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: GSAAAdvantage.gov

SecureSoft Technologies, LLC
Unlocking Tailored Results

Contract Number: GS35F348GA
Contract Period: April 4, 2017 through April 3, 2022

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

Schedule Title: Multiple Award Schedule
Federal Supply Group: Information Technology

Contractor: Securesoft Technologies LLC
85 S Bragg Street, Suite 600-F
Alexandria, VA 22312-2797

Business Size: Small Business

Telephone: 240-770-2097
Web Site: www.secsofttech.com
E-mail: waddai@secsofttech.com
Contract Administration: William Addai, President/CEO

Pricelist current through Modification #PS-0015, dated January 14, 2021.
CUSTOMER INFORMATION:

1a. Table of Awarded Special Item Number(s) with appropriate cross-reference to page numbers:

<table>
<thead>
<tr>
<th>SIN</th>
<th>SIN Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151HACS &amp; 54151HACSRC</td>
<td>Highly Adaptive Cybersecurity Services (HACS)</td>
</tr>
<tr>
<td>54151S &amp; 54151SRC</td>
<td>Information Technology Professional Services</td>
</tr>
<tr>
<td>OLM &amp; OLMRC</td>
<td>Order Level Materials</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. See Pricing Page 5.

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. See Labor Category Descriptions Page 6.

2. Maximum Order: For SINs 54151HACS and 54151S - $500,000.00
For SIN OLM - $250,000.00

3. Minimum Order: $100.00

4. Geographic Coverage (delivery Area): Domestic

5. Point(s) of production (city, county, and state or foreign country):
Securesoft Technologies LLC
85 S Bragg Street, Suite 600-F
Alexandria, VA 22312-2797

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

7. Quantity discounts: 1% for orders greater than $1,000,000.00.

8. Prompt payment terms: Net 30 days
Information for Ordering Offices: Prompt payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions

9. Foreign items (list items by country of origin): None

10a. Time of Delivery (Contractor insert number of days): Negotiated at time of delivery order for services.

10b. Expedited Delivery. The Contractor will insert the sentence “Items available for expedited delivery are noted in this price list.” under this heading. The Contractor may use a symbol of its choosing to highlight items in its price list that have expedited delivery: Negotiated at time of delivery order for services.
10c. Overnight and 2-day delivery. The Contractor will indicate whether overnight and 2-day delivery are available. Also, the Contractor will indicate that the schedule customer may contact the Contractor for rates for overnight and 2-day delivery: Contact Contractor

10d. Urgent Requirements. The Contractor will note in its price list the “Urgent Requirements” clause of its contract and advise agencies that they can also contact the Contractor’s representative to effect a faster delivery: Contact Contractor

11. F.O.B Points(s): Destination

12a. Ordering Address(es): Securesoft Technologies LLC
85 S Bragg Street, Suite 600-F
Alexandria, VA 22312-2797

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

13. Payment address(es): Securesoft Technologies LLC
85 S Bragg Street, Suite 600-F
Alexandria, VA 22312-2797

14. Warranty provision: N/A

15. Export Packing Charges (if applicable): 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

18. Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices (if applicable): N/A

18a. 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. Environmental attributes, e.g., recycled content, energy efficiency, and/or reduced pollutants: N/A

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/.

23. Data Universal Numbering System (DUNS) number: 173563847
24. Notification regarding registration in System for Award Management (SAM) database:
Registered.
GSA Awarded Pricing for SIN 54151S & SIN 54151HACS

The rates are inclusive of the Industrial Funding Fee (IFF) of 0.75%.

<table>
<thead>
<tr>
<th>SIN</th>
<th>Labor Category</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151HACS</td>
<td>Cyber Security Capability Integration SME - Level 4</td>
<td>$217.63</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Engineer - Level 2</td>
<td>$90.84</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Engineer - Level 3</td>
<td>$96.77</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Engineer - Level 4</td>
<td>$123.43</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Manager - Level 3</td>
<td>$123.43</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Network Architect &amp; Integration SME - Level 4</td>
<td>$217.63</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Network Design &amp; Integration SME - Level 4</td>
<td>$236.98</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Service Desk Support - Tier 2</td>
<td>$66.16</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Systems Engineer - Level 3</td>
<td>$96.77</td>
</tr>
<tr>
<td>54151S</td>
<td>Information/Cyber Security Subject Matter Expert Level 1</td>
<td>$153.27</td>
</tr>
<tr>
<td>54151S</td>
<td>Senior Information Systems Security Engineer</td>
<td>$89.77</td>
</tr>
<tr>
<td>54151S</td>
<td>Senior Web Developer</td>
<td>$87.15</td>
</tr>
</tbody>
</table>

Service Contract Labor Standards: The Service Contract Labor Standards (SCLS) are applicable to this contract as it applies to the entire Consolidated MAS Schedule and all services provided. While no specific labor categories have been identified as being subject to SCLS 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 eligible labor categories. If and/or when the contractor adds SCLS labor categories/employees to the contract through the modification process, the contractor must inform the Contracting Officer and establish a SCLS matrix identifying the GSA labor category titles, the occupational code, SCLS labor category titles and the applicable WD number. Failure to do so may result in cancellation of the contract.
Labor Category Descriptions

SIN 54151HACS

**Cyber Security Capability Integration SME -Level 4**

**Functional Responsibilities:** Manages mission-critical tasks across multiple functional areas. Provides leadership for key tasks and resolves problems for major functional areas through assessment of complex and technically challenging situations. Has domain and expert technical knowledge of functional areas and programmatic knowledge practice-wide. Manages, controls, and directs the activities of multiple functional areas through program and Project Managers (PMs) / Task Managers (TM)s with overall responsibility for the implementation of project phases. Is responsible for decision making that has long-term impact on meeting major project performance objectives.

Contributes overall strategic vision and integrates a broad range of solutions in support of client requirements for IT projects. Formulates and defines system scope and objectives, develops, or modifies processes to solve complex problems for computer systems and business and electronic interfaces to achieve desired results through the use of innovative technologies. Develops and applies advanced engineering and design methods, theories, and research techniques in the investigation and solution of complex and advanced system requirements, hardware/software interfaces and applications, and solutions. Responsible for design, development, engineering, integration, and architecture. This senior title manages, plans, and conducts major phases of significant projects.

Design and Development disciplines include, but are not limited to: Systems and Network Architecture Design And Analysis; Systems Design Engineering and Integration; Network Engineering; Enterprise Resource Planning (ERP) Integration; Systems Development; Mission Engineering; Technology Planning; Applications Development and Programming; Certification and Authentication; Data Conversion; Data Warehousing; Database Design and Administration; Enterprise Architecture (EA) Integration; Information Assurance (IA); Biometrics; Identity Protection and Access Management; Independent Verification and Validation (IV&V); Continuity Operational Planning And Disaster Recovery; Public Key Infrastructure (PKI) Development; Quality Assurance (QA) System Performance; and Test and Validation.

**Minimum Experience:** Must have a minimum of 10 years of experience in the field.
Cyber Security Engineer - Level 2

**Functional Responsibilities:** Designs, tests, and implements secure operating systems, applications, Department of Defense (DoD) networks, security monitoring, tuning, and management of IT security systems and applications, incident response, digital forensics, data loss prevention, and eDiscovery actions. Reviews vulnerability scans such as Assured Compliance Assessment Solution (ACAS) and implements or guide implementation of resolutions to associated finding including Plan of Action and Milestones (POAMs) based on Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) guidelines and DoD Cloud Computing Security Requirements Guide (SRG). Conducts risk and vulnerability assessment at the network, system, and application levels. Conducts threat modeling exercises. Develops and implements security controls and formulates operational risk mitigations along with assisting in security awareness programs. Involved in a wide range of security issues including: architectures, firewalls, electronic data traffic, and network access. Researches, evaluates, and recommends new security tools, techniques, and technologies and introduces them to the enterprise in alignment with IT security strategy. Prepares security reports to regulatory agencies. Audits and manages access management.

Reviews Cybersecurity related artifacts and develop a plan for updating Program cybersecurity artifacts. Performs reviews of existing and future technologies and standards, and advises the Senior Management of the implications that such technologies and standard may have on Customer IT security environments. Tracks various Operational and Maintenance (O&M) activities and projects to ensure a timely deliverables, and improve efficiencies. Serves as a liaison between multiple internal and customer divisions. Formulates operational procedures for inter-divisional communications. Collaborates with Change, Problem, and Release Management Personnel for security impacts to the environment. Reviews new security solutions, designs, and specifications to validate they are ready for existing security operations environment. Conducts technical policy and contract reviews as requested and advise the Senior Management accordingly.

Provides an accounting of hardware and Software inventory. Reviews all applicable Change Request, and attend Change Control Board (CCB) meetings. Remains current with trends in cybersecurity technologies, processes, and methods that can improve the Customer IT infrastructure security posture, the efficiency and effectiveness of security operations, and the quality of security services provided, and advises Customer accordingly. Reviews system audit logs and has strong background in Security Information and Event (SIEM) tools and analysis.

**Minimum Experience:** Must have a minimum of 4 years of experience in the field.
Cyber Security Engineer - Level 3

Functional Responsibilities: Has considerable security engineering and cyber security exposure and experience in designing, testing, and implementing secure operating systems, applications, security monitoring, loss prevention, and eDiscovery actions. Reviews vulnerability scans such as ACAS/Nessus and implements resolutions to associated findings including POAMs based on DISA STIGs guidelines and DoD SRG. Conducts risk and vulnerability assessment at the network, system, and application level. Develops and implements security controls and formulates operational risk mitigations. Will be involved in a wide range of security issues including architectures, firewalls, electronic data traffic, and network access. Researches, evaluates, and recommends new security tools, techniques, and technologies and introduces them to the enterprise in alignment with IT security strategy. Regularly prepares security reports as well as audits and manages access management. Must have on the job experience with the Risk Management Framework (RMF), have Authorization and Assessment Experience, as well as research and analytical skills and ability to pinpoint significant patterns related to cyber threats. Works well independently as well as in dynamic, team-oriented environments. Possesses strong organizational, presentation, communication, and critical thinking skills. Tasks and responsibilities include:

- Understands and applies security engineering concepts to resolve and mitigate risks.
- Reviews IA related artifacts, develops a plan for updating Program IA artifacts, and updates and/or create cyber security artifacts including compelling evidence artifacts.
- Provides an accounting of hardware and Software inventory.
- Understands cybersecurity architectures.
- Reviews all applicable Change Request and attends CCB meetings.
- Identifies applications and operating systems machine data and logs for SIEM analysis.
- Conducts RMF activities and related tasks.
- Develops and maintains RMF package, including maintaining the system/program artifacts (compelling evidence) and assigning security controls based on the system categorization.
- Implements and validates assigned Security Controls including execution of the System Security Plan (SSP), coordination of related activities, and supporting continuous monitoring activities.

Minimum Experience: Must have a minimum of 6 years of experience in the field.
Cyber Security Engineer - Level 4

Functional Responsibilities: Possesses expertise in security engineering and information/cyber security particularly in RMF, Authorization and Assessment Experience, Security Architectures, and vulnerability assessments including penetration testing, incident response, cyber hunt activities, as well as research and analytical skills and ability to pinpoint significant patterns related to cyber threats. Possess significant experience in the following areas:

- Understands and applies security engineering concepts to resolve and mitigate risks.
- Collects and documents evidentiary material for security control implementations.
- Writes, documents, and provides first level of approval for Cybersecurity document/artifacts in support of Authority to Operate (ATO); example of artifacts include: Continuity of Operations Plan, Security Concept of Operations, and Incident Response Plan.
- Analyzes and provides first level of approval for all DISA STIGs and SRG documentation.
- Reviews and provides first level of approval for the development and implementation of security controls and formulates operational risk mitigations.
- Reviews vulnerability scans such as ACAS/Nessus and implements resolutions to associated findings including POAMs based on DISA STIGs guidelines and DoD SRG.
- Conducts risk and vulnerability assessment at the network, system, and application level.
- Involved in a wide range of security issues including architectures, firewalls, electronic data traffic, and network access.
- Researches, evaluates, and recommends new security tools, techniques, and technologies and introduces them to the enterprise in alignment with IT security strategy.
- Performs system security architecture reviews.
- Designs penetration tests based on client requirements.
- Regularly prepares security reports as well as audits and manages access management. Works well independently as well as in dynamic, team-oriented environments.
- Possesses strong organizational, presentation, communication, and critical thinking skills.

Minimum Experience: Must have a minimum of 8 years of experience in the field.
**Cyber Security Manager - Level 3**

**Functional Responsibilities:** Provides managerial and technical direction for problem definition, analysis, requirements development, and implementation for complex to extremely complex systems in the subject matter area of Information Security. Makes recommendations and advises on organization-wide system improvements, optimization, or maintenance efforts in the following specialties: information systems security; architecture; automation; communications protocols; risk management/electronic analysis; software; lifecycle management; software development methodologies; and test and evaluation.

Provides final recommendations in risk assessment during the System Assessment and Authorization (otherwise known as Certification and Accreditation) process. Designs, develops, implements, and integrates IA architecture, system, or system component for use within data center, network, and enclave environments. Plays a pivotal role in information systems risk assessments and designs security countermeasures to mitigate identified risks. Ensures that the architecture and design of Client’s Information Systems (IS) are functional and secure.

As necessary, designs and develops IA or IA enabled products, interfaces specifications, and approaches to secure the environment. Applies knowledge of existing IA policy, procedures, and structures to design, develop, and implement systems, components, or architectures. Ensures that the implementation of security designs properly mitigate identified threats. Documents system security design features and provides input to implementation plans and Standard Operating Procedures (SOPs).

**Minimum Experience:** Must have a minimum of 8 years of experience in the field.
**Cyber Security Network Architect & Integration SME - Level 4**

**Functional Responsibilities:** Manages mission-critical Network tasks across multiple functional areas. Provides leadership for key Networking tasks and resolves problems for major functional areas through assessment of complex and technically challenging situations. Implements key network components supporting cyber security architecture. Possesses expertise in implementation of and Next Generation Firewalls. Designs and establishes networking environment by designing system configuration, directing system installation, and defining, documenting, and enforcing system standards.

Designs and implements new solutions and improve resilience of the current environment. Maximizes network performance by monitoring performance, troubleshooting network problems and outages, scheduling upgrades, and collaborating with network architects on network optimization. Undertakes data network fault investigations in local and wide area environments using information from multiple sources. Secures network systems by establishing and enforcing policies, and defining and monitoring access. Supports and administers firewall environments in line with IT security policy.

Reports network operational status by gathering and prioritizing information and managing projects. Upgrades data network equipment to the latest stable firmware releases. Configures routing, switching equipment, and firewalls. Provides on-site support to local engineers and End Users (EUs) / customers during installation. Provides on-site troubleshooting and fault finding if issues occur upon initial installation. Includes network and security design work. Possess Cisco Certified Internetwork Expert (CCIE) Routing and Switching Certification (400-101) and/or Cisco Certified Design Expert (352-101), CompTIA Security +. Possesses specialized experience with Local Area Networks (LANs), Wide Area Networks (WANs), Transmission Control Protocol/Internet Protocol (TCP/IP), Firewalls, Routers, and Switches. Has working experience installing rack mounted equipment including basic cabling to peripheral devices and power distribution units. Possess experience with network and infrastructure monitoring to ensure efficient use of power and cooling resources. Possesses professional oral and written communication skills, excellent problem solving, and analytical skills and ability to work independently and on global teams.

**Minimum Experience:** Must have a minimum of 10 years of experience in the field.
**Cyber Security Network Design & Integration SME - Level 4**

**Functional Responsibilities:** Cisco Certified Network Professional (CCNP) or CCIE with hands on experience designing managing, sustaining, and configuring networks as well as Virtual networking (to include VMWare). Possess Cisco Hyperconverged Infrastructure (HCI) implementation experience and NetFlow Configurations. Has working knowledge to tools like Gigamon, Cyber Security Operations Center (CSOC) operations, Viavi, Red Seal, IBM QRadar, and Rapid 7 (Nexpose and Metasploit).

**Minimum Experience:** Must have a minimum of 10 years of experience in the field.

---

**Cyber Security Service Desk Support - Tier 2**

**Functional Responsibilities:** Provides fast and useful technical assistance on information/Computer systems. Responds to queries on basic - moderately complex technical issues and offer advice to solve them. Is customer-oriented and has the patience to deal with difficult customers. Serves as the first/second Point-Of-Contact (POC) for customers seeking technical assistance over the phone or email. Performs remote troubleshooting through diagnostic techniques and pertinent questions. Determines the best solution based on the issue and details provided by customers. Walks the customer through the problem-solving process. Directs unresolved issues to the next level of support personnel. Provides accurate information on IT products or services. Records events and problems and their resolution in logs. Follows-up and updates customer status and information. Passes on any feedback or suggestions by customers to the appropriate internal teams. Identifies and suggests possible improvements on procedures. Possesses working knowledge of office automation products, databases, and remote control tools/applications. Has working knowledge of computer systems, mobile devices, and other technical products. Has the ability to diagnose and resolve basic-moderately complex technical issues. Proficient in English and has excellent communication skills.

**Minimum Experience:** Must have a minimum of 3 years of experience in the field.
Cyber Security Systems Engineer - Level 3

Functional Responsibilities: Provides support of the design, execution, and oversight of IT projects including direct experience in the design and development of integrated software and hardware solutions in the private or public sector. Supports business case analysis, such as and identification of alternative solutions and resulting business impacts. Performs in a role of a requirements to make recommendations for solutions or improvements that can be accomplished through new technology or alternative uses of existing technology. Analyzes and communicates stakeholder needs by translating business requirements into software requirements. Functions as liaison between business stakeholders, such as management, customers, or EUs, and the software development team. Collaborates with project stakeholders to identify and prioritize system requirements. Possesses familiarity and experience documenting Software Requirements Specification (SRS), which may include both functional and non-functional components as well as requirement traceability matrix.

Creates system design documentation to encompass all technical aspects regarding the design of a new system or completing an upgrade of one that currently exists, including design constraints and future contingencies. Uses data modeling techniques to define, develop, and support customer driven requirements including the utilization of standard data modeling tools to create conceptual, logical, and physical data models. Evaluates customer provided data and supporting information to draw logical conclusions regarding to how to best implement or improve a business process or system. Supports all program related initiatives, including project planning and milestone development. Has experience with the design, execution, and oversight of IT projects. This includes direct experience in the design and development of integrated software and hardware solutions in the private or public sector.

Experience includes:

- Ability to lead teams, generate solutions, and work autonomously.
- Experience with DoD / Defense Logistics Agency (DLA) and related business processes and technical requirements.
- Understanding of NIST, RMF, and cybersecurity requirements at DOD.
- Experience with Eagle ECRT or ITS.
- Familiarity with Gold Documentation/ DoD Architecture Framework (DODAF) standards.
- Experience in software development and testing in DISA environment.
- Experience in Amazon Web Services (AWS), web services, mobile application development, and deployment.
- Experience/familiarity with Microsoft Web Services/Cloud or .Mil cloud solutions.
- Experience integration solutions across distributed systems architecture including interfaces.
- Experience with performance tuning and load balancing.
- Ability to design systems and appropriately scope and size for required solution.
- Experience with system failover and design / Continuity of Operations Plan (COOP).
- Has a business or requirements analyst background with sufficient technical breadth and superior communication and collaboration skills in order to successfully work with key stakeholders to solve business related problems or implement new solutions.
- Performs detailed functional analysis and gap/fit analysis of software solution packages.
- Performs software solution package selection and business case development.
- Conducts software and system developmental and acceptance testing.
• Experience with legacy system data exchange design, development, and implementation.
• Has a previous background creating SRS and systems design documentation for large projects.
• Experience with usage of data modeling tools in order to create data models.
• Utilizes an Agile approach to project management in a fast-paced development environment.
• Has a Security+ or equivalent IA Technical (IAT) / Identity Protection and Access Management (IAM) / IA System Architecture and Engineering (IASAE) Level II Certification.
• Possesses a Microsoft Windows 10 Operating System Certification.

Minimum Experience: Must have a minimum of 8 years of experience in the field.
SIN 54151S

Information/Cyber Security Subject Matter Expert Level 1

Functional Responsibilities: Provides technical, managerial, and administrative direction for problem definition, analysis, requirements development, and implementation for complex to extremely complex systems in the subject matter area of Information Security. Makes recommendations and advises on organization-wide system improvements, optimization, or maintenance efforts in the following specialties: information systems security; architecture; automation; communications protocols; risk management/electronic analysis; software; lifecycle management; software development methodologies; and test and evaluation. Participates risk assessment during the Certification and Accreditation process. Designs, develops, implements, and integrates IA architecture, system, or system component for use within data center, network, and enclave environments. Plays a pivotal role in information systems risk assessments and designs security countermeasures to mitigate identified risks. Ensures that the architecture and design of Client's Information Systems (IS) are functional and secure. As necessary, designs and develops IA or IA-enabled products, interface specifications, and approaches to secure the environment. Applies knowledge of existing IA policy, procedures, and structures to design, develop, and implement systems, components, or architectures. Ensures that the implementation of security designs properly mitigate identified threats. Documents system security design features and provides input to implementation plans and Standard Operating Procedures (SOPs).

Minimum Experience: Must have a minimum of 8 years of experience in the IT field. Specialized Experience: At least 6 years of combined new and related older technical experience in the IT field directly related to the required area of expertise.
**Senior Information Systems Security Engineer**

**Functional Responsibilities:** Analyzes and defines security requirements for information’s systems and applications. Designs, develops, engineers, and implements solutions that meet security requirements. Responsible for integration and implementation of the information system security solution. Gathers and organizes technical information about an organization’s mission goals and needs, existing security products, and ongoing programs in information security. Performs risk analyses of information systems and applications during all phases of the system development lifecycle. Designs architectures to include the software, hardware, and communications to support the total requirements, as well as provide for present and future cross-functional requirements and interfaces. Ensures these systems are compatible and in compliance with the standards for open systems and Client’s architectures. Determines and identifies high level functional and technical requirements based on interactions with the user community and knowledge of the enterprise architecture. Identifies, assesses, and presents options for meeting the functional and technical security requirements including hardware and software updates or upgrades. Formulates and defines specifications for operating system applications or modifies and maintains existing applications using engineering releases and utilities from the manufacturer. Creates detailed security design specifications for use by software development staff members. Interacts with project management to plan project schedules and technical direction. Develops software security design documents and technology white papers. Instrumental in selection of development tools.

Responsible for developing high level system design diagrams and for program design, coding, testing, debugging, and documentation. Instructs, directs, and checks the work of other task personnel. Responsible for QA review and the evaluation of existing and new software products.

**Minimum Experience:** Must have a minimum of 4 years of experience. Specialized Experience: At least 3 years of experience in defining computer security requirements for systems or high-level applications, evaluating approved security product capabilities, and developing computer system security solutions.

**Senior Web Developer**

**Functional Responsibilities:** Uses web technologies such as Ruby on Rails, CSS, Java, JavaScript, Extensible Markup Language (XML), PL/SQL, PHP, and others in a Unix environment and databases such as Oracle and MySQL to support projects. Coordinates with other project resources to establish interface standards. Uses industry best practices and agile development process as guidance in developing project requirements. Supports technical stakeholder briefing, project documentation, and QA measures for project.

**Minimum Experience:** Must have a minimum of 5 years’ experience in web Development, CSS, Java, Procedural Language (PL) / Structured Query Language (SQL), Personal Home Page (PHP), and Unix. Ruby programming in Rails environment (Ruby on Rails) a plus.
**Experience & Degree Substitution Equivalencies**
Experience exceeding the minimum shown may be substituted for education. Likewise, education exceeding the minimum shown may be substituted for experience.

<table>
<thead>
<tr>
<th>Equivalent Degree</th>
<th>Experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associate’s</td>
<td>2 years relevant experience</td>
</tr>
<tr>
<td>Bachelor’s</td>
<td>Associate’s degree + 2 years relevant experience or 4 years relevant experience</td>
</tr>
<tr>
<td>Master’s</td>
<td>Bachelor’s plus 2 years relevant experience or Associate’s degree + 4 years relevant experience or 6 years relevant experience</td>
</tr>
<tr>
<td>PhD</td>
<td>Master’s + 2 years relevant experience, or Bachelor’s + 4 years relevant experience or Associate’s + 6 years relevant experience or 8 years relevant experience</td>
</tr>
</tbody>
</table>