GENERAL SERVICES ADMINISTRATION

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: GSA Advantage.gov

Multiple Award Schedule
FSC Group, Part, and Section or Standard Industrial Group: 7010

FSC Class(es)/Product code(s) and/or Service Codes (as applicable) Contract Number
47QTCA19D00MZ: R425, D302, D306, D301, D314, D310

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

Contract Period: September 30 12, 2019 – September 29, 2024

Sharp Solutions, Inc.
6175 hickory Flat Hwy, Suite 110 #285
Canton, GA 30115
(404) 713-1615
www.sharpsolutionsinc.com

Business Size: Small Business

Point of Contact (POC): for Contract Administration:
Gary K. Miller Jr., Director of Operations
6175 Hickory Flat Hwy, Suite 110 #285
Canton, GA 30115-7210
Phone: (703) 249-5057 or (703) 851-8712
Facsimile: (404) 420-2822
Email: gary.miller@sharpsolutionsinc.com
Customer Information:

1a. Awarded Special Item Number(s):

<table>
<thead>
<tr>
<th>SIN</th>
<th>SIN Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S</td>
<td>Information Technology Professional Services</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Highly Adaptive Cybersecurity Services (HACS)</td>
</tr>
<tr>
<td>OLM</td>
<td>Order-Level Materials (OLMs)</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: Not applicable.

1c. Descriptions of all corresponding commercial job titles with experience, function responsibility and education are provided beginning on page 6.

2. Maximum order: $500,000

3. Minimum order: $100

4. Geographic Coverage: Domestic Delivery to include the 50 contiguous states, Alaska, Hawaii, Puerto Rice, Washington, DC, and U.S. Territories

5. Point of Production: Not Applicable

6. Discount from list prices or statement of net price: Prices Shown Herein are Net (discount deducted)

7. Quantity Discount: None

8. Prompt Payment Terms: 1% 20 Days, Net 30. Information for Ordering Offices: Prompt payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions.

9. Foreign Items: None

10a. Time of Delivery: The Contractor shall deliver to destination within the number of calendar days after receipt of order (ARO), as set forth below:

10b. Expedited Delivery: Consult with Contractor

10c. Overnight/2 day Delivery: Consult with Contractor

10d. 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.

11. FOB Point: Destination

12a. Ordering Address:

Sharp Solutions, Inc.
6175 Hickory Flat Hwy, Suite 110 #285
Canton, GA 30115-7210
Phone: (703) 249-5057
Facsimile: (404) 420-2822
https://www.sharpsolutionsinc.com/
DUNS: 039435400

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:

Sharp Solutions, Inc.
6175 Hickory Flat Hwy, Suite 110 #285
Canton, GA 30115-7210
Phone: (703) 249-5057
Facsimile: (404) 420-2822
https://www.sharpsolutionsinc.com/
DUNS: 039435400

14. Warranty Provisions: Contractor’s Standard Warranty

15. Export Packing Charges: Not applicable.

16. Terms and Conditions of rental, maintenance, and repair: Not applicable.

17. Terms and Conditions of installation: Not applicable.

18a. Terms and Conditions of repair parts indicating date of parts price lists and any discounts from list prices: Not applicable.

18b. Terms and Conditions of any other service parts: Not applicable.

19. List of Service and Distribution Points: Not applicable.
20. List of Participating Dealers: Not applicable.


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

22b. Section 508 compliance information is available by contacting Sharp Solutions, Inc. directly.

23. DUNS: 039435400       UEI: VIXEWEFTU7N!

24. Sharp Solutions, Inc. is registered in the System for Award Management (SAM) Database.
# Sharp Solutions, Inc.
## GSA Advantage! Price List
(Effective September 30, 2019)

<table>
<thead>
<tr>
<th>SIN</th>
<th>Labor Category</th>
<th>Year 3 9/30/21 - 9/29/22</th>
<th>Year 4 9/30/22 - 9/29/23</th>
<th>Year 5 9/30/23 - 9/29/24</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S</td>
<td>Business Analyst Entry-Level</td>
<td>$91.00</td>
<td>$93.27</td>
<td>$95.60</td>
</tr>
<tr>
<td>54151S</td>
<td>Business Analyst Journeyman</td>
<td>$122.91</td>
<td>$125.98</td>
<td>$129.13</td>
</tr>
<tr>
<td>54151S</td>
<td>Data Technician Entry-Level</td>
<td>$42.46</td>
<td>$43.52</td>
<td>$44.61</td>
</tr>
<tr>
<td>54151S</td>
<td>Enterprise Architect Journeyman</td>
<td>$103.14</td>
<td>$105.72</td>
<td>$108.36</td>
</tr>
<tr>
<td>54151S</td>
<td>Enterprise Architect Senior</td>
<td>$144.95</td>
<td>$148.57</td>
<td>$152.28</td>
</tr>
<tr>
<td>54151S</td>
<td>Network Engineer Journeyman</td>
<td>$73.31</td>
<td>$75.15</td>
<td>$77.03</td>
</tr>
<tr>
<td>54151S</td>
<td>Network Engineer Senior</td>
<td>$118.08</td>
<td>$121.03</td>
<td>$124.06</td>
</tr>
<tr>
<td>54151S</td>
<td>Project Manager Journeyman</td>
<td>$141.70</td>
<td>$145.24</td>
<td>$148.87</td>
</tr>
<tr>
<td>54151S</td>
<td>Subject Matter Expert Journeyman</td>
<td>$125.93</td>
<td>$129.08</td>
<td>$132.30</td>
</tr>
<tr>
<td>54151S</td>
<td>Subject Matter Expert Senior</td>
<td>$158.64</td>
<td>$162.61</td>
<td>$166.67</td>
</tr>
<tr>
<td>54151S</td>
<td>Subject Matter Expert Master</td>
<td>$169.42</td>
<td>$173.66</td>
<td>$178.00</td>
</tr>
<tr>
<td>54151S</td>
<td>Systems Engineer Journeyman</td>
<td>$132.52</td>
<td>$135.83</td>
<td>$139.23</td>
</tr>
<tr>
<td>54151S</td>
<td>Technical Writer Journeyman</td>
<td>$62.90</td>
<td>$64.47</td>
<td>$66.09</td>
</tr>
<tr>
<td>54151S</td>
<td>Web Development Specialist Journeyman</td>
<td>$69.32</td>
<td>$71.05</td>
<td>$72.83</td>
</tr>
</tbody>
</table>

| 54151HACS | Information Security Consultant Journeyman | $115.49 | $118.37 | $121.33 |
| 54151HACS | Information Security Consultant Senior    | $137.84 | $141.29 | $144.82 |
| 54151HACS | Infosec Engineer Journeyman              | $117.83 | $120.77 | $123.79 |
| 54151HACS | IT Security Specialist Journeyman         | $101.98 | $104.53 | $107.15 |
| 54151HACS | Security Engineer Journeyman              | $100.87 | $103.40 | $105.98 |

## Sharp Solutions, Inc.
### Labor Category Descriptions
SIN 54151S IT PROFESSIONAL SERVICES
LABOR CATEGORY DESCRIPTIONS

Business Analyst Entry-Level

Minimum Experience: 0-2 years of relevant experience

Functional Responsibility: Collects and evaluates IT requirements, develops business case analysis using Government templates, as provided, conducts analysis of investment cost/schedule/benefit/performance/return on investment, assesses and determines strategic plan/objective linkages, analyzes alternatives and risk assessment, and facilitates stakeholder coordination in the ranking of IT investments based on a defined set of evaluation criteria. Leverages Federal best practices in the completion of the project, as requested. Assists in updating and maintaining process guides, detailing end-to-end processes and business rules. Provides assistance in implementing lessons learned, best practices, improvements, and suggestions on processes and products. Ensures alignment with Federal policy and guidelines, as requested. Recommends solutions based on Government/industry management best practices. Provides updates and maintains the repository with the processes, templates, and completed plans. Provides analysis and recommendations to more senior staff for approval and decision. Analyzes process and re-engineering, with an understanding of technical problems and solutions as they relate to the current and future business environment. Creates process change by integrating new processes with existing ones and communicating these changes to impacted Business Systems teams. Recommends and facilitates quality improvement efforts.

Minimum Education: Bachelor’s Degree in Business, Science, Information Technology, Engineering or Mathematics

Business Analyst Journeyman

Minimum Experience: 2-5 years of relevant experience
**Functional Responsibility:** Collects and evaluates IT requirements, develops business case analysis using Government templates, as provided, conducts analysis of investment cost/schedule/benefit/performance/return on investment, assesses and determines strategic plan/objective linkages, analyzes alternatives and risk assessment, and facilitates stakeholder coordination in the ranking of IT investments based on a defined set of evaluation criteria. Leverages Federal best practices in the completion of the project, as requested. Assists in updating and maintaining process guides, detailing end-to-end processes and business rules. Provides assistance in implementing lessons learned, best practices, improvements, and suggestions on processes and products. Ensures alignment with Federal policy and guidelines, as requested. Recommends solutions based on Government/industry management best practices. Provides updates and maintains the repository with the processes, templates, and completed plans. Provides analysis and recommendations to more senior staff for approval and decision. Analyzes process and re-engineering, with an understanding of technical problems and solutions as they relate to the current and future business environment. Creates process change by integrating new processes with existing ones and communicating these changes to impacted Business Systems teams. Recommends and facilitates quality improvement efforts.

**Minimum Education:** Bachelor’s Degree in Business, Science, Information Technology, Engineering or Mathematics

**Data Technician Entry-Level**

**Minimum Experience:** 0-2 years of relevant experience

**Functional Responsibility:** Responsible for review of Cyber Security documents for data verification and entry to records and databases. Responsible for retrieving Cyber Security data as requested. Compares data entered with source documentation, or data re-entry data in verified format on screen to detect errors. Keeps track of Cyber Security data received as well as source documentation. Prepares and sorts Cyber Security source documents. Identifies and interprets data to be entered. Works with source document authors and assessors to resolve questions, inconsistencies, or missing data. Reviews and makes required corrections to information entered. Compiles, sorts, and verifies accuracy of Cyber Security & system relevant data prior to entry. Processes various Cyber Security forms. Assists in establishing and maintaining an effective and efficient Cyber Security records management system. Generates reports and responds to inquiries regarding entered data as requested. Contributes to a Cyber Security team effort and accomplishes related results as required. Maintains confidential Cyber Security information. Performs general duties such as data entry, answering phones, quality and standards analysis, etc. Performs other job-related duties as assigned.

**Minimum Education:** Bachelor’s Degree in Business, Science, Information Technology, Engineering or Mathematics

**Enterprise Architect Journeyman**
Minimum Experience: 2-5 years of relevant experience

Functional Responsibility: Provides expertise with Federal enterprise architecture framework; including, scope, direction, and governance practices. Selects and implements Commercial Off-the-Shelf (COTS) enterprise solution applications. Provides recommendations in the design, execution, and oversight of large-scale IT projects. Supports functional lead for requirements definition to the IT system development project and support fit/gap analyses of Government Off-the-Shelf (GOTS) and COTS software. Engages with stakeholders to determine how IT enterprise platforms enable organizational business strategies and functions. Assists with developing IT strategies and designing enterprise architectures that align IT capabilities to strategic goals and priorities. Participates in business case development by supporting identification of functional impacts for alternative solutions. Advises on selection of technological purchases with regards to processing, data storage, data access, and applications development. Sets standards for the client/server relational database structure for the organization (SQL, ORACLE, SYBASE, etc.). Advises of feasibility of potential future projects to management. May supervise and provide direction to less skilled workforce.

Minimum Education: Bachelor’s Degree in Business, Science, Information Technology, Engineering or Mathematics

Enterprise Architect Senior

Minimum Experience: 5 years of relevant experience

Functional Responsibility: Provides expertise with Federal enterprise architecture framework; including, scope, direction, and governance practices. Selects and implements Commercial Off-the-Shelf (COTS) enterprise solution applications. Provides recommendations in the design, execution, and oversight of large-scale IT projects. Functional lead for requirements definition to the IT system development project and support fit/gap analyses of Government Off-the-Shelf (GOTS) and COTS software. Leads Client engagements to show how IT enterprise platforms enable organizational business strategies and functions. Lead the development of IT strategies and designing enterprise architectures that align IT capabilities to strategic goals and priorities. Leads jr level staff in business case development by supporting identification of functional impacts for alternative solutions. Advises entry level staff on selection of technological purchases with regards to processing, data storage, data access, and applications development. Sets standards for the client/server relational database structure for the organization (SQL, ORACLE, SYBASE, etc.). Advises of feasibility of potential future projects to management. May supervise and provide direction to less skilled workforce.

Minimum Education: Bachelor’s Degree in Business, Science, Information Technology, Engineering or Mathematics

Network Engineer Journeyman
Minimum Experience: 2-5 years of relevant experience

Functional Responsibility: Provides technical guidance for directing and monitoring information systems operations. Designs, builds, and implements network systems. Directs compilation of records and reports concerning network operations and maintenance. Troubleshoots network performance issues. Analyzes network traffic and provides capacity planning solutions. Monitors and responds to complex technical control facility hardware and software problems. Interfaces with vendor support service groups to ensure proper escalation during outages or periods of degraded system performance. Manages the purchase, testing, installation, and support of network communications, including LAN/MAN/WAN systems. Performs system-level design and configuration of products including determination of hardware, OS, and other platform specifications. Plans large-scale systems projects through vendor comparison and cost studies. Performs a variety of systems engineering tasks and activities that are broad in nature and are concerned with major systems design, integration, and implementation, including personnel, hardware, software, budgetary, and support facilities and/or equipment. Provides quality assurance review and the evaluation of new and existing software products. Provides assistance and oversight for all information systems operations activities, including computer and telecommunications/communications operations, data entry, data control, LAN/MAN/WAN administration and operations support, operating systems programming, system security policy procedures, and/or web strategy and operations. Provides input to policy level discussions regarding standards and budget constraints. Supervises all personnel engaged in the operation and support of network facilities, including all communications equipment on various platforms in large scale or multi-shift operations. Supervises complex operations that involve two or more additional functions such as, but not limited to, network operations, systems security, systems software support, and production support activities. Monitors and responds to hardware, software, and network problems. Provides the routine testing and analysis of all elements of the network facilities (including power, software, communications machinery, lines, modems, and terminals). Utilizes software and hardware tools and identifies and diagnoses complex problems and factors affecting network performance. Troubleshoots network systems when necessary and makes improvements to the network.

Minimum Education: Bachelor’s Degree in Business, Science, Information Technology, Engineering or Mathematics

Network Engineer Senior

Minimum Experience: 6-10 years of relevant experience
**Functional Responsibility:** Provides technical guidance for directing and monitoring information systems operations. Designs, builds, and implements network systems. Directs compilation of records and reports concerning network operations and maintenance. Troubleshoots network performance issues. Analyzes network traffic and provides capacity planning solutions. Monitors and responds to complex technical control facility hardware and software problems. Interfaces with vendor support service groups to ensure proper escalation during outages or periods of degraded system performance. Manages the purchase, testing, installation, and support of network communications, including LAN/MAN/WAN systems. Performs system-level design and configuration of products including determination of hardware, OS, and other platform specifications. Plans large-scale systems projects through vendor comparison and cost studies. Performs a variety of systems engineering tasks and activities that are broad in nature and are concerned with major systems design, integration, and implementation, including personnel, hardware, software, budgetary, and support facilities and/or equipment. Provides quality assurance review and the evaluation of new and existing software products. Provides assistance and oversight for all information systems operations activities, including computer and telecommunications/communications operations, data entry, data control, LAN/MAN/WAN administration and operations support, operating systems programming, system security policy procedures, and/or web strategy and operations. Provides input to policy level discussions regarding standards and budget constraints. Supervises all personnel engaged in the operation and support of network facilities, including all communications equipment on various platforms in large scale or multi-shift operations. Supervises complex operations that involve two or more additional functions such as, but not limited to, network operations, systems security, systems software support, and production support activities. Monitors and responds to hardware, software, and network problems. Provides the routine testing and analysis of all elements of the network facilities (including power, software, communications machinery, lines, modems, and terminals). Utilizes software and hardware tools and identifies and diagnoses complex problems and factors affecting network performance. Troubleshoots network systems when necessary and makes improvements to the network.

**Minimum Education:** Bachelor’s Degree in Business, Science, Information Technology, Engineering or Mathematics

---

**Project Manager Journeyman**

**Minimum Experience:** 2-5 years of relevant experience
**Functional Responsibility:** Leads team on large projects or significant segment of large complex projects. Analyzes new and complex project related problems and creates innovative solutions involving finance, scheduling, technology, methodology, tools, and solution components. Provides applications systems analysis and programming activities for a Government site, facility or multiple locations. Prepares long and short-range plans for application selection, systems development, systems maintenance, and production activities and for necessary support resources. Oversees all aspects of projects.

**Minimum Education:** Bachelor’s Degree in Business, Science, Information Technology, Engineering or Mathematics

---

**Subject Matter Expert Journeyman**

**Minimum Experience:** 2-5 years of relevant experience

**Functional Responsibility:** Serves as subject matter expert, possessing in-depth knowledge of a particular area, such as business, computer science, engineering, mathematics, or the various sciences. Provides technical knowledge and analysis of highly specialized applications and operational environments, high-level functional systems analysis, design, integration, documentation and implementation advice on exceptionally complex problems that need extensive knowledge of the subject matter for effective implementation. Participates as needed in all phases of software development with emphasis on the planning, analysis, testing, integration, documentation, and presentation phases. Applies principles, methods and knowledge of the functional area of capability to specific task order requirements, advanced mathematical principles and methods to exceptionally difficult and narrowly defined technical problems in engineering and other scientific applications to arrive at automated solutions.

**Minimum Education:** Bachelor’s Degree in Business, Science, Information Technology, Engineering or Mathematics

---

**Subject Matter Expert Senior**

**Minimum Experience:** 6-10 years of relevant experience
**Functional Responsibility:** Serves as subject matter expert, possessing in-depth knowledge of a particular area, such as business, computer science, engineering, mathematics, or the various sciences. Provides technical knowledge and analysis of highly specialized applications and operational environments, high-level functional systems analysis, design, integration, documentation and implementation advice on exceptionally complex problems that need extensive knowledge of the subject matter for effective implementation. Participates as needed in all phases of software development with emphasis on the planning, analysis, testing, integration, documentation, and presentation phases. Applies principles, methods and knowledge of the functional area of capability to specific task order requirements, advanced mathematical principles and methods to exceptionally difficult and narrowly defined technical problems in engineering and other scientific applications to arrive at automated solutions.

**Minimum Education:** Bachelor’s Degree in Business, Science, Information Technology, Engineering or Mathematics

---

**Subject Matter Expert Master**

**Minimum Experience:** 10+ years of relevant experience

**Functional Responsibility:** Serves as subject matter expert, possessing in-depth knowledge of a particular area, such as business, computer science, engineering, mathematics, or the various sciences. Provides technical knowledge and analysis of highly specialized applications and operational environments, high-level functional systems analysis, design, integration, documentation and implementation advice on exceptionally complex problems that need extensive knowledge of the subject matter for effective implementation. Participates as needed in all phases of software development with emphasis on the planning, analysis, testing, integration, documentation, and presentation phases. Applies principles, methods and knowledge of the functional area of capability to specific task order requirements, advanced mathematical principles and methods to exceptionally difficult and narrowly defined technical problems in engineering and other scientific applications to arrive at automated solutions.

**Minimum Education:** Bachelor’s Degree in Business, Science, Information Technology, Engineering or Mathematics

**Systems Engineer Journeyman**
Minimum Experience: 2-5 years of relevant experience

Functional Responsibility: Provides analysis related to the design, development, and integration of hardware, software, man-machine interfaces and all system level requirements to provide an integrated IT solution. Develops integrated system test requirement, strategies, devices and systems. Directs overall system level testing.

Minimum Education: Bachelor’s Degree in Business, Science, Information Technology, Engineering or Mathematics

Technical Writer Journeyman

Minimum Experience: 2-5 years of relevant experience

Functional Responsibility: Writes reports, manuals, service guides, training courses, and other documents, and ensures quality of those documents written by others. Reviews grammar, writing style, and syntax of documentation.

Minimum Education: Bachelor’s Degree in Business, Science, Information Technology, Engineering or Mathematics

Web Development Specialist Journeyman

Minimum Experience: 2 years of relevant experience

Functional Responsibility: Responsible for maintaining knowledge on large or enterprise wide systems. Assists with translating requirements into software specifications and design documents. Assists with the designs, development, testing and implementation of software in different languages, using different development techniques and methodologies on different platforms and in different environments. Follows more Senior staff for project estimates for agile development estimates and schedules. Reviews existing programs and assists in making recommendations for improvement by reducing operating time and improving current techniques.

Minimum Education: Bachelor’s Degree in Business, Science, Information Technology, Engineering or Mathematics
SIN 54151HACS HIGHLY ADAPTIVE CYBERSECURITY SERVICES
LABOR CATEGORY DESCRIPTIONS

<table>
<thead>
<tr>
<th>Level</th>
<th>Knowledge/Skill Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry-Level</td>
<td>Applies fundamental concepts, processes, practices, and procedures on technical assignments. Performs work that requires practical experience and training. Work is performed under supervision.</td>
</tr>
<tr>
<td>Journeyman</td>
<td>Possesses and applies expertise on multiple complex work assignments. Assignments may be broad in nature, requiring originality and innovation in determining how to accomplish tasks. Operates with appreciable latitude in developing methodology and presenting solutions to problems. Contributes to deliverables and performance metrics where applicable.</td>
</tr>
<tr>
<td>Senior</td>
<td>Possesses and applies a comprehensive knowledge across key tasks and high impact assignments. Plans and leads major technology assignments. Evaluates performance results and recommends major changes affecting short-term project growth and success.</td>
</tr>
<tr>
<td>Master</td>
<td>Provides technical/management leadership on major tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that technical requirements are met. Interactions involve client negotiations and interfacing with senior management. Decision making and domain knowledge may have a critical impact on overall project implementation. May supervise others.</td>
</tr>
</tbody>
</table>

Notes: For equivalences, a Masters degree may be substituted for 4 years experience, a Doctor or PHD will count for 8 additional years of experience.

Information Security Consultant Journeyman

Minimum Experience: 2-5 years of relevant IT or consulting experience with a focus on IT Cyber Security policies, architectures, and/or standard operating procedures, or four years minimum experience in an information security or information assurance role and a minimum of two years direct experience with information security. Must have a thorough knowledge of the Risk Management Framework (RMF) six-step process and experience with the conducting technical Cyber Security assessments of complex information systems with minimal to no supervision.

Functional Responsibility: Conducts Cyber Security assessments of Federal information systems in accordance with the Federal Information Security Management Act (FISMA), NIST SP 800-37 and 800-53 (as amended) guidance. Develops security authorization packages for newly developed systems. Coordinates all aspects of the effort with identified points of contact, working with a high degree of independence. Collaborates with information system owners, security officers, developers and IT operations personnel to conduct system security categorizations in accordance with NIST SP 800-60 and FIPS 199 requirements (as amended). Documents Cyber Security control selections and apply control tailoring guidance in accordance with NIST SP 800-53 and NIST SP 800-18 (as amended). Develops initial system cyber security plans and contingency plans aligned with organizational policies and NIST SP 800-18, NIST SP 800-34 (as amended) and security best practices. Provides recommendations to organizational stakeholders for preliminary POA&M remediation and application of security engineering principles (NIST SP 800-27 Rev. A). Develops security assessment plans, carry out technical Cyber Security assessments of all selected management, operational and technical security controls, and documents results of the Cyber Security assessment and a concurrent risk assessment in a Security Assessment Report (SAR). Develops POA&M Reports including all identified weaknesses, recommended actions for remediation or mitigation and provide weakness criticality ratings based on the risk assessment results. Provides multi-discipline security administrative and technical Cyber Security support to the IA RMF and Continuous Monitoring...
Programs. Areas of responsibility include Physical, Computer, Personnel, Information, Administrative, Operational, and Communications Security analysis, Cyber Security assessment, and reporting. Key focus areas are continuous monitoring program support and strategic security control implementation and assessment. May consult with contractors or corporations that store Federal data on NIST compliance, Cyber Security programs, risk analysis, FISMA compliance, Interconnection standards, or cloud security. Capable of conducting 3rd Party Risk Assessments for Federal, State, or Local agencies and reporting posture to senior management. Including incident response, vulnerability scanning, baseline compliance, facility assessments, security control assessment, and policy and procedure analysis and development. Conducts hands on testing utilizing industry tools to analyses risk with IT Systems, Databases, Source Code, Web Applications, Cloud hosted systems (IaaS, PaaS, SaaS), etc. Capable of calculating risk and tailoring it to the local security posture via the analysis of Impact and Likelihood with frameworks such as NIST, CVE, CVSS.

Minimum Education: Bachelor's Degree and four years relevant experience or Master's Degree and three years relevant experience or six years relevant experience. Industry recognized technical certification accepted in lieu of two years of experience. Multiple certifications strongly preferred:


Information Security Consultant Senior

Minimum Experience: 6 years of relevant IT or consulting experience with a focus on IT Cyber Security policies, architectures, and/or standard operating procedures, or four years minimum experience in an information security or information assurance role and a minimum of two years direct experience with information security. Must have a thorough knowledge of the Risk Management Framework (RMF) six-step process and experience with the conducting technical Cyber Security assessments of complex information systems with minimal to no supervision.

Functional Responsibility: Conducts Cyber Security assessments of Federal information systems in accordance with the Federal Information Security Management Act (FISMA), NIST SP 800-37 and 800-53 (as amended) guidance. Develops security authorization packages for newly developed systems. Coordinates all aspects of the effort with identified points of contact, working with a high degree of independence. Collaborates with information system owners, security officers, developers and IT operations personnel to conduct system security categorizations in accordance with NIST SP 800-60 and FIPS 199 requirements (as amended). Documents Cyber Security control selections and apply control tailoring guidance in accordance with NIST SP 800-53 and NIST SP 800-18 (as amended). Develops initial system cyber security
plans and contingency plans aligned with organizational policies and NIST SP 800-18, NIST SP 800-34 (as amended) and security best practices. Provides recommendations to organizational stakeholders for preliminary POA&M remediation and application of security engineering principles (NIST SP 800-27 Rev. A). Develops security assessment plans, carry out technical Cyber Security assessments of all selected management, operational and technical security controls, and documents results of the Cyber Security assessment and a concurrent risk assessment in a Security Assessment Report (SAR). Develops POA&M Reports including all identified weaknesses, recommended actions for remediation or mitigation and provide weakness criticality ratings based on the risk assessment results. Provides multi-discipline security administrative and technical Cyber Security support to the IA RMF and Continuous Monitoring Programs. Areas of responsibility include Physical, Computer, Personnel, Information, Administrative, Operational, and Communications Security analysis, Cyber Security assessment, and reporting. Key focus areas are continuous monitoring program support and strategic security control implementation and assessment. May consult with contractors or corporations that store Federal data on NIST compliance, Cyber Security programs, risk analysis, FISMA compliance, Interconnection standards, or cloud security. Capable of conducting 3rd Party Risk Assessments for Federal, State, or Local agencies and reporting posture to senior management. Including incident response, vulnerability scanning, baseline compliance, facility assessments, security control assessment, and policy and procedure analysis and development. Conducts hands on testing utilizing industry tools to analyses risk with IT Systems, Databases, Source Code, Web Applications, Cloud hosted systems (IaaS, PaaS, SaaS), etc. Capable of calculating risk and tailoring it to the local security posture via the analysis of Impact and Likelihood with frameworks such as NIST, CVE, CVSS.  

**Minimum Education:** Bachelor's Degree and four years relevant experience or Master's Degree and three years relevant experience or six years relevant experience. Industry recognized technical certification accepted in lieu of two years of experience. Multiple certifications strongly preferred:


**Infosec Engineer Journeyman**

**Minimum Experience:** 2-5 years of relevant experience directing projects or in a relevant Cyber Security, technical engineer role. Has direct experience developing IT security policies, architectures, and standard operating procedures with a strategic & Cyber Security perspective. Extensive knowledge of and practical experience with Federal Information Security Management Act (FISMA), implementing standard methodologies used in the Risk Management Framework (RMF), HIPPA, PCI, and other applicable Cyber Security frameworks. Expert-level knowledge
and experience with National Institute of Standards and Technology (NIST) guidelines and industry best practices for: Cyber Security, Risk Assessment and Management, Vulnerability Analysis, Contingency Planning, Disaster Recovery, Configuration Management, Security Assessments and developing Mitigation Plans. Must have a minimum of 4 years direct full-time experience conducting security assessments and developing all deliverables within a system authorization package. Must have detailed and extensive experience with integrating Cyber Security and risk management activities into the system development life cycle and implementing, evaluating and documenting all security controls as defined by the NIST SP 800-53 (as-amended). Knowledge of core IT & Cyber Security products and concepts including: Operating systems, databases, networking, firewalls, and major IT software (i.e. Linux, Windows, Cisco, Oracle, scripting languages, etc.)

**Functional Responsibility:** Provides multi-discipline Cyber Security and Information Assurance administrative and technical security support to client (IA) RMF efforts. Areas of responsibility include Physical, Computer, Personnel, Information, Administrative, Operational, and Communications Security analysis, assessment, and reporting.

Specific roles include:

- Provides recommendations to client leadership, offices and divisions for the integration of security processes and compliance with Federal regulations and Departmental policy.
- Directs security efforts to increase efficiencies and enforce a global security mindset.
- Provides strategic guidance for the further development of the security program within IA.
- Develops policies and procedures supporting regulations, directives, and Departmental policy.
- Assists senior management with establishing a plan of action for the remediation of organization wide weaknesses.
- Provides direct information assurance guidance pertaining to the development and modification of systems.
- Provides strategic insight and continuous support for the integration of the system development life cycle throughout IA.
- Assists the client by providing recommendations concerning new and existing projects and assist project managers with security oversight.
- Coordinates with representatives and Subject Matter Experts (SME) from other Federal Agencies and commercial organizations to maintain awareness of upcoming changes to regulations and technologies.
- Conduct all compliant NIST processes with in the RMF (i.e. Risk Assessment, Vulnerability Assessment, Contingency Planning and Testing, Disaster Recovery Planning, Security Impact Assessments, Incident Response Planning, Change Management, Baseline Compliance Analysis, FIPS compliance, etc.)
- Conduct vulnerability scanning with applicable scanning tools, baseline compliance, network analysis, malicious software scanning, audit log review, and security program management with NIST 800-53 controls.
• Function in the NIST roles of Information System Security Officer (ISSO), Certification Agent (CA), or team lead.

**Minimum Education:** Bachelor's Degree and four years relevant experience or Master's Degree and three years relevant experience or six years relevant experience. Industry recognized technical certification accepted in lieu of two years of experience. Multiple certifications strongly preferred:

- CompTIA Security+
- GIAC Certified Incident Handler (GCIH)
- GIAC Security Essentials Certification (GSEC)
- GIAC Security Expert (GSE)
- GIAC Information Security Professional (GISP)
- GIAC Security Leadership Certification (GSLC)
- ISC2 Certified Authorization Professional (CAP)
- ISC2 System Security Certified Practitioner (SSCP)
- ISC2 Certified Information System Security Professional (CISSP)
- ISC2 Certified Information System Security Associate (CISSA)
- ISACA Certified Information Systems Auditor (CISA)
- GIAC Systems and Network Auditor (GSNA)
- Electronic Commerce Council Certified Ethical Hacker (CEH)

**IT Security Specialist Journeyman**

**Minimum Experience:** 2-5 years of relevant IT or Cyber Security consulting experience with a preferred focus on IT security policies, architectures, and/or standard operating procedures, or four years minimum experience in an information security or information assurance role and a minimum of two years direct experience with Cyber Security. The IT Security Specialist II must have a strong background adhering to Federal Information Security Management Act (FISMA) Standards using the Risk Management Framework (RMF) and be familiar with a variety of the field's concepts, practices, and procedures. Must be able to conduct Assessment and Accreditation (A&A) reviews and perform continuous monitoring functions and assist in maintaining Systems Authorization to Operate (ATO) for systems and re-certifications. Must have experience as an ISSO and/or working closely with ISSOs and System Owners to implement security/Cyber Security controls mitigating risks; Experience preparing complete Assessment and Authorization System Security documentation for review and approval by the Authorizing Official; Experience and proficient in applying NIST Risk Management Framework to Federal Systems NIST 800-37 guidelines; Ability to lead meetings, prepare/provide presentations, and coordinate security mitigation activities supporting the ISSO function; Utilize proficient, clear and concise English written and verbal communication skills in order to effectively interact with clients. Successfully communicate with individuals at various levels of Cyber Security expertise in subject areas of concern.
**Functional Responsibility:** Analyze information security systems and applications and recommends and/or develops security/Cyber Security measures to protect information against unauthorized modification or loss.

- Conduct audits and provide guidance of security programs (i.e., A&A, Continuous Monitoring, FISMA, NIST, Local Agency) policies and procedures.
- Prepare risk analysis reports (RAR), Security Assessment Reports (SAR) and provide recommendations to the client.
- Analyze penetration testing (PTR) and vulnerability scan reports (VAR) on all systems as required.
- Conduct vulnerability scanning with applicable scanning tools, baseline compliance, network analysis, malicious software scanning, audit log review, and overall compliance with NIST 800-53 controls.
- Provide impact analysis on local Federal Civilian Agency with regard to updates and version changes on National Institute of Standards and Technology (NIST) Security Publications and FISMA notices.
- Update and develop security Standards and templates as required to meet new government and regulatory requirements.
- Use risk management techniques to develop and complete risk assessments based on NIST standards to ensure Information Assurance design sufficiently mitigates the risk.
- Relies on experience and judgment to plan and accomplish goals.
- May lead and direct the work of others. Typically reports to a project leader or team lead.
- Function in the NIST roles of Information System Security Officer (ISSO), Certification Agent (CA), or trusted advisor to key security personnel.

**Minimum Education:** BS/BA degree in a related area (or equivalent), and 4 years of experience in the field or in a related area. Industry-recognized technical certification accepted in lieu of one-year experience with one of the following certifications:

- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- GIAC Certified Incident Handler (GCIH)
- GIAC Security Essentials Certification (GSEC)
- GIAC Security Expert (GSE)
- GIAC Information Security Professional (GISP)
- GIAC Security Leadership Certification (GSLC)
- ISC2 Certified Authorization Professional (CAP)
- ISC2 System Security Certified Practitioner (SSCP)
- ISC2 Certified Information System Security Professional (CISSP)
- ISC2 Certified Information System Security Associate (CISSA)
- ISACA Certified Information System Manager (CISM)
**Security Engineer Journeyman**

**Minimum Experience:** 2-5 years of relevant experience leading and directing projects in a relevant technical engineer and/or Cyber Security role. Has direct experience developing IT security policies, architectures, and standard operating procedures with a strategic /Cyber Security perspective. Extensive knowledge of Federal Information Security Management Act (FISMA) Standards and practical experience with implementing standard methodologies used in the Risk Management Framework (RMF) six-step process. Expert-level knowledge and experience with National Institute of Standards and Technology (NIST) guidelines and industry best practices for: Risk Assessment and Management, Vulnerability Analysis, Contingency Planning, Disaster Recovery, Configuration Management, Security/Cyber Security Assessments and developing Mitigation Plans. Must have a minimum of 8 years direct full-time experience conducting security assessments and developing all deliverables within a system authorization package. Must have detailed and extensive experience with implementing, evaluating and documenting all technical, management, and operational security controls as defined by the NIST SP 800-53 (as-amended).

**Functional Responsibility:** Leads projects/programs. Provides multi-discipline security/Cyber Security administrative and technical security support to client (IA) RMF effort. Areas of responsibility include Physical, Computer, Personnel, Information, Administrative, Operational, Communications and Cyber Security analysis, assessment, and reporting. Specific roles include:

- Provides recommendations to client leadership, offices and divisions for the integration of security/Cyber Security processes and compliance with Federal regulations and Departmental policy.
- Directs security/Cyber Security efforts to increase efficiencies and enforce a global security mindset.
- Develop foundational documents for an IT Security Program supporting sites or agencies.
- Provides strategic guidance for the further development of the security program within IA.
- Develops policies and procedures supporting regulations, directives, and Departmental policy.
- Assists senior management with establishing a plan of action for the remediation of organization wide weaknesses.
- Provides direct information assurance guidance pertaining to the development and modification of systems.
- Provides strategic insight and continuous support for the integration of the system development life cycle throughout IA.
- Assists the client by providing recommendations concerning new and existing projects and assist project managers with security oversight.
- Coordinates with representatives and Subject Matter Experts (SME) from other Federal Agencies and commercial organizations to maintain awareness of upcoming changes to regulations and technologies.
• Develops Risk Assessments in accordance with NIST guidance and deliver risk analysis and guidance as needed.
• Provide expert analysis of vulnerabilities and risk impacting a system and provide mitigation or remediation recommendations.
• Capable of conducting vulnerability validation utilizing penetration testing techniques.
• Function in the NIST roles of Information System Security Officer (ISSO), Certification Agent (CA), or trusted advisor to senior management, stakeholder boards.
• Capable of conducting and training team members in vulnerability scanning with applicable scanning tools, baseline compliance, network analysis, malicious software scanning, audit log review, and over all compliance with NIST 800-53 controls.

**Minimum Education:** Bachelor's Degree and four years relevant experience or Master's Degree and three years relevant experience or six years relevant experience. Industry recognized technical certification accepted in lieu of two years of experience. Multiple certifications strongly preferred:

- CompTIA Security+
- GIAC Certified Incident Handler (GCIH)
- GIAC Security Essentials Certification (GSEC)
- GIAC Security Expert (GSE)
- GIAC Information Security Professional (GISP)
- GIAC Security Leadership Certification (GSLC)
- ISC2 Certified Authorization Professional (CAP)
- ISC2 System Security Certified Practitioner (SSCP)
- ISC2 Certified Information System Security Professional (CISSP)
- ISC2 Certified Information System Security Associate (CISSA)
- ISACA Certified Information System Manager (CISM)
- Certified Information Systems Auditor (CISA)
- GIAC Systems and Network Auditor (GSNA)
- Electronic Commerce Council Certified Ethical Hacker (CEH)