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

**SCHEDULE TITLE:** Multiple Award Schedule (MAS)

Special Item Number (SIN):

- 54151HACS – HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS)
- SIN 54151S - INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES

**FSC Classes/Product Codes:**

- FSC/PSC Class – D301  IT Facility Operation and Maintenance
- FSC/PSC Class - D399  Other Information Technology Services, Not Elsewhere Classified.

**CONTRACT NUMBER:** GS-35F-0689R

**CONTRACT PERIOD:** June 24, 2015 – June 23, 2025

**Modification#:** PO-0021, effective June 24, 2020

For more information on ordering from Federal Supply go to this website: www.gsa.gov/schedules

Securicon, LLC
5400 Shawnee Road, Suite 206
Alexandria, VA 22312
Phone: (703) 914-2780
Fax: (703) 914-2785

**CONTRACTOR’S ADMINISTRATION SOURCE:** Paul W. Hurley, CEO
5400 Shawnee Road, Suite 206
Alexandria, VA 22312
Phone number: (571) 253-6540
Fax number: (703) 914-2785
E-Mail: Paul.Hurley@securicon.com

**BUSINESS SIZE:** Small Business
CUSTOMER INFORMATION:

1a. TABLE OF AWARDED SPECIAL ITEM NUMBERS (SINs)

<table>
<thead>
<tr>
<th>SIN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151HACS</td>
<td>HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS)</td>
</tr>
<tr>
<td>SIN 54151S</td>
<td>INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES</td>
</tr>
</tbody>
</table>

Cooperative Purchasing (STLOC) and Disaster Recovery Purchasing (RC) are available

1b. LOWEST PRICED MODEL NUMBER AND PRICE FOR EACH SIN: See page 9 of 9

(Government net price based on a unit of one)

1c. HOURLY RATES (Services only): See page 9 of 9

2. MAXIMUM ORDER*: $500,000 per order for SINs 54151S & 54151HACS

NOTE TO ORDERING ACTIVITIES: *If the best value selection places your order over the Maximum Order identified in this catalog/pricelist, you have an opportunity to obtain a better schedule contract price. Before placing your order, contact the aforementioned contactor for a better price. The contractor may (1) offer a new price for this requirement (2) offer the lowest price available under this contract or (3) decline the order. A delivery order that exceeds the maximum order may be placed under the schedule contract in accordance with FAR 8.404.

3. MINIMUM ORDER: $100 or Negotiated at the Task Order Level.

4. GEOGRAPHIC COVERAGE: Domestic, 48 states and Washington, DC, and to a CONUS port or consolidation point for orders received from overseas activities.

5. POINT(S) OF PRODUCTION: N/A

6. DISCOUNT FROM LIST PRICES: GSA Net Prices are shown on the attached GSA Pricelist. Negotiated discount has been applied and the IFF has been added.

7. QUANTITY DISCOUNT(S): None

8. PROMPT PAYMENT TERMS: Net 30 days

9. FOREIGN ITEMS: N/A

10a. TIME OF DELIVERY: 30 days or negotiated at the Task Order level.

10b. EXPEDITED DELIVERY: Items available for expedited delivery are noted in this price list or negotiated at the task order level.

10c. OVERNIGHT AND 2-DAY DELIVERY: Overnight and 2-day delivery are available. Contact the Contractor for rates.

10d. URGENT REQUIREMENTS: Agencies can contact the Contractor’s representative to affect a faster delivery. Customers are encouraged to contact the contractor for the purpose of requesting accelerated delivery.

11. FOB POINT: Destination

12a. ORDERING ADDRESS: Same as contractor address if different
12b. ORDERING PROCEDURES: Ordering activities shall use the ordering procedures described in Federal Acquisition Regulation 8.405-3 when placing an order or establishing a BPA for supplies or services. The ordering procedures, information on Blanket Purchase Agreements (BPA’s) and a sample BPA can be found at the GSA/FSS Schedule Homepage (fss.gsa.gov/schedules).

13. PAYMENT ADDRESS: Same as contractor address if different

14. WARRANTY PROVISION: N/A

15. EXPORT PACKING CHARGES: N/A

16. TERMS AND CONDITIONS OF RENTAL, MAINTENANCE, AND REPAIR (IF APPLICABLE): N/A

17. TERMS AND CONDITIONS OF INSTALLATION (IF APPLICABLE): N/A

18a. TERMS AND CONDITIONS OF REPAIR PARTS INDICATING DATE OF PARTS PRICE LISTS AND ANY DISCOUNTS FROM LIST PRICES (IF AVAILABLE): N/A

18b. TERMS AND CONDITIONS FOR ANY OTHER SERVICES (IF APPLICABLE): N/A

19. LIST OF SERVICE AND DISTRIBUTION POINTS (IF APPLICABLE): N/A

20. LIST OF PARTICIPATING DEALERS (IF APPLICABLE): N/A

21. PREVENTIVE MAINTENANCE (IF APPLICABLE): N/A

22a. SPECIAL ATTRIBUTES SUCH AS ENVIRONMENTAL ATTRIBUTES (e.g. recycled content, energy efficiency, and/or reduced pollutants): N/A

22b. Section 508 Compliance for Electronic and Information Technology (EIT): Section 508 compliance information on the supplies and services in this contract are available at the following website address (URL): www.securicon.com

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

23. Unique Entity Identifier (UEI): FT29M6JLNQ44

24. NOTIFICATION REGARDING REGISTRATION IN SYSTEM FOR AWARD MANAGEMENT (SAM) DATABASE: Contractor has an Active Registration in the SAM database.
JOB TITLE: SECURITY ENGINEER

**Minimum/General Experience:** Three (3) years of technical experience performing network, system and application security tasks, including security assessments, and developing risk mitigation strategies, including secure implementation of firewalls, routers, switches, hubs, proxy servers, and security servers.

**Functional Responsibility:** Work with clients to implement technical solutions to support client requirements in solving complex network, application and system security problems. Typical focus areas include security, analytical and engineering solutions based on information security/assurance policy doctrine and regulations. Responsibilities include: Developing and engineering secure systems, Analyzing system/security requirements, Conducting security and risk assessments, performing analysis and troubleshooting network security, Establishing access controls (firewalls, filters), encryption/authentication, and system monitoring, Performing on secure operating systems, workstations, data management, networks, web technology, protocols firewalls, and encryption, and Key management distributed authentication devices.

**Minimum Education:** A Bachelor's degree in Computer or Information Science or an equivalent combination of education, training, and work experience.

JOB TITLE: SENIOR SECURITY ENGINEER

**Minimum/General Experience:** Five (5) years’ technical experience leading and conducting network, system and application security tasks, including security assessments, and developing risk mitigation strategies, including secure implementation of firewalls, routers, switches, hubs, proxy servers, and security servers.

**Functional Responsibility:** Work with clients to determine security and assessment requirements, design and supervise penetration testing and security assessments, as well as participate in the development of proprietary security assessment tools, develop and recommend technical solutions to support client requirements in solving complex network, application and system security problems. Typical focus areas include security analytical and engineering solutions based on information security/assurance policy, doctrine and regulations. Responsibilities include: Developing and engineering secure systems, Analyzing system/security requirements, Leading and conducting security assessments, including penetration testing and vulnerability and risk assessments, Performing analysis and troubleshooting network security, Establishing access controls (firewalls, filters), encryption/authentication, and system monitoring, Performing audits and configuration of secure operating systems, workstations, data management, networks, web technology, protocols firewalls, and encryption, and Key management distributed authentication devices

**Minimum Education:** A Bachelor's degree in Computer or Information Science or an equivalent combination of education, training, and work experience.

JOB TITLE: SECURITY ANALYST

**Minimum/General Experience:** Three years of technical experience conducting network, system and application vulnerability and risk assessments, including penetration testing, and developing risk mitigation strategies. Strong problem solving and resolution skills. Knowledgeable of secure implementation principles for firewalls, routers, switches, hubs, proxy servers, and security servers.
**Functional Responsibility:** Work with clients to determine security and assessment requirements, design security and risk assessment solutions, as well as participate in the development of proprietary security and risk assessment tools, develop and recommend technical solutions to support client requirements in solving complex network, application and system security problems. Typical focus areas include security, analytical and engineering solutions based on information security/assurance policy doctrine and regulations. Responsibilities include: Developing and engineering secure solutions for systems, analyzing system/security requirements, conducting security and risk assessments, performing analysis and troubleshooting network security, establishing access controls (firewalls, filters), encryption/authentication, and system monitoring, performing assessments, or implementing secure operating systems, workstations, data management, networks, web technology, protocols firewalls, and encryption and key management distributed authentication devices.

**Minimum Education:** A Bachelor’s degree in Computer or Information Science or an equivalent combination of education, training, and work experience is required for this position.

**JOB TITLE: SENIOR SECURITY TECHNICAL WRITER**

**Minimum/General Experience:** Minimum of six (6) years experience in the preparation of written instructions, procedures, reports, minutes, hardware/software descriptions, and other technical documentation. Two (2) years must be specifically in support of security assessments, security architecture reviews, and security policy development.

**Functional Responsibility:** Apply comprehensive knowledge of technical editing and writing, as well as network and computer systems to create or review/edit highly technical security documentation, to include security and risk assessments, security architecture documentation and other security deliverables. To ensure they are meaningful and useful to a consulting client. Specific responsibilities include: assists in the analysis of vulnerability data to create security and risk analysis reports, creates templates and worksheets for Security Engineers to use in data collection during technical vulnerability assessments and risk analyses, creates standards and templates to standardize types and format of findings and recommendations documentation to the consulting client, and edits and formats draft reports submitted by security engineers to ensure that they are consistent and accurately portray the findings of the consulting effort.

**Minimum Education:** A Bachelor's degree in Computer or Information Science or an equivalent combination of education, training, and work experience.

**JOB TITLE: PROGRAM MANAGER**

**Minimum/General Experience:** Ten (10) years of progressive experience in managing, directing, and implementing information technology projects. Experienced in managing a diverse group of functional activities, subordinate groups of technical and administrative personnel. Experienced in management and control of large funds and resources, and demonstrated capability in managing complex, multi-task commercial and government contracts. Securicon’s Program Managers are our most senior and valuable employees and are responsible for directing corporate business units and business areas.

**Functional Responsibility:** For a given task order, the Program Manager serves as Securicon’s single task manager, and will be Securicon’s authorized interface with the government’s Contracting officer’s Representative (COR), other government management personnel, and customer agency representatives. The Program Manager is responsible for formulating and enforcing work standards, schedules, and communicating policies, purposes, and goals to subordinates and subcontractors. In short, the Program Manager is responsible for the overall contract performance. Securicon’s Program Managers manage information technology services and operations for one or more projects, organize resources to support multiple concurrent projects and manages the execution of multiple concurrent projects. The Program Manager conducts oral and written communications with all levels of management for planning and control of projects and communicates with Government management personnel, other contract personnel, and customer agency representatives. The Program Manager also reviews work of subordinate Project Managers, including subcontractors. The Program Manager will be an employee of Securicon.

**Minimum Education:** Bachelor’s Degree in Business, Engineering, Computer Science, Information Systems, Social Science, or other related analytical, scientific, or technical disciplines.
**JOB TITLE: SENIOR SUBJECT MATTER EXPERT**

**Minimum/General Experience:** Senior Subject Matter Experts (SSMEs) have fifteen (15) years of progressive experience in supporting large information technology projects related to the individual’s subject matter expertise. These personnel are often corporate officers, leaders, and directors with many years of experience, and are nationally and/or internationally acknowledged experts in either functional domains (e.g., finance, personnel, acquisition, etc.) or technical disciplines (e.g., computer security, network engineering, etc.). They have advanced degrees, and all have extensive experience as technical leaders and/or senior Project Managers.

**Functional Responsibility:** Senior Subject Matter Experts (SSMEs) serve as technical experts in areas relevant to a particular project. SSMEs produce and/or review substantive and/or complex technical documentation reflecting detailed knowledge of technical areas as identified in the statement of work. Documentation subjects include, but are not limited to, systems design, system architecture, feasibility studies, and system specifications.

**Minimum Education:** Master’s Degree in Business, Engineering, Computer Science, Information Systems, Social Science, or other related analytical, scientific, or technical disciplines.

---

**LABOR CATEGORIES FOR SIN 54151HACS**

**JOB TITLE: CYBER SECURITY ENGINEER**

**Minimum/General Experience:** Three (3) years of technical experience conducting network, system and application vulnerability and risk assessments, including penetration testing, and developing risk mitigation strategies. Strong problem solving and resolution skills. Comprehensive knowledge of secure implementation principles for firewalls, routers, switches, hubs, proxy servers, and security servers.

**Functional Responsibility:** Work with clients to conduct penetration testing and vulnerability assessment requirements, design penetration testing and security assessments, as well as participate in the development of proprietary security assessment tools, develop and recommend technical solutions to support client requirements in solving complex network, application and system security problems. Typical focus areas include security, analytical and engineering solutions based on information security/assurance policy doctrine and regulations. Responsibilities include: Developing and engineering secure systems, Analyzing system/security requirements, Conducting security assessments, including penetration testing and vulnerability and risk assessments, Performing analysis and troubleshooting network security, Establishing access controls (firewalls, filters), encryption/authentication, and system monitoring, Performing on secure operating systems, workstations, data management, networks, web technology, protocols firewalls, and encryption, and Key management distributed authentication devices.

**Minimum Education:** A Bachelor's degree in Computer or Information Science or an equivalent combination of education, training, and work experience.

---

**JOB TITLE: CYBER SENIOR SECURITY ENGINEER**

**Minimum/General Experience:** Five (5) years’ experience leading and conducting penetration and vulnerability assessment tasks for networks, systems and applications, as well as developing risk mitigation strategies. The Cyber Senior Security Engineer is also experienced in managing, designing, and implementing technical security solutions, including firewalls, virtual private networks, and intrusion detection systems; and/or experienced in application code reviews.

**Functional Responsibility:** Work with clients to determine security and assessment requirements and scope, design and supervise penetration testing and security assessments, as well as participate in the development of proprietary security assessment tools, develop and recommend technical solutions to support client requirements in solving complex network, application and system security problems. Typical focus areas include security analytical and engineering solutions based on information security/assurance policy, doctrine and regulations. Responsibilities include: Developing and engineering secure systems, Analyzing system/security requirements, Leading and conducting security assessments, including penetration testing and vulnerability and risk assessments, Performing analysis and troubleshooting network security, Establishing access controls (firewalls, filters), encryption/authentication, and system monitoring, Performing audits and configuration of secure operating systems, workstations, data management, networks, web technology, protocols firewalls, and encryption, and Key management distributed authentication devices.

**Minimum Education:** A Bachelor's degree in Computer or Information Science or an equivalent combination of education, training, and work experience.
JOB TITLE: CYBER SECURITY ANALYST

Minimum/General Experience: Three years of technical experience conducting network, system and application vulnerability and risk assessments, including penetration testing, and developing risk mitigation strategies. Strong problem solving and resolution skills. Knowledgeable of secure implementation principles for firewalls, routers, switches, hubs, proxy servers, and security servers.

Functional Responsibility: Work under supervision of senior leadership within Securicon security assessment teams to conduct penetration testing and security assessments, as well as participate in the development of proprietary security assessment tools, develop and recommend technical solutions to support client requirements in solving complex network, application and system security problems. Typical focus areas include security, analytical and engineering solutions based on information security/assurance policy doctrine and regulations. Responsibilities include: developing and engineering secure systems, analyzing system/security requirements, conducting security assessments, including penetration testing and vulnerability and risk assessments, Performing analysis and troubleshooting network security. Establishing access controls (firewalls, filters), encryption/authentication, and system monitoring, performing assessments of secure operating systems, workstations, data management, networks, web technology, protocols firewalls, and encryption and key management distributed authentication devices.

Minimum Education: A Bachelor’s degree in Computer or Information Science or an equivalent combination of education, training, and work experience is required for this position.

JOB TITLE: CYBER SENIOR SECURITY TECHNICAL WRITER

Minimum/General Experience: Minimum of six (6) years experience in the preparation of written instructions, procedures, reports, minutes, hardware/software descriptions, and other technical documentation. Two (2) years must be specifically in support of vulnerability and penetration security assessments, security architecture reviews, security policy development, and other security testing.

Functional Responsibility: Apply comprehensive knowledge of technical editing and writing, as well as network and computer system security to communicate the results of highly technical security vulnerability and penetration assessments and recommendations into meaningful written communication to a consulting client. Specific responsibilities include: assists in the analysis of vulnerability data to create vulnerability assessments and risk analysis reports, creates templates and worksheets for Security Engineers to use in data collection during technical vulnerability assessments and risk analyses, creates standards and templates to standardize types and format of findings and recommendations documentation to the consulting client, and edits and formats draft reports submitted by security engineers to ensure that they are consistent and accurately portray the findings of the consulting effort.

Minimum Education: A Bachelor's degree in Computer or Information Science or an equivalent combination of education, training, and work experience.

JOB TITLE: CYBER PROGRAM MANAGER

Minimum/General Experience: Ten (10) years of progressive experience in managing, directing, and implementing cyber security projects. Experienced in managing a diverse group of functional cyber security activities, subordinate groups of technical and administrative personnel, especially involving cyber penetration and vulnerability assessments. Experienced in management and control of large funds and resources, and demonstrated capability in managing complex, multi-task commercial and government cyber security contracts. Securicon’s Program Managers are our most senior and valuable employees and are responsible for directing corporate business units and business areas.

Functional Responsibility: For a given task order, the Program Manager serves as Securicon’s single contract manager, and will be Securicon’s authorized interface with the government’s Contracting officer’s Representative (COR), other government management personnel, and customer agency representatives. The Program Manager is responsible for formulating and enforcing work standards, schedules, and communicating policies, purposes, and goals to subordinates and subcontractors. In short, the Program Manager is responsible for the overall contract performance. Securicon’s Program Managers manage cyber security services and operations for one or more projects, organize resources to support multiple concurrent projects and manages the execution of multiple concurrent projects. The Program Manager conducts
oral and written communications with all levels of management for planning and control of cyber security projects and communicates with Government management personnel, other contract personnel, and customer agency representatives. The Program Manager also reviews work of subordinate Project Managers, including subcontractors. The Program Manager will be an employee of Securicon.

**Minimum Education:** Bachelor’s Degree in Business, Engineering, Computer Science, Information Systems, Social Science, or other related analytical, scientific, or technical disciplines.

**JOB TITLE: CYBER SENIOR SUBJECT MATTER EXPERT**

**Minimum/General Experience:** Senior Subject Matter Experts (SSMEs) have fifteen (15) years of progressive experience in supporting high value and high visibility cyber security projects related to the individual’s subject matter expertise. These personnel are often corporate officers, leaders, and directors with many years of experience, and are nationally and/or internationally acknowledged experts in either functional domains (e.g., industrial control system cyber security, chief information security officer, etc.). They have advanced degrees, and all have extensive experience as technical leaders, senior industry leaders or nationally/internationally recognized experts and spokespersons within their area of cyber security expertise.

**Functional Responsibility:** Senior Subject Matter Experts (SSMEs) serve as technical experts in areas relevant to a particular project. SSMEs produce and/or review substantive and/or complex technical documentation reflecting detailed knowledge of technical areas as identified in the statement of work. Documentation subjects include, but are not limited to, systems design, system architecture, feasibility studies, and system specifications.

**Minimum Education:** Master’s Degree in Business, Engineering, Computer Science, Information Systems, Social Science, or other related analytical, scientific, or technical disciplines.
**SECURICON, LLC’S AUTHORIZED HOURLY RATES**

<table>
<thead>
<tr>
<th>SINs</th>
<th>Labor Categories</th>
<th>GSA Hourly Rate*</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151HACS, 54151S</td>
<td>Cyber Security Engineer, Security Engineer</td>
<td>$155.64</td>
</tr>
<tr>
<td>54151HACS, 54151S</td>
<td>Cyber Senior Security Engineer, Senior Security Engineer</td>
<td>$179.70</td>
</tr>
<tr>
<td>54151HACS, 54151S</td>
<td>Cyber Security Analyst, Security Analyst</td>
<td>$128.46</td>
</tr>
<tr>
<td>54151HACS, 54151S</td>
<td>Cyber Senior Security Technical Writer, Senior Security Technical Writer</td>
<td>$122.17</td>
</tr>
<tr>
<td>54151HACS, 54151S</td>
<td>Cyber Program Manager, Program Manager</td>
<td>$207.25</td>
</tr>
<tr>
<td>54151HACS, 54151S</td>
<td>Cyber Senior Subject Matter Expert, Senior Subject Matter Expert</td>
<td>$249.22</td>
</tr>
</tbody>
</table>

**SIN 54151HACS includes the following subcategories**
- Risk and Vulnerability Assessments (RVA)
- Penetration Testing
- High Value Assets (HVA)
- Incident Response
- Cyber Hunt