Federal Supply Service

Authorized Federal Supply Schedule Price List

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

Multiple Award Schedule

FSC Group: Information Technology

Contract Number: 47QTCA19D0037

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

Contract Period: December 12, 2018 – December 11, 2023

Information Technology Solutions & Security, Inc.
105 S Turnberry
Williamsburg, VA 23188-8924
703-966-9229
www.infotech-security.com

Contract Administration Source:

Business Size: Small
Woman Owned (WOSB)

Price list current as of Mass Mod # A826 effective 11.19.2020

Prices Shown Herein are Net (discount deducted)
CUSTOMER INFORMATION

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

<table>
<thead>
<tr>
<th>SINs</th>
<th>Recovery</th>
<th>SIN Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151HACS</td>
<td>54151HACSRC</td>
<td>Geographic Information Systems (GIS) Services</td>
</tr>
<tr>
<td>54151S</td>
<td>54151SRC</td>
<td>Information Technology Professional Services</td>
</tr>
<tr>
<td>OLM</td>
<td>OLMRC</td>
<td>Order-Level Materials (OLM’s)</td>
</tr>
</tbody>
</table>

1b. Identification of the lowest priced model number and lowest unit price for that model for each special item number awarded in the contract. This price is the Government price based on a unit of one, exclusive of any quantity/dollar volume, prompt payment, or any other concession affecting price. Those contracts that have unit prices based on the geographic location of the customer, should show the range of the lowest price, and cite the areas to which the prices apply. Please see attached rate table.

1c. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles, experience, functional responsibility and education for those types of employees or subcontractors who will perform services shall be provided. If hourly rates are not applicable, indicate “Not applicable” for this item. Please see attached labor category descriptions.

2. Maximum order:

<table>
<thead>
<tr>
<th>SINs</th>
<th>Maximum Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151HACS</td>
<td>$500,000</td>
</tr>
<tr>
<td>54151S</td>
<td>$500,000</td>
</tr>
<tr>
<td>OLM</td>
<td>$250,000</td>
</tr>
</tbody>
</table>

3. Minimum order: $100

4. Geographic coverage (delivery area). Domestic

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

   Information Technology Solutions & Security, Inc.
   105 S Turnberry
   Williamsburg, VA 23188-8924

6. Discount from list prices or statement of net price. Government Net Prices (discounts already deducted.)

7. Quantity discounts. 1% > $50k in labor

8. Prompt payment terms. Information for Ordering Offices: Prompt payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions. 1% 15 – Net 30
9. Foreign items (list items by country of origin). **Not Applicable**

10a. Time of delivery. (Contractor insert number of days.) **30 days ARO**

10b. Expedited Delivery. Items available for expedited delivery are noted in this price list. **Contact Contractor**

10c. Overnight and 2-day delivery. **Contact Contractor**

10d. Urgent Requirements. **Contact Contractor**

11. F.O.B. point(s). **Origin**

12a. Ordering address(es):

   **Information Technology Solutions & Security, Inc.**
   105 S Turnberry
   Williamsburg, VA 23188-8924

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

13. Payment address(es):

   **Information Technology Solutions & Security, Inc.**
   105 S Turnberry
   Williamsburg, VA 23188-8924

14. Warranty provision. **Standard Commercial Warranty Terms & Conditions**

15. Export packing charges, if applicable. **Not Applicable**

16. Terms and conditions of rental, maintenance, and repair (if applicable). **Not Applicable**

17. Terms and conditions of installation (if applicable). **Not Applicable**

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

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

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

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

21. Preventive maintenance (if applicable). **Not Applicable**
22a. Special attributes such as environmental attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants). **Not Applicable**

22b. If applicable, indicate that Section 508 compliance information is available on Electronic and Information Technology (EIT) supplies and services and show where full details can be found (e.g. contractor’s website or other location.) The EIT standards can be found at: [www.Section508.gov/](http://www.Section508.gov/). **Not Applicable**

23. Data Universal Number System (DUNS) number. **963023317**

24. Notification regarding registration in System for Award Management (SAM) database. **Information Technology Solutions & Security, Inc. is registered and active in SAM.**
Service Contract Labor Standards: The Service Contract Labor Standards (SCLS), formerly known as the Service Contract Act (SCA), is applicable to this contract as it applies to the entire Multiple Award Schedule (MAS) and all services provided. While no specific labor categories have been identified as being subject to SCLS/SCA due to exemptions for professional employees (FAR 22.1101, 22.1102 and 29 CRF 541.300), this contract still maintains the provisions and protections for SCLS/SCA eligible labor categories. If and/or when the contractor adds SCLS/SCA labor categories to the contract through the modification process, the contractor must inform the Contracting Officer and establish a SCLS/SCA matrix identifying the GSA labor category titles, the occupational code, SCLS/SCA labor category titles and the applicable WD number. Failure to do so may result in cancellation of the contract.

**ESCALATION CHART**

<table>
<thead>
<tr>
<th>SIN(s)</th>
<th>Labor Category</th>
<th>Year 1 12/12/2018 - 12/11/2019</th>
<th>Year 2 12/12/2019 - 12/11/2020</th>
<th>Year 3 12/12/2020 - 12/11/2021</th>
<th>Year 4 12/12/2021 - 12/11/2022</th>
<th>Year 5 12/12/2022 - 12/11/2023</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S</td>
<td>Authorization &amp; Accreditation Mgr</td>
<td>$169.27</td>
<td>$172.65</td>
<td>$176.11</td>
<td>$179.63</td>
<td>$183.22</td>
</tr>
<tr>
<td>54151HACS 54151S</td>
<td>Sr. Security Engineer</td>
<td>$147.02</td>
<td>$149.96</td>
<td>$152.96</td>
<td>$156.02</td>
<td>$159.14</td>
</tr>
<tr>
<td>54151HACS 54151S</td>
<td>Sr. Security Analyst</td>
<td>$127.68</td>
<td>$130.23</td>
<td>$132.84</td>
<td>$135.49</td>
<td>$138.20</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Engineer</td>
<td>$147.02</td>
<td>$149.96</td>
<td>$152.96</td>
<td>$156.02</td>
<td>$159.14</td>
</tr>
<tr>
<td>54151HACS 54151S</td>
<td>Security Engineer</td>
<td>$127.68</td>
<td>$130.23</td>
<td>$132.84</td>
<td>$135.49</td>
<td>$138.20</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Jr. Cyber Security Engineer</td>
<td>$169.27</td>
<td>$172.65</td>
<td>$176.11</td>
<td>$179.63</td>
<td>$183.22</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Security Analyst</td>
<td>$116.07</td>
<td>$118.39</td>
<td>$120.76</td>
<td>$123.17</td>
<td>$125.64</td>
</tr>
<tr>
<td>54151S</td>
<td>IT Systems Engineer</td>
<td>$111.23</td>
<td>$113.46</td>
<td>$115.73</td>
<td>$118.04</td>
<td>$120.40</td>
</tr>
</tbody>
</table>
Authorization & Accreditation Manager

Functional Responsibilities:

- The A&A Manager is responsible for supporting compliance regulations such as the Federal Information Security Management Act (FISMA), National Institute for Science and Technology (NIST) guidelines, Federal Information Processing Standard (FIPS), Defense Information Assurance Certification and Accreditation Program (DIACAP), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI) Data Security Standards, as well as privacy and other requirements for storing US Government and Personal Identifiable Information (PII) in the cloud or other data depository environments.

- The A&A Manager is responsible for innovative solutions and is able to manage a wide range of compliance initiatives. The A&A Manager focuses on the security and compliance of InfoTech’s, as well as their customer’s environment by directing the evaluation of security and control risks and vulnerabilities.

- The A&A Manager is responsible for directing the preparation of detailed System Security Plans and supporting documentation responsive to the customer’s compliance requirements.

- The A&A Manager is responsible for conducting and/or supporting NIST, DIACAP and other Certification and Accreditation and/or Assessment and Authorization efforts.

- The A&A Manager is responsible for evaluating the effectiveness of the established security and privacy controls by conducting internal reviews and continuously monitoring compliance provisions established by laws, regulations and government requirements.

- The A&A Manager is responsible for utilizing skills to drive change across InfoTech and business partners, and coordinate change management efforts to ensure ongoing compliance.

- The A&A Manager is responsible for addressing bottlenecks, providing escalation management, anticipating and making adjustments, balancing the business needs versus technical constraints.

**Minimum Experience:** Minimum 7 years of related experience in security assessments and information assurance, and demonstrated experience in information security.

**Minimum Education:** Bachelor’s Degree in Computer Science, Information Systems, or an engineering
Sr. Security Engineer

Functional Responsibilities:

- The Senior Information Security Engineer is responsible for performing all activities necessary to ensure the compliance of information technology systems in support of the security authorization requirements for the Federal Information System Management Act (FISMA) and the Federal Risk and Authorization Management Program (FedRAMP). Depending on the environment, the Senior Information Security Engineer may be responsible for performing all activities necessary to ensure the compliance of information technology systems with DoD regulations in support of the DoD IA C&A Process (DIACAP)

- The Senior Information Security Engineer is responsible for serving as the lead tester on various Certification and Accreditation (C&A) or Information Assurance (IA) test events assessing IT systems against NIST SP 800-53 security controls or DoD 8500.2 IA controls.

- The Senior Information Security Engineer is responsible for providing direction for the assessment team and especially for junior or less experienced team members

- The Senior Information Security Engineer is responsible for recommending security countermeasures to identified vulnerabilities, keeping in mind the business mission of the organization

- The Senior Information Security Engineer is responsible for leading the management and configuration of vulnerability management tools, including scanners and source code analysis solution

- The Senior Information Security Engineer is responsible for evaluating emerging vulnerabilities and identifies security risks, threats and vulnerabilities

- The Senior Information Security Engineer is responsible for conducting hands-on security testing ad well as automated vulnerability scanning

- The Senior Information Security Engineer is responsible for working with federal regulations related to information security (FISMA, Computer Security Act, The Privacy Act, etc.)

Minimum Experience:

- Minimum of six to eight (6-8) years of experience in enterprise systems with increasing responsibility leading to system engineering experience

- Minimum of five (5) years of demonstrated system engineer experience required

- Minimum of three (3) years of C&A/IA testing experience required

Minimum Education: Bachelor’s Degree in Computer Science, Information Systems Engineering, Management of Information Systems or a related technical discipline, or the equivalent combination of education, professional training or work experience
Sr. Security Analyst

Functional Responsibilities:

• The Senior Security Analyst is responsible for information security policy development and the maintenance and design of security policy education, training, and awareness activities

• The Senior Security Analyst is responsible for defining, documenting, and implementing security strategies, architectures, and procedures, and verifying that the information system and associated infrastructure are properly protected from internal and external threats

• The Senior Security Analyst is responsible for the monitoring and the analysis of antivirus, firewall logs, router logs, syslogs, and network/host-based Intrusion Detection/ Prevention systems (IDS/IPS)

• The Senior Security Analyst is responsible for providing in-depth support for information security incidents including internal violations, hacker attacks, viruses, and system outages

• The Senior Security Analyst is responsible for assisting with the investigation of security breaches, policy violations, and other security incidents

• The Senior Security Analyst is responsible for developing, implementing and maintaining a robust continuous monitoring program

Minimum Experience:

• Minimum eight (8) years of related experience in security administration and information assurance and demonstrated experience in information security and/or IT operations in progressively responsible positions.

• Minimum of three (3) years of experience in the Federal Authorization and Accreditation (A&A) process/Certification and Accreditation (C&A) process, or DoD IA processes system assessments

• Strong knowledge and understanding of federal government or DoD IT policies, theories, principles, practices, procedures, and workforce structure required

• Federal Risk and Authorization Management Program (FedRAMP), NIST and FISMA compliance experience is required

• Experience in security event/alert monitoring employed in a SOC, CSIRT, or on a Security Response Team required

• Experience with the monitoring and the analysis of antivirus, firewall logs, router logs, syslogs, and network/host-based Intrusion Detection/ Prevention systems (IDS/IPS) required

• Hands on experience with various network security services including Cisco firewalls, Virtual Private Network (VPN) and Public Key Infrastructure (PKI) is required
• Experience with security practices on current releases of VMware, ESX, and Citrix XenServer Hypervisors required

Minimum Education: Bachelor’s Degree in Computer Science, Information Systems Engineering, Management of Information Systems, Engineering or a related technical discipline, or the equivalent combination of education, professional training or work experience

**Cyber Security Engineer**

Functional Responsibilities:

• The Cyber Security - Privacy Engineer is responsible for applying his/her security engineering, and privacy expertise to enhance the security and mission of the client’s systems.

• The Cyber Security - Privacy Engineer is responsible for developing technical solutions to help mitigate privacy vulnerabilities and evangelize strong privacy design across the organization.

• The Cyber Security - Privacy Engineer is responsible for providing the first level of IDS monitoring, analysis, and incident response to information security alert events.

• The Cyber Security - Privacy Engineer is responsible for investigating intrusion attempts and performing analysis of exploits.

• The Cyber Security - Privacy Engineer is responsible for performing forensic activities and conducting Reverse Code (RE) Engineering.

**Minimum Experience:**

• Six (6) years of experience with service infrastructure components, infrastructure automation and support services

• Minimum of two (2) years of Forensic analysis experience with EnCase and Revere Code Engineering Experience.

• Minimum of two (2) years of experience with Network security experience, network protocols and packet captures, and Wireshark, SNORT, and other network level security tools

• Minimum of two (2) years of experience configuring and deploying IDS, SIM and vulnerability assessment tools

Minimum Education: Bachelor’s Degree in Computer Science, Information Systems Engineering, Management of Information Systems or a related technical discipline, or the equivalent combination of education, professional training or work experience
Security Engineer

Functional Responsibilities:

- The Information Security Engineer is responsible for assisting with the coordination of information security activities and collaborating with appropriate stakeholders to ensure that information systems are implemented in accordance with the organization’s mission, information security best practices, and Federal and State laws and regulations.

- The Information Security Engineer is responsible for addressing security infrastructure needs, from vetting internal and external applications to defining security policy and overseeing its execution.

- The Information Security Engineer is responsible for multiple daily security operational tasks, evaluation of requests for security changes, performing security research, assisting with security assessments, and managing systems critical to the organization’s security.

- The Information Security Engineer is responsible for assisting in the review and recommending the installation, modification or replacement of hardware or software components and any configuration change(s) that affects security.

- The Information Security Engineer is responsible for assisting in providing oversight and enforcement of security directives, orders, standards, plans and procedures at server sites.

- The Information Security Engineer is responsible for providing ongoing frontline support and guidance to IT support staff and users on a variety of security issues.

- The Information Security Engineer is responsible for developing tests and operating firewalls, intrusion detection systems, enterprise anti-virus systems and software deployment tools.

- The Information Security Engineer is responsible for working with leading firewall, network scanning and intrusion detection products and authentication technologies. Experience working with federal regulations related to information security (FISMA, Computer Security Act, The Privacy Act, etc.)

Minimum Experience:

- Minimum of three to six (3-6) years of experience in enterprise systems with increasing responsibility leading to system engineering experience.

- Minimum of two (2) years of combined IT and security work experience with a broad exposure to infrastructure/network and multi-platform environments.

- Minimum of four (4) years of demonstrated system engineer experience required.

Minimum Education: Bachelor’s Degree in Computer Science, Information Systems Engineering, Management of Information Systems or a related technical discipline, or the equivalent combination of education, professional training or work experience.
Sr. Cyber Security Engineer

Functional Responsibilities:

- The Senior Cyber Security -Privacy Engineer is responsible for performing and leading technical security assessments of commercial, Federal, and DoD clients.

- The Senior Cyber Security - Privacy Engineer is responsible for performing security assessments in accordance with DIACAP and FISMA C&A processes

- The Senior Cyber Security -Privacy Engineer is responsible for leading the efforts to decompose and reverse complex operational systems.

- The Senior Cyber Security -Privacy Engineer is responsible for designing and implementing policies and procedures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction.

- The Senior Cyber Security -Privacy Engineer is responsible for analyzing for weaknesses and vulnerabilities in client systems and networks.

- The Senior Cyber Security -Privacy Engineer is responsible for enhancing trust and confidence in data and IT services, detecting and countering advanced persistent threats, and detecting and countering insider threats.

Minimum Experience:

- Eight (8) years of experience with service infrastructure components, infrastructure automation and support services

- Minimum of two (2) years security or privacy experience, incident handling and intrusion detection

- Minimum of two (2) years of experience with firewall and perimeter protection, forensics, and advanced Hacker techniques.

- Minimum of two (2) years of experience with information assurance/cyber security and vulnerability assessments. Demonstrated understanding and experience in the implementation of DoD and Federal security and IA requirements as outlined in DoDI 8500.2, NIST 800-53, NIST 800-53A controls, and DISA STIGs.

- Minimum of two (2) years of experience with network security features including ACLs, VPN, L2VPN, L3VPN, IPSEC, GRE, within a Cisco platform

- Significant working knowledge of information security principles and practices and at least five or more years technical experience with relevant (Cisco) LAN/WAN security hardware and software including IDS/IPS, ASAs, Routers 28xx, 29xx, 38xx, switches – 29xx, 35xx, 36xx, 37xx, 45xx, 65xx, Nexus 5K&7K, WAPs, Firewalls, VoIP and some experience with the Windows Server platform.
Minimum of two (2) years of experience with enterprise switching/routing and protocols including OSPF, BGP, EIRGP, HSRP and MPLS/VPLS.

Minimum of two (2) years of experience with network and web related protocols (e.g. TCP/IP, UDP, IPSEC, HTTP, HTTPS).

Experience with other Cisco products used in security including Web Security Appliance (WSA), Email Security Appliance (ESA), Identity Services Engine (ISE), Wireless IPS, CSM and NCM is required.

**Minimum Education:** Bachelor’s Degree in Computer Science, Information Systems Engineering, Management of Information Systems or a related technical discipline, or the equivalent combination of education, professional training or work experience.

**Security Analyst**

**Functional Responsibilities:**

- The Security Analyst is responsible for participating in computer forensic activities and incident response.
- The Security Analyst is responsible for supporting computer hardware and systems maintenance.
- The Security Analyst is responsible for identifying risks associated with operations and collaborates in producing reports for senior leaders.
- The Security Analyst is responsible for developing NIST and DIACAP accreditation documentation as needed.
- The Security Analyst is responsible for providing advice and recommendations on Information Assurance (IA) and Certification and Accreditation (C&A) issues.
- The Security Analyst is responsible for assessing the strengths, weaknesses and vulnerabilities of networks and IT in general.
- The Security Analyst is responsible for the monitoring and the analysis of antivirus, firewall logs, router logs, syslog, and network/host-based Intrusion Detection/Prevention systems (IDS/IPS).
- The Security Analyst is responsible for providing recommendations to mitigate computer security vulnerability.
- The Security Analyst is responsible for assisting with the investigation of security breaches, policy, and other security incidents.
- The Security Analyst is responsible for conducting computer system tests and evaluations monthly or as required.
Minimum Experience:

- Minimum four (4) years of related experience in security administration and information assurance and demonstrated experience in information security and/or IT operations in progressively responsible positions.

- Minimum of two (2) years of experience in the Federal Authorization and Accreditation (A&A) process/Certification and Accreditation (C&A) process, or DoD IA processes system assessments

- Minimum two (2) experience with the monitoring and the analysis of antivirus, firewall logs, router logs, syslogs, and network/host-based Intrusion Detection/ Prevention systems (IDS/IPS)

- Strong knowledge and understanding of federal government or DoD IT policies, theories, principles, practices, procedures, and workforce structure required

- Federal Risk and Authorization Management Program (FedRAMP), NIST and FISMA compliance experience is required

- Hands on experience with various network security services including Cisco firewalls, Virtual Private Network (VPN) and Public Key Infrastructure (PKI) is required

- Experience with security practices on current releases of VMware, ESX, and Citrix XenServer Hypervisors is required

Minimum Education: Bachelor’s Degree in Computer Science, Information Systems Engineering, Management of Information Systems, Engineering or a related technical discipline, or the equivalent combination of education, professional training or work experience

**IT Systems Engineer**

Functional Responsibilities:

- The IT Systems Engineer is responsible for demonstrating indepth knowledge of engineering principles and providing expertise, judgment, and analysis for the design, development and implementation of technical systems.

- The IT Systems Engineer is responsible for providing security analysis and consultation services for system and network architecture designs

- The IT Systems Engineer is responsible for resolving highly complex technical issues, integration, and testing.

- The IT Systems Engineer is responsible for verifying and validating complex system designs to ensure conformance with architecture, functional specifications and customer requirements
• The IT Systems Engineer is responsible for recommending design alternatives to improve performance and efficiency of products and/or design procedures

Minimum Experience: Five (5) years of experience in a technical role, working on projects and programs for Government and Industry customers; expert knowledge of Exchange 2007, 2010, Windows OS, SAN technologies (EMC VXE, Lefthand Networks), and experience working with networking protocols such as TCP/IP

Minimum Education: Bachelor’s Degree in Computer Science, Information Systems Engineering, Management of Information Systems, Electrical Engineering, Computer Engineering, or a related technical discipline, or the equivalent combination of education, professional training or work experience