comply with all regulations, policies and procedures of networks connected to the Services. Customer acknowledges and agrees that IT-CNP neither endorses the contents of any customer communications or Customer Data nor assumes any responsibility for any threatening, libelous, obscene, harassing or offensive material contained therein, any infringement of third party intellectual property rights arising therefrom or any crime facilitated thereby. IT-CNP may remove any violating content posted on the Services or transmitted through the Services, without notice to Customer.

6.2 External Links/Resources. IT-CNP shall have no liability, obligation or responsibility whatsoever arising out of or in connection with any external website content, links to other web sites or resources. Customer acknowledges and agrees that IT-CNP is not responsible for the availability of such external sites or resources, and does not endorse and is not responsible or liable for any content, advertising, products, services or other materials on or available from such sites or resources. IT-CNP shall not be responsible or liable, directly or indirectly, to Customer or to any third party for any damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such content, goods or services available on such external sites or resources.

7. FEES AND TAXES.

7.1 Fees. Fees should be addressed in the schedule contract (price list) and negotiated at the task order level. Prices referenced in the price list include taxes and duties.

7.2 Payments. Payments terms are addressed in the schedule contract and negotiated at the task order level.

8. TERM. The contract duration should be stated in the task order. Termination will be effective at the end of the applicable term in which such notice is received. Customer shall be responsible for all Fees for the applicable term in which termination occurs, and IT-CNP shall not issue any refunds for such term.

9. TERMINATION.

9.1 Termination. Termination/cancellation terms are governed by the schedule contract and Federal Acquisition Regulations (FAR).

9.2 Effect of Termination. Upon the effective date of expiration or termination of service for any reason, whether by Customer or IT-CNP, Customer's right to use the Services shall immediately cease. Sections 5, 6, 9, 10, 11, 12, 13 and 14 of this Agreement shall survive its expiration or termination for any reason. IT-CNP shall retain Customer Data for a period of thirty (30) days after expiration or termination of service. Customer may request that IT-CNP conduct an export of Customer Data, and IT-CNP agrees to provide such services on a time and materials basis pursuant to a separate agreement. After thirty (30) days, IT-CNP may delete and destroy all Customer Data without notice or further liability to Customer.

10. PROPRIETARY RIGHTS. Customer acknowledges that the Services and all IT-CNP owned content contained therein where applicable, including but not limited to text, software, music, sound, photographs, video, graphics, and third party materials, excluding any Customer Data, (collectively, "Content") is proprietary to IT-CNP or such third parties, and IT-CNP or such third parties retain exclusive ownership of the same throughout the world, including all related copyrights, trademarks, service marks, patents, trade secrets or other proprietary rights thereto. Except as expressly stated herein, this Agreement do not transfer any right, title or interest in the Services or the Content to the Customer.

11. CONFIDENTIALITY.

11.1 Obligations. Each of the parties agrees to maintain in confidence any non-public information of the other party, whether written or otherwise, disclosed by the other party in the course of performance of this Agreement that a party knows or reasonably should know is considered confidential by the disclosing party ('Confidential Information'). The receiving party shall not disclose, use, transmit, inform or make available to any entity, person or body any of the Confidential Information, except as a necessary part of performing its obligations hereunder, and shall take all such actions as are reasonably necessary and appropriate to preserve and protect the Confidential Information and the parties' respective rights therein, at all times exercising at least a reasonable level of care. Each party agrees to restrict access to the Confidential Information of the other party to those employees or agents who require access in order to perform hereunder, and, except as otherwise provided, neither party shall make Confidential Information available to any other person or entity without the prior written consent of the other party.

11.2 Exclusions. Confidential Information shall not include any information that is (i) already known to the receiving party at the time of the disclosure; (ii) publicly known at the time of the disclosure or becomes publicly known through no wrongful act or failure of the receiving party; (iii) subsequently disclosed to the receiving party on a non-confidential basis by a third party not having a confidential relationship with the other party hereto that rightfully acquired such information; or (iv) communicated to a third party by the receiving party with the express written consent of the other party hereto. A disclosure of Confidential Information that is legally compelled to be disclosed pursuant to Freedom of Information Act (FOIA), subpoena, summons, order or other judicial or governmental process shall not be considered a breach of this Agreement; provided the receiving party provides prompt notice of any such subpoena, order, or the like to the other party so that such party will have the opportunity to obtain a protective order or otherwise oppose the disclosure.

11.3 Destruction or Return of Confidential Information. Upon expiration or termination of service for any reason, each party shall promptly return to the other party, or destroy, as the parties agree, all copies of the other party's Confidential Information. All copies, notes or other derivative material relating to the Confidential Information shall be promptly retrieved or destroyed, as agreed, and no such material shall be retained or used by the receiving party in any form or for any reason.

12. LIMITED WARRANTY AND WARRANTY DISCLAIMER.

12.1 Limited Warranty. IT-CNP warrants that the Services will perform substantially in accordance with the functions described in the documentation provided by IT-CNP under normal use and circumstances by authorized users of the Services.

12.2 Disclaimer. EXCEPT AS EXPRESSLY STATED IN SECTION 13.1, THERE ARE NO WARRANTIES OR CONDITIONS (WHETHER IMPLIED OR ARISING BY STATUTE OR OTHERWISE IN LAW OR FROM A COURSE OF DEALING OR USAGE OF TRADE) FOR THE SERVICES OR SUPPORT. IT-CNP DISCLAIMS ALL STATUTORY OR IMPLIED WARRANTIES AND CONDITIONS. IT-CNP DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SERVICES WILL MEET THE CUSTOMER'S REQUIREMENTS OR THAT THE OPERATION OF THE SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE. FURTHER, IT-CNP DOES NOT WARRANT THAT ALL ERRORS IN THE SERVICES CAN OR WILL BE CORRECTED. CUSTOMER UNDERSTANDS AND AGREES THAT ANY MATERIAL OR DATA DOWNLOADED OR OTHERWISE OBTAINED THROUGH THE SERVICES IS DONE AT CUSTOMER'S OWN DISCRETION AND RISK, AND THAT CUSTOMER WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO CUSTOMER'S COMPUTER SYSTEM OR LOSS OF DATA THAT RESULTS FROM THE DOWNLOAD OR USE OF SUCH MATERIAL OR DATA. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, SO SOME OF THE ABOVE EXCLUSIONS MAY NOT APPLY TO CUSTOMER.

13. LIMITATION OF LIABILITY.

13.1 Limitation on Direct Damages. IN NO EVENT SHALL IT-CNP'S AGGREGATE LIABILITY, IF ANY, ARISING OUT OF OR IN ANY WAY RELATED TO THIS DOCUMENT EXCEED THE FEES PAID BY CUSTOMER IN THE MONTHLY TERM IN WHICH THE ACTION AROSE, FOR THE SERVICES THAT DIRECTLY GAVE RISE TO THE DAMAGES CLAIMED, WITHOUT REGARD TO WHETHER SUCH CLAIM IS BASED IN CONTRACT OR TORT, INCLUDING NEGLIGENCE.

13.2 Disclaimer of Consequential Damages. IN NO EVENT SHALL IT-CNP OR ITS SUPPLIERS BE LIABLE (A) FOR ANY INDIRECT, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR (B) TO THIRD PARTIES CLAIMING THROUGH CUSTOMER; EVEN IF IT-CNP HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

13.3 Essential Purpose. The essential purpose of this Section 13 is to limit the potential liability of the parties arising under this document. The parties acknowledge that the limitations set forth in this Section 13 are intricate to the amount of consideration levied in connection with the license of the Services and that, were IT-CNP to assume any further liability, such consideration would out of necessity, been set much higher. This Section 13, Limitation of Liability, shall not impair the U.S. Government's right to recover for fraud or crimes arising out of or related to this Agreement under any federal fraud statute. Furthermore, this clause shall not impair nor prejudice the U.S. Government's right to express remedies provided in the schedule contract (i.e. Price Reductions, Patent Indemnification, Liability for Injury or Damage, Price Adjustment, Failure to Provide Accurate Information.)

14. GENERAL. All notices to a party shall be in writing and sent to the addresses specified and shall be deemed to have been duly given when received, if personally delivered; when receipt is electronically confirmed, if transmitted by facsimile or email; the day after it is sent, if sent for next day delivery by recognized overnight delivery service; and upon receipt, if sent by certified or registered mail, return receipt requested. Neither Service nor any Services license may be assigned or transferred by Customer, by merger, operation of law or otherwise, without IT-CNP' prior written consent. The terms of the schedule and the task order would take precedence over the terms of this agreement. This document may be amended or superseded only by a written instrument signed by both parties. This document shall be governed by the federal laws of the United States of America. The parties agree that the Uniform Computer Information Transactions Act (UCITA) is hereby excluded from application to this document. Any provision of this document held to be unenforceable shall not affect the enforceability of any other provisions of this document. In the event of any conflict between the terms of this document and the terms of any agreement, the terms of this document shall control. Neither party shall be in default if its failure to perform any obligation under this document is caused solely by supervening conditions beyond that party's reasonable control, including acts of God, civil commotion, war, strikes, labor disputes, third party Internet service interruptions or slowdowns, vandalism or "hacker" attacks, acts of terrorism or governmental demands or requirements. Customer agrees that IT-CNP may issue a press release identifying Customer as an IT-CNP customer, subject to customer's

prior approval, which will not be unreasonably withheld or delayed. The parties agree that any press release or other public comments issued by either party relating to this document, any dispute of this document, or Customer's use of the Services, will be prepared jointly between IT-CNP and Customer and will be issued upon mutual agreement of the parties. Both parties agree that Customer maintains sole discretion over the use of its name or logo and requires IT-CNP to obtain Customer's approval through written consent prior to any use. Pre-printed terms and conditions on or attached to any Customer purchase order shall be of no force or effect.

EXHIBIT A - SERVICE LEVEL AGREEMENT

1. SERVICE AVAILABILITY. IT-CNP, Inc. will use commercially reasonable efforts to ensure that the Services will be available 24 hours per day, 7 days per week, excluding any Scheduled Downtime or Unscheduled Downtime events, each as defined below. The Service availability shall be measured as the total number of minutes in a month minus the total number of minutes in that month that comprise Schedule Downtime or Unscheduled Downtime events ("Scheduled Uptime").

2. SCHEDULED DOWNTIME. A minimum of (7) day advance notice will be provided for all scheduled downtime to perform system maintenance, backup and upgrade functions for the Services (the "Scheduled Downtime") if the Services will be unavailable due to the performance of system maintenance, backup and upgrade functions. Scheduled Downtime will not exceed eight (8) hours per month and will be scheduled in advance during off-peak hours (based on U.S. Eastern Standard Time). IT-CNP will notify the Customer administrator via email of any Scheduled Downtime that will exceed (2) hours. The duration of Scheduled Downtime is measured, in minutes, as the amount of elapsed time from when the Services are not available to perform operations to when the Services become available to perform operations. Daily system logs will be used to track Scheduled Downtime and any other Service outages.

3. UNSCHEDULED DOWNTIME. Unscheduled Downtime is defined as any time outside of the Scheduled Downtime when the Services are not available to perform operations, excluding any outages caused by the failure of any third party vendors, the Internet in general, or any emergency or force majeure event. The measurement is in minutes.

4. SERVICE LEVEL CREDITS. IT-CNP's goal is to achieve 100% Scheduled Uptime Availability for all customers. Subject to Sections 5 and 6 below, if IT-CNP does not meet the Scheduled Uptime levels set forth below, Customer will be entitled, upon written request, to a Service Level Credit to be calculated as follows, with the credit being calculated on the basis of the monthly service charge for the affected Services:

• If Scheduled Uptime is 100% of the month's minutes, no Service Level Credit is awarded.

• If Scheduled Uptime is 99.75% to 99.999% (inclusive) of the month's minutes, Customer will be eligible for a credit of 5% of a monthly fee paid to IT-CNP.

• If Scheduled Uptime is 99.50% to 99.74% (inclusive) of the month's minutes, Customer will be eligible for a credit of 7.5% of a monthly fee paid to IT-CNP.

• If Scheduled Uptime is less than 99.50% of the month's minutes, Customer will be eligible for a credit of 10.0% of a monthly fee paid to IT-CNP.

For annual paying Customers, the monthly fee for the purposes of calculating the Service Level Credit due shall be a monthly average fee derived from one-twelfth (1/12th) of the then-current annual fee paid to IT-CNP for the affected Services.

5. EXCEPTIONS. Customer shall not receive any credits under this SLA in connection with any failure or deficiency of system availability caused by or associated with: (a) circumstances beyond IT-CNP's reasonable control, including, without limitation, acts of any governmental body, war, insurrection, sabotage, armed conflict, embargo, fire, flood, strike or other labor disturbance, interruption of or delay in transportation, unavailability of or interruption or delay in telecommunications or third party services, virus attacks or hackers, failure of third party software (including, without limitation, e-commerce software, payment gateways, chat, statistics or free scripts) or inability to obtain raw materials, supplies, or power used in or equipment needed for provision of this SLA; (b) failure of access circuits to network, unless such failure is caused solely by IT-CNP; (c) scheduled maintenance and emergency maintenance and upgrades; (d) DNS issues outside the direct control of IT-CNP; (e) issues with FTP, POP, or SMTP access; (f) customer's acts or omissions (or acts

or omissions of others engaged or authorized by customer), including, without limitation, custom scripting or coding (e.g., CGI, Perl, HTML, ASP, etc), any negligence, willful misconduct, or use of the Services in breach of Customer Conduct Obligations; (g) email delivery and transmission; (h) DNS (Domain Name Server) propagation; (i) outages elsewhere on the Internet that hinder access to your account. IT-CNP is not responsible for browser or DNS caching that may make your site appear inaccessible when others can still access it. IT-CNP will guarantee only those areas considered under the direct control of IT-CNP.

6. SERVICE LEVEL CREDIT REQUEST PROCEDURES. To receive a credit, the customer must make a request therefore by sending an e-mail message to accounting@it-cnp.com. The e-mail message MUST include the domain or system name of the customer's account in the "Subject" line. Each request in connection with this SLA must include the customer's account number (per IT-CNP 's invoice) and the dates and times of the unavailability of customer's system, and must be received by IT-CNP within ten (10) business days after the customer's system was not available. If the unavailability is confirmed by IT-CNP and is determined to be within the scope of IT-CNP's control, Service Level Credits will be applied within two billing cycles after IT-CNP's receipt of the customer's credit request. Service Level Credits are not refundable and can be used only towards future billing charges. Notwithstanding anything to the contrary herein, the total amount credited to customer in a particular month under this SLA shall not exceed the total hosting fee paid by customer for such month for the affected Services. Credits are exclusive of any applicable taxes charged to customer or collected by IT-CNP. Service Level Credits shall be Customer's sole and exclusive remedy in the event of any failure to meet the Service Levels.

10. USA Commitment To Promote Small Business Participation Procurement Programs

PREAMBLE

IT-CNP, 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 IT-CNP, Inc. at (410) 884-1004.

11. Best Value Blanket Purchase Agreement Federal Supply Schedule

(Insert Customer Name)

In the spirit of the Federal Acquisition Streamlining Act (**ordering activity**) and **IT-CNP, Inc.** 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	IT-CNP, Inc.	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.

****

12. Basic Guidelines For Using "Contractor Team Arrangements"

Federal Supply Schedule Contractors may use “Contractor Team Arrangements” (see FAR 9.6) to provide solutions when responding to a ordering activity requirements.

These Team Arrangements can be included under a Blanket Purchase Agreement (BPA). BPAs are permitted under all Federal Supply Schedule contracts.

Orders under a Team Arrangement are subject to terms and conditions or the Federal Supply Schedule Contract.

Participation in a Team Arrangement is limited to Federal Supply Schedule Contractors.

Customers should refer to FAR 9.6 for specific details on Team Arrangements.

Here is a general outline on how it works:

- The customer identifies their requirements.
- Federal Supply Schedule Contractors may individually meet the customers needs, or -
- Federal Supply Schedule Contractors may individually submit a Schedules “Team Solution” to meet the customer’s requirement.
- Customers make a best value selection.