Federal Supply Service

Authorized Federal Supply Schedule Price List

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

Multiple Award Schedule

FSC Group: Information Technology

Contract Number 47QTCA20D0072

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

Contract Period March 10, 2020 through March 9, 2025

Wise Technical Innovations, LLC
DBA WTI Networks
9509 Densmore Place
Norfolk, VA 23503
www.wtinetworks.com
For Contract Information, please contact Koren Archibald koren@wtinetworks.com

Business Size: Small Business
Prices Shown Herein are Net (discount deducted)

Pricelist Current Through Mod: PS-002 Effective: 07/24/2020
Information for Ordering Activities

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

<table>
<thead>
<tr>
<th>SIN</th>
<th>Labor Category</th>
<th>GSA Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S/RC</td>
<td>Information Technology Professional Services</td>
<td></td>
</tr>
<tr>
<td>54151HEAL/RC</td>
<td>Health Information Technology Services</td>
<td></td>
</tr>
<tr>
<td>54151HACS/RC</td>
<td>Highly Adaptive Cyber Security Services</td>
<td></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 (base year):

<table>
<thead>
<tr>
<th>SIN</th>
<th>Labor Category</th>
<th>GSA Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S, 54151HEAL</td>
<td>Integrated Systems Technician</td>
<td>$39.62</td>
</tr>
</tbody>
</table>

1c. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles, experience, functional responsibility and education for those types of employees or subcontractors who will perform services shall be provided. Please refer to Wise Technical Innovations LLC attached labor category descriptions on page 9.

2. Maximum Order: $500,000

3. Minimum Order: $0

4. Geographic Coverage (delivery area):

<table>
<thead>
<tr>
<th>SIN</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S</td>
<td>U-50 St, DC, Terr</td>
</tr>
<tr>
<td>54151HEAL</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td></td>
</tr>
</tbody>
</table>

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

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

7. Quantity/Volume discounts: 1% for Task Orders > $350,000

8. Prompt payment terms: Net 30. Information for Ordering Activities: Prompt Payment Terms cannot be negotiated outside of the contractual agreement in exchange for other concessions.
9. Foreign items (list items by country of origin). **Not Applicable**

10a. Time of Delivery – **30 DARO**

10b. Expedited Delivery: **Contact Contractor**

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

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

11. F.O.B. point(s): **Destination**

12a. Ordering Address: Wise Technical Innovations
LLC Db a WTI Networks
9509 Densmore Place
Norfolk, VA 23503

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: Wise Technical Innovations LLC
Db a WTI Networks
9509 Densmore Place
Norfolk, VA 23503

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**

18a. Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices (if applicable): **N/A**
18b. Terms and conditions for any other services (if applicable): N/A
19. List of services 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): N/A
23. Data Universal Number System (DUNS) number: 82547399
24. Notification regarding registration in Supply Award Management (SAM) database: Wise Technical Innovations LLC has an active registration in the SAM database.
RATES AND ESCALATION CHART

The following pages contain GSA Rates including IFF with 2% annual escalation.
<table>
<thead>
<tr>
<th>SIN</th>
<th>Awarded Labor Category</th>
<th>Year 1 03.10.2020 to 03.09.2021</th>
<th>Year 2 03.10.2021 to 03.09.2022</th>
<th>Year 3 03.10.2022 to 03.09.2023</th>
<th>Year 4 03.10.2023 to 03.09.2024</th>
<th>Year 5 03.10.2024 to 03.09.2025</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S, 54151HEAL</td>
<td>System Security Engineer (Patching)</td>
<td>$92.85</td>
<td>$94.70</td>
<td>$96.60</td>
<td>$98.53</td>
<td>$100.50</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Systems Engineer (Advanced Troubleshooting)</td>
<td>$113.37</td>
<td>$115.64</td>
<td>$117.95</td>
<td>$120.31</td>
<td>$122.72</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Sr. Systems Engineer</td>
<td>$147.58</td>
<td>$150.53</td>
<td>$153.54</td>
<td>$156.61</td>
<td>$159.74</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Database Architect</td>
<td>$95.78</td>
<td>$97.69</td>
<td>$99.65</td>
<td>$101.64</td>
<td>$103.67</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Sr. Database Architect</td>
<td>$109.46</td>
<td>$111.65</td>
<td>$113.88</td>
<td>$116.16</td>
<td>$118.48</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Computer Programmer/Analyst</td>
<td>$71.64</td>
<td>$73.07</td>
<td>$74.53</td>
<td>$76.02</td>
<td>$77.54</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Sr. Computer Programmer/Analyst</td>
<td>$113.37</td>
<td>$115.64</td>
<td>$117.95</td>
<td>$120.31</td>
<td>$122.72</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Web Designer/Developer (Sharepoint Tickets)</td>
<td>$92.85</td>
<td>$94.70</td>
<td>$96.60</td>
<td>$98.53</td>
<td>$100.50</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Sr. Web Developer (DRL Advanced Troubleshooting and Maintenance)</td>
<td>$122.17</td>
<td>$124.61</td>
<td>$127.10</td>
<td>$129.64</td>
<td>$132.24</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Web Tech Administrator</td>
<td>$87.96</td>
<td>$89.72</td>
<td>$91.51</td>
<td>$93.34</td>
<td>$95.21</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Web Content Manager</td>
<td>$86.01</td>
<td>$87.73</td>
<td>$89.48</td>
<td>$91.27</td>
<td>$93.09</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Computer Systems Analyst</td>
<td>$107.00</td>
<td>$109.14</td>
<td>$111.33</td>
<td>$113.55</td>
<td>$115.82</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Jr. Web Developer</td>
<td>$133.30</td>
<td>$135.97</td>
<td>$138.69</td>
<td>$141.46</td>
<td>$144.29</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Disaster Recovery Specialist</td>
<td>$124.12</td>
<td>$126.60</td>
<td>$129.14</td>
<td>$131.72</td>
<td>$134.35</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Backup/Restore Administrator</td>
<td>$94.80</td>
<td>$96.70</td>
<td>$98.63</td>
<td>$100.60</td>
<td>$102.62</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Data Manager</td>
<td>$140.74</td>
<td>$143.55</td>
<td>$146.42</td>
<td>$149.35</td>
<td>$152.34</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Computer Operations Manager</td>
<td>$95.78</td>
<td>$97.69</td>
<td>$99.65</td>
<td>$101.64</td>
<td>$103.67</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Communications Engineer</td>
<td>$114.35</td>
<td>$116.63</td>
<td>$118.97</td>
<td>$121.35</td>
<td>$123.77</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Jr. Network Engineer</td>
<td>$115.32</td>
<td>$117.63</td>
<td>$119.98</td>
<td>$122.38</td>
<td>$124.83</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Network Engineer</td>
<td>$125.10</td>
<td>$127.60</td>
<td>$130.15</td>
<td>$132.76</td>
<td>$135.41</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Sr. Network Engineer</td>
<td>$157.35</td>
<td>$160.50</td>
<td>$163.71</td>
<td>$166.98</td>
<td>$170.32</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Principal Network Engineer</td>
<td>$187.65</td>
<td>$191.40</td>
<td>$195.23</td>
<td>$199.13</td>
<td>$203.12</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Network Administrator</td>
<td>$104.57</td>
<td>$106.67</td>
<td>$108.80</td>
<td>$110.98</td>
<td>$113.19</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Sr. Network Administrator</td>
<td>$124.12</td>
<td>$126.60</td>
<td>$129.14</td>
<td>$131.72</td>
<td>$134.35</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Hardware Specialist</td>
<td>$96.76</td>
<td>$98.69</td>
<td>$100.66</td>
<td>$102.68</td>
<td>$104.73</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Quality Assurance/IV&amp;V Analyst</td>
<td>$78.19</td>
<td>$79.75</td>
<td>$81.35</td>
<td>$82.97</td>
<td>$84.63</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Quality Assurance/IV&amp;V Specialist</td>
<td>$81.12</td>
<td>$82.74</td>
<td>$84.40</td>
<td>$86.08</td>
<td>$87.81</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Quality Assurance IV&amp;V Manager</td>
<td>$131.94</td>
<td>$134.58</td>
<td>$137.27</td>
<td>$140.02</td>
<td>$142.82</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Configuration Management Specialist</td>
<td>$97.73</td>
<td>$99.69</td>
<td>$101.68</td>
<td>$103.72</td>
<td>$105.79</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Sr. Configuration Mgt. Specialist</td>
<td>$119.23</td>
<td>$121.62</td>
<td>$124.05</td>
<td>$126.53</td>
<td>$129.06</td>
</tr>
<tr>
<td>54151S, 54151HEAL, 54151HACS</td>
<td>Training Specialist/Instructor</td>
<td>$81.12</td>
<td>$82.74</td>
<td>$84.40</td>
<td>$86.08</td>
<td>$87.81</td>
</tr>
<tr>
<td>54151S, 54151HEAL, 54151HACS</td>
<td>Sr. Training Specialist/Instructor</td>
<td>$107.51</td>
<td>$109.66</td>
<td>$111.85</td>
<td>$114.09</td>
<td>$116.37</td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Testing and Validation Specialist</td>
<td>$73.30</td>
<td>$74.77</td>
<td>$76.26</td>
<td>$77.79</td>
<td>$79.34</td>
</tr>
<tr>
<td>Code</td>
<td>Position</td>
<td>Junior</td>
<td>Intermediate</td>
<td>Senior</td>
<td>Sr. Senior</td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>----------</td>
<td>--------------</td>
<td>----------</td>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td>54151S, 54151HEAL, 54151HACS</td>
<td>Senior Testing and Validation Specialist</td>
<td>$106.53</td>
<td>$108.66</td>
<td>$110.83</td>
<td>$113.05</td>
<td></td>
</tr>
<tr>
<td>54151S, 54151HEAL, 54151HACS</td>
<td>Instructional System Designer</td>
<td>$85.03</td>
<td>$86.73</td>
<td>$88.46</td>
<td>$90.23</td>
<td></td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Sr. Instructional System Designer</td>
<td>$100.66</td>
<td>$102.68</td>
<td>$104.73</td>
<td>$106.83</td>
<td></td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Graphic Design Specialist</td>
<td>$76.23</td>
<td>$77.76</td>
<td>$79.31</td>
<td>$80.90</td>
<td></td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Sr. Graphic Design Specialist</td>
<td>$89.91</td>
<td>$91.71</td>
<td>$93.55</td>
<td>$95.42</td>
<td></td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Contract Administrator</td>
<td>$87.96</td>
<td>$89.72</td>
<td>$91.51</td>
<td>$93.34</td>
<td></td>
</tr>
<tr>
<td>54151S, 54151HEAL, 54151HACS</td>
<td>Sr. Contract Administrator</td>
<td>$103.60</td>
<td>$105.67</td>
<td>$107.78</td>
<td>$109.94</td>
<td></td>
</tr>
<tr>
<td>54151S, 54151HEAL, 54151HACS</td>
<td>Documentation Specialist</td>
<td>$87.96</td>
<td>$89.72</td>
<td>$91.51</td>
<td>$93.34</td>
<td></td>
</tr>
<tr>
<td>54151S, 54151HEAL, 54151HACS</td>
<td>Technical Editor</td>
<td>$95.78</td>
<td>$97.69</td>
<td>$99.65</td>
<td>$101.64</td>
<td></td>
</tr>
<tr>
<td>54151S, 54151HEAL</td>
<td>Project Coordinator</td>
<td>$77.21</td>
<td>$78.75</td>
<td>$80.33</td>
<td>$81.93</td>
<td></td>
</tr>
<tr>
<td>54151S, 54151HEAL, 54151HACS</td>
<td>Program Manager</td>
<td>$171.03</td>
<td>$174.45</td>
<td>$177.94</td>
<td>$181.50</td>
<td></td>
</tr>
<tr>
<td>54151S, 54151HEAL, 54151HACS</td>
<td>Sr. Program Manager</td>
<td>$181.78</td>
<td>$185.42</td>
<td>$189.13</td>
<td>$192.91</td>
<td></td>
</tr>
<tr>
<td>54151S, 54151HEAL, 54151HACS</td>
<td>Project Manager</td>
<td>$153.44</td>
<td>$156.51</td>
<td>$159.64</td>
<td>$162.83</td>
<td></td>
</tr>
<tr>
<td>54151S, 54151HEAL, 54151HACS</td>
<td>Sr. Project Manager</td>
<td>$170.06</td>
<td>$173.46</td>
<td>$176.93</td>
<td>$180.46</td>
<td></td>
</tr>
<tr>
<td>54151S, 54151HEAL, 54151HACS</td>
<td>Computer Network Defense (CND) Analyst - Junior</td>
<td>$96.76</td>
<td>$98.69</td>
<td>$100.66</td>
<td>$102.68</td>
<td></td>
</tr>
<tr>
<td>54151S, 54151HEAL, 54151HACS</td>
<td>Computer Network Defense (CND) Analyst - Senior</td>
<td>$168.10</td>
<td>$171.46</td>
<td>$174.89</td>
<td>$178.39</td>
<td></td>
</tr>
<tr>
<td>54151S, 54151HEAL, 54151HACS</td>
<td>Security Architect - Junior</td>
<td>$135.85</td>
<td>$138.57</td>
<td>$141.34</td>
<td>$144.16</td>
<td></td>
</tr>
<tr>
<td>54151S, 54151HEAL, 54151HACS</td>
<td>Security Architect - Intermediate</td>
<td>$170.06</td>
<td>$173.46</td>
<td>$176.93</td>
<td>$180.46</td>
<td></td>
</tr>
<tr>
<td>54151S, 54151HEAL, 54151HACS</td>
<td>Security Architect - Senior</td>
<td>$207.19</td>
<td>$211.34</td>
<td>$215.56</td>
<td>$219.88</td>
<td></td>
</tr>
<tr>
<td>54151S, 54151HEAL, 54151HACS</td>
<td>Information Assurance Analyst - Junior</td>
<td>$109.38</td>
<td>$111.57</td>
<td>$113.80</td>
<td>$116.08</td>
<td></td>
</tr>
<tr>
<td>54151S, 54151HEAL, 54151HACS</td>
<td>Information Assurance Analyst - Intermediate</td>
<td>$142.75</td>
<td>$145.61</td>
<td>$148.52</td>
<td>$151.49</td>
<td></td>
</tr>
<tr>
<td>54151S, 54151HEAL, 54151HACS</td>
<td>Information Assurance Analyst - Senior</td>
<td>$172.41</td>
<td>$175.86</td>
<td>$179.38</td>
<td>$182.97</td>
<td></td>
</tr>
<tr>
<td>54151S, 54151HEAL, 54151HACS</td>
<td>Penetration Tester - Intermediate</td>
<td>$142.69</td>
<td>$145.54</td>
<td>$148.45</td>
<td>$151.42</td>
<td></td>
</tr>
<tr>
<td>54151S, 54151HEAL, 54151HACS</td>
<td>Penetration Tester - Senior</td>
<td>$160.28</td>
<td>$163.49</td>
<td>$166.76</td>
<td>$170.09</td>
<td></td>
</tr>
<tr>
<td>54151S, 54151HEAL, 54151HACS</td>
<td>Cybersecurity Engineer - Junior</td>
<td>$89.91</td>
<td>$91.71</td>
<td>$93.55</td>
<td>$95.42</td>
<td></td>
</tr>
<tr>
<td>54151S, 54151HEAL, 54151HACS</td>
<td>Cybersecurity Engineer - Intermediate (Certificate and Encryption Services)</td>
<td>$124.12</td>
<td>$126.60</td>
<td>$129.14</td>
<td>$131.72</td>
<td></td>
</tr>
<tr>
<td>Position</td>
<td>Grades</td>
<td>Pay Range</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------------</td>
<td>--------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cybersecurity Engineer - Senior</td>
<td></td>
<td>$161.26 - $174.55</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cybersecurity Technical Writer - Junior</td>
<td></td>
<td>$81.12 - $87.81</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cybersecurity Technical Writer - Intermediate</td>
<td></td>
<td>$116.30 - $125.89</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CyberSecurity Assessment and Authorization (A&amp;A) Analyst - Junior</td>
<td></td>
<td>$105.55 - $114.25</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CyberSecurity Assessment and Authorization (A&amp;A) Analyst - Intermediate</td>
<td></td>
<td>$140.74 - $152.34</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CyberSecurity Assessment and Authorization (A&amp;A) Analyst - Senior</td>
<td></td>
<td>$177.87 - $192.54</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Security Analyst (Data Protection) - Junior</td>
<td></td>
<td>$130.58 - $141.34</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Security Analyst (Data Protection) - Intermediate</td>
<td></td>
<td>$163.22 - $176.68</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Security Analyst (Data Protection) - Senior</td>
<td></td>
<td>$197.68 - $213.98</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability Management Analyst - Junior</td>
<td></td>
<td>$136.83 - $148.11</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability Management Analyst - Intermediate</td>
<td></td>
<td>$171.03 - $185.13</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability Management Analyst - Senior</td>
<td></td>
<td>$208.17 - $225.33</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud Computing Security Specialist (CCSS) - Staff</td>
<td></td>
<td>$154.16 - $166.86</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud Computing Security Specialist (CCSS) - Intermediate</td>
<td></td>
<td>$191.34 - $207.11</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud Computing Security Specialist (CCSS) - Senior</td>
<td></td>
<td>$245.74 - $266.00</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operational Technology Security Engineer - Junior</td>
<td></td>
<td>$128.03 - $138.58</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operational Technology Security Engineer - Intermediate</td>
<td></td>
<td>$163.21 - $176.67</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operational Technology Security Engineer - Senior</td>
<td></td>
<td>$200.35 - $216.87</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

Systems Security Engineer (Patching)

Minimum/General Experience:
Requires some experience and at least two years' directly related experience in patching systems. Also requires knowledge of the principles, methods, and techniques used in the engineering, development, maintenance, and application of multiple operating systems; knowledge of or certification in one or more specific applications or processes may be required, depending on job assignment; must have the ability to write, maintain, and modify technical documentation/specifications.

Education: Associate’s Degree

Functional Responsibility:
Assists in the design, development, analysis, installation, maintenance, operation and servicing of computer operating/hardware systems within a secure environment; provides customer support; works under direct supervision; does related work as required.

Systems Engineer (Advanced Troubleshooting)

Minimum/General Experience: Must have three years’ experience of which at least one year must be specialized. Specialized experience includes analytically solving workflows, organization, and/or planning problems. General experience includes increasing responsibilities in systems engineering.

Functional Responsibility: Designs software tools and subsystems to support software reuse and domain analysis within a cybersecurity environment. Interprets software requirements and design specifications to code and integrates and tests software components.

Education: Bachelor’s Degree

Sr. Systems Engineer

Minimum/General Experience: Must have seven or more years' directly related experience in all phases of systems engineering. Also requires advanced knowledge of the principles, methods, and techniques used in all phases of the engineering, application, and development of multiple operating systems; knowledge of or certification in specific applications or processes may be required, depending on job assignment.

Functional Responsibility: Ensures the stability, integrity, and efficient operation of the inhouse information systems that support core organizational functions. This is achieved by monitoring, maintaining, supporting, and optimizing all networked software and associated operating systems. The Senior Systems Engineer will apply proven communication, analytical, and problem-solving skills to help identify, communicate, and resolve issues in order to maximize the benefit of IT systems investments. This individual will also mentor and provide guidance to the Systems Engineer staff. determines data requirements for internal processes and external interfaces; develops new systems or tailors commercial products to meet user requirements; directs and coordinates all activities necessary to complete a major engineering project or several small projects to specification and on schedule; may serve as task or project lead, exercising leadership in either a technical role training other hardware engineers and implementing and enforcing established standards and technologies, or in a project coordination role leading tasks

FEDERAL SUPPLY SCHEDULE PRICE LIST
Wise Technical Innovations LLC
Contract Number: 47QTCA20D0072
and assuming responsibility for the design, development, test and delivery of a software system or applications.

Education: Bachelor’s Degree

Database Architect

Minimum/General Experience: Requires at least three years’ directly related experience in the design, maintenance, and coding of secure environment databases. Also requires knowledge of the principles, methods, and techniques used in all phases of database development, coding, and design, including business analysis, event modeling, logical and physical database design, data access analysis and design, DBMS optimization, archive and recovery strategy, load strategy design and implementation, security, and change management.

Functional Responsibility: Designs, maintains, enhances, and codes relational databases within a cybersecurity environment; analyzes and determines information needs and elements, data relationships and attributes, data flow and storage requirements, and data output and reporting capabilities; develops data modeling and participates in data acquisition and access analysis and design, and archive, recovery, and load strategy design and implementation; coordinates new data development ensuring consistency and integration with existing data warehouse structure; reviews requests for data and data usage, researches data sources for new and better data feeds; participates in continuous improvement efforts in enhancing performance and providing increased functionality; designs data structures to accommodate database production, storage, maintenance, and accessibility; develops screens and queries; tests designed applications; performs upgrades and maintenance of hardware and software; provides technical support and guidance to users; maintains current knowledge of relevant hardware and software applications as assigned; may serve as team or technical task lead; participates in special projects as required.

Education: Bachelor’s Degree

Sr. Database Architect

Minimum/General Experience: Requires at least five years’ directly related experience in the design, maintenance, and coding of secure environment databases. Also requires advanced knowledge of the principles, methods, and techniques used in all phases of database development, coding, and design, including business analysis, event modeling, logical and physical database design, data access analysis and design, DBMS optimization, archive and recovery strategy, load strategy design and implementation, security, and change management.

Functional Responsibility: Designs, maintains, enhances, and codes relational databases within a cybersecurity environment; analyzes and determines information needs and elements, data relationships and attributes, data flow and storage requirements, and data output and reporting capabilities; develops data modeling and is responsible for data acquisition and access analysis and design, and archive, recovery, and load strategy design and implementation; coordinates new data development ensuring consistency and integration with existing data warehouse structure; reviews business requests for data and data usage, researches data sources for new and better data feeds; participates in continuous improvement efforts in enhancing performance and providing increased functionality; designs data structures to accommodate database
production, storage, maintenance, and accessibility; develops screens and queries; tests
designed applications; may perform upgrades and maintenance of hardware and software;
provides technical support and guidance to users; maintains current knowledge of relevant
hardware and software applications as assigned; may serve as team or technical task lead and
provide guidance and training to lower-level staff; participates in special projects as required.
Education: Bachelor’s Degree

Computer Programmer/Analyst

Minimum/General Experience: Must have at least two years’ experience in the secure
environment computer programming field. Depending on the job assignment, knowledge of or
certification in specific applications or processes may be required in the following areas: Web
technologies, design technologies, specific programming languages, authoring languages and
systems, and Modeling and Simulation (M&S) technologies, processes, and tools.
Functional Responsibility: Generates new code and corrects, converts, and/or modifies existing
code to meet documented standards within a cybersecurity environment; designs new and/or
redesigns and maintains existing software products; identifies client needs and requirements
based on evaluation of client documentation and interviews; performs data and technical
analysis; performs a variety of testing procedures on assigned products, analyzes test results,
and corrects problems; prepares test scripts and descriptions and examines to locate necessary
modifications; analyzes and modifies program specifications and documentation to support
contract requirements; may design and develop computer-based and/or multimedia courseware
for customer training initiatives utilizing appropriate authoring languages, systems, animation and
graphics software; provides customer support to clients and troubleshoots problems.
Education: Associate’s Degree

Sr. Computer Programmer/Analyst

Minimum/General Experience: Requires at least five years’ experience in the secure environment
computer programming field. Depending on the job assignment, knowledge of or certification in
specific applications or processes may be required in the following areas: Web technologies,
design technologies, specific programming languages, authoring languages and systems, and
Modeling and Simulation (M&S) technologies, processes, and tools.
Functional Responsibility: Participates in all phases of software development, including system
design, analysis, architecture, and engineering; programs, designs, analyzes, codes, implements,
and tests software applications, modules, and databases in various languages, including those
associated with scientific, technical, or engineering problems within a cybersecurity environment;
performs process analyses in order to recommend improvements; performs system, network,
and/or database administration, analysis, design, implementation, and testing; analyzes and
documents client needs and requirements; provides technical support including providing
technical solutions and training; writes, modifies, and maintains software documentation and
specifications; Performs a variety of testing for computer operating and/or network systems;
performs data and technical analysis and information engineering; installs, configures, and
troubleshoots various hardware and software platforms; may design and develop computer
based and/or multimedia courseware for customer training initiatives utilizing appropriate
authoring languages, systems, animation and graphics software; participates in meetings and
design reviews; prepares reports on analyses, findings, and project progress; performs technical

FEDERAL SUPPLY SCHEDULE PRICE LIST
Wise Technical Innovations LLC
Contract Number: 47QTCA20D0072
research on emerging technologies to determine impacts on application execution; may serve as a technical task or team lead.
Education: Bachelor’s Degree

**Web Designer/Developer (Sharepoint Tickets)**

Minimum/General Experience: Requires at least three years’ experience in secure environment software development, installation, and modification in an online environment.  
Functional Responsibility: Provides application development and technical support for internal and external Webs within a cybersecurity environment; develops Web pages and applications for customers; collaborates with graphic artists to develop Web page graphics that support interactive, marketing-focused content; provides technical consultation in new systems development, new package evaluations and enhancements of existing systems; prepares functional specifications from which programs will be written, then designs, codes, tests, debugs and documents programs; participates in the technical design, development, testing, implementation and maintenance of Web site enhancements; plans, schedules and conducts systems tests, monitors test results, and takes appropriate corrective action; may prepare technical user guides.
Education: Associate’s Degree

**Sr. Web Developer (DRL Advanced Troubleshooting and Maintenance)** Minimum/General Experience: Requires at least five years’ experience, of which at least two years must include technical leadership experience and at least four years’ experience in secure environment software development, installation, and modification in an online environment.  
Functional Responsibility: Designs and develops well-integrated and cost-effective solutions for internal and external Webs within a cybersecurity environment; works closely with client project managers and technical leaders to understand customers’ business objectives and systems requirements; designs and develops Web infrastructures; designs and implements an intranet strategy for authorization of users to access controlled components; designs relational databases to perform well logically and physically for decision support; coordinates enhancements and maintenance of Web systems and sites; provides recommendations for server operating systems, hardware requirements and encryption standards for communications to and from secure servers; provides technical advice and expertise to Webmasters and Web developers in the installation, acceptance testing, and evaluation of newly released and beta software; may serve as a functional/technical team or task lead.
Education: Bachelor’s Degree

**Web Tech Administrator**

Minimum/General Experience: Requires at least three years’ experience in secure environment systems technology. Must understand federal information security/assurance policies, standards and regulations.  
Functional Responsibility: Responsible for achieving overall technical integrity of organization’s Website within a cybersecurity environment. Maintains and upgrades hardware and software including website technical architecture related to hardware and telecommunication connectivity. Administers email, chat, and FTP and HTTP services. Communicates router configuration changes and troubleshoots system errors and bugs. Maintains servers, creates monitoring
reports and logs, and ensures functionality of links. Monitors site for acceptable performance and user accessibility. Establishes backups and monitors site security.
Education: Bachelor’s Degree

Web Content Manager

Minimum/General Experience: Requires at least two years’ experience in secure environment production management, Web page design, Web design languages, and Web graphics types and standards.
Functional Responsibility: Responsible for developing and providing content within a cybersecurity environment that will motivate and entertain users so that they regularly access the Website and utilize it as a major source for information and decision making. Responsible for managing/performing Website editorial activities including gathering and researching information that enhances the value of the site. Locates, negotiates, and pursues content. Seeks out customers to gather feedback for Website improvement and enhancements.
Education: Associate’s Degree

Computer Systems Analyst

Minimum/General Experience: Must have at least three years of computer experience in assignments of a secure environment technical nature working under close supervision and direction. Must have at least one-year experience in analyzing and programming applications on large-scale on mid-tier computers (or LAN-based) with a minimum of one year of design and programming of moderately complex ADP systems.
Functional Responsibility: Develops requirements for information systems from a project's inception to conclusion. Develops required specifications for simple to moderately complex systems within a cybersecurity environment. Assists senior computer systems analyst in preparing input and test data for the proposed system.
Education: Bachelor’s Degree

Sr. Computer Systems Analyst

Minimum/General Experience: Must have seven years of computer experience working independently or under general direction on complex secure environment application problems involving all phases of systems analysis. At least five years’ experience in analysis and design of business applications for complex, large-scale or mid-tier computer systems, or LAN-based systems.
Functional Responsibility: Analyzes and evaluates user needs and identifies resources required for each task to determine functional requirements within a cybersecurity environment; conceptualizes, develops, and implements complex systems designed to meet client requirements; defines systems objectives and prepares system design specifications to meet requirements; designs, develops, implements, and tests new systems or modifies existing systems that meet the user’s needs; codes applications and tests to software requirements; writes or updates software specifications; analyzes procedures and systems to refine their formulation and convert to programmable formats; analyzes data requirements to determine data source and destinations; coordinates with client to define problem, determine data availability, report requirements, and resolve system design problems; creates logical data models based on functional requirements; performs quality review of specifications for internal and external

FEDERAL SUPPLY SCHEDULE PRICE LIST
Wise Technical Innovations LLC
Contract Number: 47QTCA20D0072
delivery; troubleshoots and provides technical support and solutions to users; develops analytical tools for use in the design and redesign of programs as assigned; may serve as a technical team or task lead.

Education: Bachelor’s Degree

Disaster Recovery Specialist

Minimum/General Experience: Must have at least five years’ experience, of which at least three years must be secure environment. Experienced in designing, implementing, and managing various DR technologies. Must have a strong knowledge of accompanying storage solutions.

Functional Responsibility: This role will work with other key leaders of the IT organization, and system developers to ensure proper technology risk considerations are addressed at each phase of the system development life cycle (SDLC) and provide proactive solutions to correct exposures or mitigate risk.

Interpret security standards, procedures, and guidelines for multiple platforms and diverse environments (e.g. client server, distributed, mainframe, etc.) in designing solutions, recommending enhancements or defining mitigating controls to existing systems. The individual should demonstrate an understanding of application security and will exercise sound judgment within existing practices and policies.

Maintain responsibility for developing, maintaining and updating the business continuity plan to be used in the event of an unexpected outage that significantly impacts our end user’s ability to consume IT services through our normal channels. In partnership with the established IT disaster recovery team, the individual will be responsible for identifying solutions and vendors that can help us minimize disruption to the business and ensure ongoing operations are possible within established RTO guidelines.

This opportunity is perfect for an IT professional who is looking to grow their career with an industry leader. You will focus on critical business initiatives and collaborate with senior IT leaders in region and globally. This is a unique opportunity for you to advance your career with a proven leader in the cement and construction materials industry.

Education: Bachelor’s Degree

Backup/Restore Administrator

Minimum/General Experience: Must have at least three years’ experience backing up and restoring data in secure enterprise environment. Experienced in working with various DR technologies.

Functional Responsibility: Provides highly technical expertise and guidance in the design, implementation, operation and maintenance of database management systems (DBMS) within a cybersecurity environment. Evaluates and recommends available DBMS products after matching requirements with system capabilities. Determines file organization, indexing methods, and security procedures for specific applications. Controls the design and use of databases. Controls the global view of databases, controls the access to the databases, assures the safekeeping of the databases (from accidental or intentional damage or loss), and monitors the use of databases. Must be capable of defining all required database administration policies, procedures, standards, and guidelines. Is an authority on the design of databases and the use of database management systems. Evaluates and recommends available DBMS products after matching
requirements with system capabilities. Prepares and delivers presentations on DBMS concepts.
Education: Bachelor’s Degree

Data Manager

Minimum/General Experience: Must have at least five years’ experience, of which at least five
must be secure environment specialized. Specialized experience includes demonstrated
experience using current DBMS technologies, application design utilizing various database
management systems and experience with DBMS internals. General experience includes
increasing responsibilities in DBMS systems analysis and programming. Must demonstrate the
ability to work independently or under only general direction.
Functional Responsibility: Manages the development of database projects within a cybersecurity
environment. Plans and budgets staff and database resources. When necessary, reallocates
resources to maximize benefits. Prepares and delivers presentations on Database Management
Systems (DBMS) concepts. Provides daily supervision and direction to support staff.
Education: Bachelor’s Degree

Computer Operations Manager

Minimum/General Experience: Must have at least five years’ experience, of which at least three
years are secure environment specialized. Specialized experience includes supervision and
operations experience on a large-scale computer system, knowledge of hardware, software and
operating systems. General experience includes operations experience on a large-scale
computer system.
Functional Responsibility: Manages the work of computer operations personnel within a
cybersecurity environment; identifies processing requirements and schedules job streams for
computer runs; responsible for security and routing of input and output data, problem resolution
and restart/recovery, interpreting technical documentation standards and preparation of
documentation according to standards; interfaces with client and/or other government personnel;
determines appropriate course of action in case of malfunction and confers with and directs staff
as warranted.
Education: Bachelor’s Degree

Communications Engineer

Minimum/General Experience: Must have at least seven years of general experience with secure
environment telecommunications systems including three years of specialized experience.
Functional Responsibility: Provides technical support for telecommunications activities including
planning, designing, installing, and maintaining large telecommunications networks within a
cybersecurity environment. Develops, operates, and maintains voice, video, and/or data
communications systems. Applies telecommunications engineering principles and theory to
propose design and configuration alternatives. Evaluates existing communications systems to
identify deficiencies and performance improvements. Consults with user personnel to ensure that
problems have been properly identified and that the solution will meet the requirements. Analyzes
system performance, usage and traffic flows, accesses and interfaces, transmission techniques,
and protocols. Performs system analyses and feasibility studies concerning communications and
communication networks. Prepares studies and gives presentations on communications
concepts. Provides technical guidance to other personnel concerning data communications
requirements. Participates in preparing specifications for acquiring commercially available data communications networks.
Education: Bachelor’s Degree

**Jr. Network Engineer**

Minimum/General Experience: This position requires one year of experience or up to six years’ related secure environment network design/administration experience. Also requires knowledge of the principles, methods, and techniques used in network administration and engineering plus knowledge of and ability to use relevant hardware, software and other equipment. Certification in specific applications may be required, depending on job assignment.
Functional Responsibility: Performs basic engineering work concerned with the analysis, planning, designing, evaluating, selecting, and upgrading of network systems within a cybersecurity environment; performs various tests and documents results; administers and maintains local and wide area networks; provides technical support and troubleshooting to users; configures systems to user environments; assists in telecommunications activities including planning, designing, installing, and maintaining large telecommunications networks; assists in the maintenance and operation of voice, video, and data communications systems; supports the acquisition of hardware and software as well as subcontractor services as needed.
Education: Associate’s Degree

**Network Engineer**

Minimum/General Experience: Must have at least two 3 years’ related secure environment network design/administration experience. Also requires knowledge of the principles, methods, and techniques used in network administration and engineering plus knowledge of and ability to use relevant hardware, software and other equipment. Certification in specific applications may be required, depending on job assignment.
Functional Responsibility: Analyzes local and wide area network systems, including planning, designing, evaluating, selecting, and upgrading operating systems and protocol suites and configuring communication media with concentrators, bridges, and other devices within a cybersecurity environment; resolves interoperability problems to obtain operations across all platforms including email, file transfer, multimedia, teleconferencing, and the like; configures systems to user requirements; supports the acquisition of hardware and software as well as subcontractor services as needed; performs various tests and documents results; administers and maintains local and wide area networks; provides technical support and troubleshooting to users; plans network layout design; may administer network security.
Education: Bachelor’s Degree

**Sr. Network Engineer**

Minimum/General Experience: Must have at least seven years’ related secure environment network design/administration experience. Also, must have advanced knowledge of the principles, methods, and techniques used in network administration and engineering plus
advanced knowledge of and ability to use relevant hardware, software and other equipment is required.

Functional Responsibility: Analyzes local and wide area network systems, including planning, designing, evaluating, selecting, and upgrading operating systems and protocol suites and configuring communication media with concentrators, bridges, and other devices within a cybersecurity environment; resolves interoperability problems to obtain operations across all platforms including email, file transfer, multimedia, teleconferencing, and the like; configures systems to user requirements; supports the acquisition of hardware and software as well as subcontractor services as needed; performs various tests and documents results; administers and maintains local and wide area networks; provides technical support and troubleshooting to users; plans network layout design; may administer network security; may perform database administration; may supervise and direct the work of lower level personnel; may serve as technical team or task lead.

Education: Bachelor’s Degree

Principal Network Engineer

Minimum/General Experience: Must have at least seven or more years’ related secure environment network design/administration experience. Expert knowledge of the principles, methods, and techniques used in network administration and engineering plus expert knowledge of and ability to use relevant hardware, software and other equipment is required.

Functional Responsibility: Provides expert level analysis of local and wide area network systems, including planning, designing, evaluating, selecting, and upgrading operating systems and protocol suites and configuring communication media with concentrators, bridges, and other devices within a cybersecurity environment; resolves interoperability problems to obtain operations across all platforms including email, file transfer, multimedia, teleconferencing, and the like; configures systems to user requirements; supports the acquisition of hardware and software as well as subcontractor services as needed; directs various testing and the documentation of results; plans network layout design; may administer network security; may perform database administration; may supervise and direct the work of lower level personnel; serves as technical team or task lead.

Education: Bachelor’s Degree

Network Administrator

Minimum/General Experience: Requires at least three years’ experience. Also requires knowledge of the principles, methods, and techniques used in secure environment network troubleshooting and support as well as knowledge of operating systems and applications and network management. Must have working knowledge of current technologies and products for Web services and security.

Functional Responsibility: Supports, installs, maintains, troubleshoots, and coordinates the usage of local and wide area networks (LAN and WAN), electronic mail, telecommunications, and PC based systems and related software within a cybersecurity environment; evaluates hardware and software, including peripheral, output, and telecommunications equipment; sets up and administers security procedures; troubleshoots problems; recommends and implements LAN policies and procedures and ensures adherence to security procedures; trains users on LAN operations and procedures.

Education: Bachelor’s Degree
Sr. Network Administrator

Minimum/General Experience: Requires seven or more years’ experience. Also requires knowledge of the principles, methods, and techniques used in secure environment network troubleshooting and support, operating systems and applications and network management. Must have working knowledge of current technologies and products for Web services and security. Functional Responsibility: Responsible for the planning, design, acquisition, installation, and maintenance of LAN and WAN, electronic mail, telecommunications, and PC based systems and related software within a cybersecurity environment; evaluates hardware and software, including peripheral, output, and telecommunications equipment; sets up and administers security procedures; troubleshoots problems; establishes and implements LAN policies and their conformance; coordinates activities of LAN support personnel, providing guidance on common networking issues; assesses vendor products; manages network performance, troubleshoots problems, and maintains network security.

Education: Bachelor’s Degree

Hardware Specialist

Minimum/General Experience: Must have at least two years’ progressive experience in systems analysis with three years’ intensive and progressive specific experience in the specialty. Functional Responsibility: Determines feasible hardware alternatives in client server cybersecurity environments. Reviews computer systems in terms of capabilities and makes recommendations for improved utilization. Prepares or directs preparation of reports concerning hardware. Prepares or participates in preparing functional requirements and specifications for hardware acquisitions.

Education: Associate’s Degree

Quality Assurance/IV&V Analyst

Minimum/General Experience: Must have at least two years’ related experience in secure environment quality assurance and/or software engineering. Must also have experience with Independent Validation and Verification (IV&V) and system configuration. Functional Responsibility: Assists in the review and evaluation of software products and systems to ensure adherence to customer quality standards within a cybersecurity environment; develops software/systems testing procedures and conducts tests; analyzes and documents IV&V issues; presents IV&V results; works under general supervision.

Education: Associate’s Degree

Quality Assurance/IV&V Specialist

Minimum/General Experience: Must have at least three years’ experience of which two years must be specialized. Specialized experience includes: secure environment Configuration Management, IV&V, software testing and integration, software metrics and their application to
software quality assessment. General experience includes increasing responsibilities in quality assurance, quality control and IV&V.

Functional Responsibility: Assists in the evaluation of software and associated documentation within a cybersecurity environment. Participates in formal and informal reviews to determine quality; presents IV&V results and troubleshoots technical problems; makes recommendations to improve overall quality.

Education: Bachelor’s Degree

Quality Assurance IV&V Manager

Minimum/General Experience: Must have at least five years of Security IT or cybersecurity engineering and/or system analysis and programming experience, including four years of quality assurance, IV&V or system configuration experience.

Functional Responsibility: Organizes and maintains all quality assurance and IV&V documentation required within a cybersecurity environment. Responsible for ensuring compliance with recognized standards and practices. Reviews all documentation for completeness, accuracy, and correctness. Supports the test and integration personnel as a witness to testing requirements; presents IV&V results and troubleshoots technical problems; makes recommendations to improve overall quality. Certifies that deliverables have met all quality requirements.

Education: Bachelor’s Degree

Configuration Management Specialist

Minimum/General Experience: Must have five years of engineering and/or Security IT or cybersecurity system analysis and programming experience, including two years of configuration management experience.

Functional Responsibility: Responsible for configuration management activities including product identification, change control, status accounting, operation of the program support library, and development and monitoring of equipment/system acceptance plans within a cybersecurity environment. Evaluates and selects configuration management tools and standards. Coordinates with users and systems development personnel on releases of both system-level software and applications software. Verifies the completeness and accuracy of release libraries before implementation and ensures that correct versions of programs are included in specified releases. Prepares configuration management plans and procedures. Responsible for configuration management of requirements, design, and code. Operates and manages program support library. Monitors library structure and procedures to assure system integrity, including procedures for collection, release, production, test, and emergency libraries and the movement/migration of components between libraries. Monitors end item acceptance plans. Will supervise lower level personnel. Must have demonstrated capability for oral and written communications.

Education: Bachelor’s Degree

Sr. Configuration Management Specialist
Minimum/General Experience: Must have at least seven years’ directly related experience in secure environment configuration management and support. Must also have advanced knowledge of the principles, methods, and techniques used in configuration management and support as well as knowledge and familiarity with Configuration Management software support packages commonly utilized in project management. Must be able to supervise and direct the work of others and can serve as a technical team or task lead.

Functional Responsibility: Conducts periodic site inventory in order to create and maintain inventories of equipment, software, and/or systems; prepares, maintains and inventories associated technical drawings for assigned projects within a cybersecurity environment; researches data, and creates and maintains inventory and other databases for assigned projects; prepares configuration change requests and verifies, tracks, and documents configuration changes; performs logistic-related tasks like shipping/receiving, tracking, and disposal of equipment, software, and/or systems; coordinates equipment/software utilization among individual users; provides documentation support for assigned projects; performs quality assurance checks on drawings prepared by other configuration management specialists; may serve as a team or task lead; may supervise and direct the work of other configuration management specialists; provides training on configuration management processes, software, and/or systems.

Education: Bachelor’s Degree

Training Specialist/Instructor

Minimum/General Experience: Must have two years’ experience in secure environment information systems development, training, or related fields. Must have two years specialized experience. Specialized experience includes experience in developing and providing IT and end-user training on computer hardware and application software. General experience includes information systems development, training, or related fields. Demonstrated ability to communicate orally and in writing.

Functional Responsibility: Conducts the research necessary to develop and revise training courses within a cybersecurity environment. Develops and revises these courses and prepares appropriate training catalogs. Prepares all instructor materials (course outline, background material, and training aids). Prepares all student materials (course manuals, workbooks, handouts, completion certificates, and course critique forms). Trains personnel by conducting formal classroom courses, workshops and seminars.

Education: Associates Degree

Sr. Training Specialist/Instructor

Minimum/General Experience: Must have five years’ experience in secure environment information systems development, training, or related fields, with at least three years’ experience developing and providing IT and end-user training on computer hardware and application software.

Functional Responsibility: Conducts the research necessary to develop and revise training courses and prepares appropriate training catalogs within a cybersecurity environment. Prepares all instructor materials (course outline, background material, and training aids). Prepares all student materials (course manuals, workbooks, handouts, completion certificates, and course
critique forms). Trains personnel by conducting formal classroom courses, workshops, and seminars. Provides daily supervision and direction to staff.

Education: Bachelor’s Degree

Testing and Validation Specialist

Minimum/General Experience: Requires two years’ experience or up to three years’ related experience in secure environment educational psychology, industrial/organizational psychology, testing, psychometrics, or instructional media/technology. Also requires knowledge of the principles, methods, and techniques used in analysis and assessment as well as the use and application of related off the shelf tools.

Functional Responsibility: Designs and develops assessment instruments and/or strategies to meet training requirements within a cybersecurity environment; conducts analysis of training requirements (needs, job, task analysis); interviews subject matter experts or incumbents to collect information; develops relevant and measurable assessment criteria, standards, and methodologies; designs reliable and valid assessment materials; gathers data and compiles information into documents related to assessment.

Education: Associate’s Degree

Sr. Testing and Validation Specialist

Minimum/General Experience: Requires at least five years’ related experience in secure environment educational psychology, industrial/organizational psychology, testing, psychometrics, or instructional media/technology. Also requires advanced knowledge of the principles, methods, and techniques used in analysis and assessment as well as the use and application of related off-the-shelf tools. Must have the ability to provide work leadership and supervision to assigned staff.

Functional Responsibility: Designs and develops assessment instruments and/or strategies to meet training requirements within a cybersecurity environment; conducts analysis of training requirements (needs, job, task analysis); interviews subject matter experts or incumbents to collect information; develops relevant and measurable assessment criteria, standards, and methodologies; designs reliable and valid assessment materials; prepares reports and technical documentation related to assessment; works on complex analysis or test development projects. Serves as a technical team/task lead and may have supervisory responsibility.

Education: Bachelor’s Degree

Instructional System Designer

Minimum/General Experience: Requires at least two years’ related experience in secure environment instructional development. Also requires knowledge of the principles, methods, and techniques used in technology-based training as well as the use and application of off the-shelf tools and associated equipment and systems.

Functional Responsibility: Designs and develops instructional approaches and/or strategies to meet training requirements within a cybersecurity environment; conducts analysis of training requirements and media requirements; develops appropriate training objectives and test methods and designs instructionally valid training materials; ensures integrity of task analysis, training requirements, training hierarchies, instructional materials, and evaluation plans; designs and develops computer based training, web-based training, electronic performance support systems
and other technology-based learning solutions; develops flow diagrams and story boards; designs instructionally sound lessons in a variety of delivery media; interacts with customer and subject matter experts to ensure technical accuracy of instructional content.

Education: Associate’s Degree

**Sr. Instructional System Designer**

Minimum/General Experience: Requires at least five years’ related experience in secure environment instructional development as well as thorough knowledge of the principles, methods, and techniques used in technology-based training and use and application of off the shelf tools and associated equipment and systems.

Functional Responsibility: Designs and develops instructional approaches and/or strategies to meet training requirements within a cybersecurity environment; conducts analysis of training requirements and media requirements; develops appropriate training objectives and test methods and designs instructionally valid training materials; ensures integrity of task analysis, training requirements, training hierarchies, instructional materials, and evaluation plans; designs and develops computer based training, web-based training, electronic performance support systems and other technology-based learning solutions; develops flow diagrams and story boards; designs instructionally sound lessons in a variety of delivery media; interacts with customer and subject matter experts to ensure technical accuracy of instructional content; may provide guidance and work leadership to lower-level personnel.

Education: Bachelor’s Degree

**Graphic Design Specialist**

Minimum/General Experience: Requires at least three years’ directly related experience in graphics design. Also requires knowledge of the principles, methods, and techniques used in the preparation of graphics material and associated software and equipment. Requires experience using graphics software programs.

Functional Responsibility: Performs a wide variety of graphics/illustration activities to produce brochures, briefings, displays, and other materials within a cybersecurity environment; involved in all aspects of graphics/illustration projects from conceptualization and development to final presentation; may act as a technical consultant on matters of design, composition and methods of presenting technical data; uses a broad range of graphics production software and equipment; exercises creative judgment and originality by translating needs into graphics capabilities; may participate in website design.

Education: Associate’s Degree

**Sr. Graphic Design Specialist**

Minimum/General Experience: Requires at least seven years’ directly related experience in graphics design. Knowledge of the principles, methods, and techniques used in the preparation of graphics materials as well as knowledge of the associated software and equipment and in-depth knowledge of graphics software programs.

Functional Responsibility: Performs high-level computer graphic design activities to produce brochures, briefings, displays, and other materials within a cybersecurity environment; involved in all aspects of graphics/illustration projects from conceptualization and development to final presentation; may act as a technical consultant on matters of design, composition and methods
of presenting technical data; uses a broad range of graphics production software and equipment; exercises creative judgment and originality by translating needs into graphics capabilities; may participate in website design; provides technical training and guidance to lower level graphics personnel and may act as a team or task lead. 
Education: Bachelor’s Degree

**Contract Administrator**

Minimum/General Experience: Requires at least two years’ related experience in secure environment contracts administration. Also requires thorough knowledge of the practices, procedures, and processes of contracts administration as well as relevant laws, regulations, terms, conditions, and policies governing assigned contracts. 
Functional Responsibility: Performs all duties of contract administration, including negotiation, correspondence, documentation, certification, financial reporting, and product delivery; implements subcontract administration procedures within a cybersecurity environment; negotiates contract terms from proposal stage to project close-out in accordance with relevant regulations; prepares and submits proposals including pricing and scheduling details and coordination of requirements; prepares consulting agreements; modifies contract schedules and participates in vendor reseller agreement negotiations when required; ensures timely processing of technical reports and deliverables; collects data for clients as requested 

Education: Associate’s Degree

**Sr. Contract Administrator**

Minimum/General Experience: Requires at least seven years’ related experience in secure environment contracts administration. Also requires advanced knowledge of the practices, procedures, and processes of contracts administration as well as thorough knowledge of relevant laws, regulations, terms, conditions, and policies governing assigned contracts including Federal Acquisition Regulations (FAR) and labor law. 
Functional Responsibility: Performs all duties of contract administration, including negotiation, correspondence, documentation, certification, financial reporting, and product delivery for complex contracts within a cybersecurity environment; implements subcontract administration procedures; negotiates contract terms from proposal stage to project close-out in accordance with relevant regulations; coordinates approval of negotiations, contracts, and subcontracts with appropriate management staff; provides advice and interpretation of contract requirements; reviews solicitation requests to ensure compliance with terms and conditions; prepares and submits cost proposals including pricing and scheduling details, coordination of requirements, and cost proposal risk assessment; prepares responses to certifications and representations; prepares consulting agreements; modifies contract schedules and participates in vendor reseller agreement negotiations when required; ensures timely processing of technical reports and deliverables; coordinates with program managers to ensure contract requirements are fulfilled; collects data for clients as requested; may provide work leadership to lower level contracts personnel. 
Education: Bachelor’s Degree

**Documentation Specialist**
Minimum/General Experience: Must have two years’ experience in composing and producing technical documentation or one-year experience in composing and producing technical documentation plus a college degree.
Functional Responsibility: Composes and finalizes technical cybersecurity documentation including specifications, user manuals, etc. in the style, content and format required by the relevant standards using input received from technical personnel.
Education: Associate’s Degree

Technical Editor

Minimum/General Experience: Must have at least two years’ directly related experience in the research and preparation of technical materials. Also requires knowledge of the principles and practices of technical research, writing, and editing, as well as word-processing and desktop publishing applications and computer equipment as required.
Functional Responsibility: Prepares and edits a wide variety of complex technical materials within cybersecurity for publication, including user’s manuals, training materials, installation guides, proposals, and reports; reviews, researches, and edits information for preparation of contract deliverables; provides support to the creation of proposals and multi-media presentation materials, including slides; responsible for the coordination of multiple aspects of document publication; participates in the design and development of marketing brochures, conference programs and proceedings, public relations announcements, and other materials when requested; may supervise and direct the work of word processing, graphics and/or technical writing staff; coordinates and attends various conferences and meetings; plans budgets, schedules and priority of work for public
Education: Associate’s Degree

Project Coordinator

Minimum Experience: Requires two years of experience.
Functional Responsibilities: Project coordinators help the project teams manage resources and information and assist with scheduling and planning meetings and project activities. The project coordinator role may include additional duties and responsibilities and require expertise in a specific area, such as IT or human resources.
Minimum Education: Associate’s Degree

Project Manager

Minimum/General Experience: Must have five years of general experience including five years of specialized Cybersecurity or Security IT and of which two years were direct supervisory experience.
Functional Responsibility: Monitors each task and keeps the Program Manager abreast of all problems and accomplishments. Anticipates problems and works to mitigate the anticipated problems. As a team or project leader, provides technical direction for the complete systems development effort. May serve as a technical authority for a design area. As a cybersecurity specialist or consultant, resolves unique and unyielding systems problems using new technology. Can complete tasks within estimated time frames and budget constraints. Schedules and assigns duties to subordinates. Interacts with government management personnel. Reports in writing and orally to contractor management and government representatives, including the government contracting officer.
Minimum Education: Bachelor’s Degree

Sr Project Manager

Minimum/General Experience: Must have seven years of general experience including five years of specialized Cybersecurity or Security IT and of which two years were direct supervisory experience. Functional Responsibility: Monitors each task and keeps the Program Manager abreast of all problems and accomplishments. Anticipates problems and works to mitigate the anticipated problems. As a team or project leader, provides technical direction for the complete systems development effort. May serve as a technical authority for a design area. As a cybersecurity specialist or consultant, resolves unique and unyielding systems problems using new technology. Can complete tasks within estimated time frames and budget constraints. Schedules and assigns duties to subordinates. Interacts with government management personnel. Reports in writing and orally to contractor management and government representatives, including the government contracting officer.
Minimum Education: Bachelor’s Degree

Program Manager

Minimum/General Experience: Must have at least seven years’ experience, of which at least six years must be specialized in Cybersecurity or Security IT. Specialized experience includes: complete engineering project development from inception to deployment, demonstrated ability to provide guidance and direction in the tasks similar to the sample tasks provided in the statement of work, proven expertise in the management and control of funds and resources, demonstrated capability in managing multi-task contracts of this type and complexity. General experience includes increasing responsibilities in information systems design and management. Functional Responsibility: Serves as the contractor’s contract manager and shall be the contractor’s authorized interface with the Government Contracting Officer (CO), the Contracting Officer’s Representative (COR), government management personnel and customer agency representatives. Responsible for formulating and enforcing work standards, assigning contractor schedules, reviewing work discrepancies, supervising contractor personnel and communicating policies, purposes, and goals of the organization to subordinates within a cybersecurity environment. Shall be responsible for the overall contract performance. Ability to manage and ensure the successful completion multiple technical tasks in assigned program(s).
Minimum Education: Bachelor’s Degree

Sr. Program Manager

Minimum/General Experience: Must have at least 10 years’ experience, of which at least five years must be supervisory experience in the Cybersecurity or Security IT arena. Must have the ability to manage and ensure the successful completion of multiple technical tasks in assigned program(s). Must have the ability to recruit, hire, manage, supervise, train, schedule, coordinate, and evaluate staff as assigned. Functional Responsibility: Responsible for managing very complex and/or high-risk cybersecurity programs. Directs daily staff and task activities to meet client and corporate work objectives. Supervises assigned technical and administrative staff, including subordinate managers. Assures quality of task products, services, and deliverables, including participating in reviews, audits, and site visits. Serves as a liaison with clients to coordinate activities, negotiate tasks, and solve problems. Responsible for coordinating and monitoring subcontractor activities.
Minimum Education: Bachelor’s Degree
Cyber Security Engineer - Junior
Minimum/General Experience: Requires at least two years' directly related experience in secure software engineering or cybersecurity, including the design, coding, testing, and documentation of computer programs. Also requires knowledge of the fundamental concepts, practices and procedures used in software engineering and applications and systems development. Functional Responsibility: Participates in the design, development, analysis, and implementation of software operating systems and software application programs within a cybersecurity environment; works under general supervision; performs software operating systems and application engineering, including full life cycle design and development; works from specifications to develop and modify operating systems and software applications; participates in the design, coding, testing, debugging, and documentation of programs; participates in the definition of limited design specifications and parameters; assists engineers or analysts with the hardware/software integration of the application or utility into software operating systems; analyzes system architecture requirements; performs requirements acquisition and definition and data analysis; may customize purchased applications; performs technical and subject matter research on emerging technologies to determine impacts on application execution; analyzes and documents client needs and requirements; participates in the writing, modifying, and maintaining technical documentation and specifications such as user manuals, system documentation, and training materials; performs integration testing. Reports to Intermediate Cyber Security Engineer.
Education: Associate’s Degree

Cyber Security Engineer – Intermediate (Certification and Encryption Services)
Minimum/General Experience: Requires at least five years' directly related experience in secure software engineering or cybersecurity, including the design, coding, testing, and documentation of computer programs. Also requires knowledge of the fundamental concepts, practices and procedures used in software engineering and applications and systems development. Functional Responsibility: Participates in the design, development, analysis, and implementation of software operating systems and software application programs within a cybersecurity environment; works under general supervision; performs software operating systems and application engineering, including full life cycle design and development; works from specifications to develop and modify operating systems and software applications; participates in the design, coding, testing, debugging, and documentation of programs; participates in the definition of limited design specifications and parameters; assists engineers or analysts with the hardware/software integration of the application or utility into software operating systems; analyzes system architecture requirements; performs requirements acquisition and definition and data analysis; may customize purchased applications; performs technical and subject matter research on emerging technologies to determine impacts on application execution; analyzes and documents client needs and requirements; participates in the writing, modifying, and maintaining technical documentation and specifications such as user manuals, system documentation, and training materials; performs integration testing.
Education: Bachelor’s Degree

Cyber Security Engineer - Senior
Minimum/General Experience: Requires at least seven years’ directly related experience in the design, writing, and testing of secure computer or cybersecurity programs or database development. Also requires comprehensive knowledge of the principles, practices, and procedures
used in all phases of full life cycle applications and systems development, engineering, programming, and analysis.

Functional Responsibility: Participates in all phases of software operating systems and software application programs engineering, including design, analysis, and modeling at a highly technical level within a cybersecurity environment; Performs software operating systems and application engineering, including full life cycle application systems design and development; assesses system architecture and hardware limitations; defines and selects new concepts and approaches for the design, development, and implementation of software engineering applications; defines complex design specifications and parameters; resolves complex hardware/software compatibility and interface design considerations; performs requirements acquisition and definition and data analysis; directs research on emerging technologies to determine impacts on application execution; performs systems modeling; may perform database analysis, design, implementation, and testing; writes, modifies, and maintains technical documentation and specifications such as user manuals, system documentation, and training materials; performs integration testing and support of various computer operating and/or network systems; troubleshoots and provides customer support for software operating systems and application issues; analyzes and documents client needs and requirements; serves as liaison with clients, participates in meetings to ensure client needs are met and may make client presentations; may serve as task or team lead, exercising leadership in either a technical role training other software engineers and implementing and enforcing established standards and technologies, or in a project coordination role leading tasks and assuming responsibility for the design, development, test and delivery of a software system or application.

Education: Bachelor’s Degree

Cyber Security Assessment and Authorization (A&A) Analyst - Junior
Minimum Experience – two years

Functional Responsibilities: Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security. Performs all procedures necessary to ensure the safety of the organization's systems, information, and transactions across the Internet/intranet. Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats. Identifies and mitigates vulnerabilities using alternate or compensating controls if necessary. Applies Internet firewall technologies to maintain security.

Ensures that the user community understands and adheres to necessary procedures to maintain security. Updates and deletes users, monitors and performs follow-up on compliance violations, and develops security policies, practices, and guidelines. Supports Security Operations Center (SOC). Assists with the installation, daily operation, and maintenance of IA systems to include technical support, troubleshooting, and system testing.

Education: Associate’s Degree

Cyber Security Assessment and Authorization (A&A) Analyst - Intermediate
Minimum Experience – five years

Functional Responsibilities: Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security. Performs all procedures necessary to ensure the safety of the organization's systems, information, and transactions across the

FEDERAL SUPPLY SCHEDULE PRICE LIST
Wise Technical Innovations LLC
Contract Number: 47QTCA20D0072
Internet/intranet. Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats. Identifies and mitigates vulnerabilities using alternate or compensating controls if necessary. Applies Internet firewall technologies to maintain security.
Ensures that the user community understands and adheres to necessary procedures to maintain security. Updates and deletes users, monitors and performs follow-up on compliance violations, and develops security policies, practices, and guidelines. Supports Security Operations Center (SOC). Assists with the installation, daily operation, and maintenance of IA systems to include technical support, troubleshooting, and system testing.

Education: Bachelor’s Degree
**Cyber Security Assessment and Authorization (A&A) Analyst - Junior**
Minimum Experience – seven years

Functional Responsibilities: Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security. Performs all procedures necessary to ensure the safety of the organization's systems, information, and transactions across the Internet/intranet. Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats. Identifies and mitigates vulnerabilities using alternate or compensating controls if necessary. Applies Internet firewall technologies to maintain security.
Ensures that the user community understands and adheres to necessary procedures to maintain security. Updates and deletes users, monitors and performs follow-up on compliance violations, and develops security policies, practices, and guidelines. Supports Security Operations Center (SOC). Assists with the installation, daily operation, and maintenance of IA systems to include technical support, troubleshooting, and system testing.
Education: Bachelor’s Degree
**Computer Network Defense (CND) Analyst - Junior**
Minimum Experience – two years

Functional Responsibilities: Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats. Performs actions to protect, monitor, detect, analyze, and respond to unauthorized activity within assigned information systems and computer networks. Employs Cybersecurity capabilities and deliberate actions to respond to a CND alert or emerging situational awareness/threat. Serves as an expert on CND requirements and compliance to such requirements by using IA tools and techniques to perform compliance analysis and correlation, tracking and remediation coordination, and escalating CND non-compliance. Provides technical analysis and sustainment support for the enterprise for IA tools and applications, and assists with the application of Defense-In-Depth signatures and perimeter defense controls to diminish network threats.

Education: Associate’s Degree
**Computer Network Defense (CND) Analyst - Intermediate**
Minimum Experience – five years

---

FEDERAL SUPPLY SCHEDULE PRICE LIST
Wise Technical Innovations LLC
Contract Number: 47QTCA20D0072
Functional Responsibilities: Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats. Performs actions to protect, monitor, detect, analyze, and respond to unauthorized activity within assigned information systems and computer networks. Employs Cybersecurity capabilities and deliberate actions to respond to a CND alert or emerging situational awareness/threat. Serves as an expert on CND requirements and compliance to such requirements by using IA tools and techniques to perform compliance analysis and correlation, tracking and remediation coordination, and escalating CND non-compliance. Provides technical analysis and sustainment support for the enterprise for IA tools and applications, and assists with the application of Defense-In-Depth signatures and perimeter defense controls to diminish network threats.

Education: Bachelor’s Degree

**Computer Network Defense (CND) Analyst - Senior**
Minimum Experience – seven years

Functional Responsibilities: Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats. Performs actions to protect, monitor, detect, analyze, and respond to unauthorized activity within assigned information systems and computer networks. Employs Cybersecurity capabilities and deliberate actions to respond to a CND alert or emerging situational awareness/threat. Serves as an expert on CND requirements and compliance to such requirements by using IA tools and techniques to perform compliance analysis and correlation, tracking and remediation coordination, and escalating CND non-compliance. Provides technical analysis and sustainment support for the enterprise for IA tools and applications, and assists with the application of Defense-In-Depth signatures and perimeter defense controls to diminish network threats.

Education: Bachelor’s Degree

**Security Architect - Junior**
Minimum Experience: two years

Functional Responsibilities: Responsible for guiding the design and implementation of secure solutions and services across business and IT support areas. Driving the successful configuration and implementation of security solutions to reduce risk to an acceptable level. Ensures that the stakeholder security requirements necessary to protect the organization’s mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes. Serves as an IA Subject Matter Expert (SME) with regards to IA Architecture policies and procedures. Provides IA Management support to Program Management Offices (PMO) for emerging information systems through the acquisition lifecycle and where applicable into sustainment. Provides technical support and guidance to facilitate the identification and integration of IA controls at the onset of the acquisition lifecycle for emerging IT capabilities. Serves as a principal liaison for Enterprise-level boundary defense initiatives to

---

FEDERAL SUPPLY SCHEDULE PRICE LIST
Wise Technical Innovations LLC
Contract Number: 47QTCA20D0072
ensure consistent and sufficient identification and implementation of applicable IA controls in concert with the agency IA and IT architecture and National Institute of Standards and Technology (NIST) security guidelines. Provides oversight for the design and implementation of Enterprise-level IA solutions providing standards for access control capabilities across the Enterprise.

Education: Associate’s Degree

**Security Architect - Intermediate**
Minimum Experience: five years

Functional Responsibilities: Responsible for guiding the design and implementation of secure solutions and services across business and IT support areas. Driving the successful configuration and implementation of security solutions to reduce risk to an acceptable level. Ensures that the stakeholder security requirements necessary to protect the organization’s mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes. Serves as an IA Subject Matter Expert (SME) with regards to IA Architecture policies and procedures. Provides IA Management support to Program Management Offices (PMO) for emerging information systems through the acquisition lifecycle and where applicable into sustainment. Provides technical support and guidance to facilitate the identification and integration of IA controls at the onset of the acquisition lifecycle for emerging IT capabilities. Serves as a principal liaison for Enterprise-level boundary defense initiatives to ensure consistent and sufficient identification and implementation of applicable IA controls in concert with the agency IA and IT architecture and National Institute of Standards and Technology (NIST) security guidelines. Provides oversight for the design and implementation of Enterprise-level IA solutions providing standards for access control capabilities across the Enterprise.

Education: Bachelor’s Degree

**Security Architect - Senior**
Minimum Experience: seven years

Functional Responsibilities: Responsible for guiding the design and implementation of secure solutions and services across business and IT support areas. Driving the successful configuration and implementation of security solutions to reduce risk to an acceptable level. Ensures that the stakeholder security requirements necessary to protect the organization’s mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes. Serves as an IA Subject Matter Expert (SME) with regards to IA Architecture policies and procedures. Provides IA Management support to Program Management Offices (PMO) for emerging information systems through the acquisition lifecycle and where applicable into sustainment. Provides technical support and guidance to facilitate the identification and integration of IA controls at the onset of the acquisition lifecycle for emerging IT capabilities. Serves as a principal liaison for Enterprise-level boundary defense initiatives to
ensure consistent and sufficient identification and implementation of applicable IA controls in
concert with the agency IA and IT architecture and National Institute of Standards and
Technology (NIST) security guidelines. Provides oversight for the design and implementation of
Enterprise-level IA solutions providing standards for access control capabilities across the
Enterprise.

Education: Bachelor’s Degree

**Information Assurance Analyst - Junior**
Minimum Experience: two years

Functional Responsibilities: Conducts comprehensive assessments of the management,
operational, and technical security controls and control enhancements employed within or
inherited by an information technology (IT) system to determine the overall effectiveness of the
controls (as defined in NIST SP 800-53 and/or SP 800-37). Demonstrated ability to independently
perform complex security analysis of applications and systems for compliance with security
requirements. Performs cybersecurity vulnerability evaluations. Uses a variety of security
techniques, technologies, and tools to evaluate security posture in highly complex computer
systems and networks. Analyzes and
defines security requirements for systems, applications and infrastructure. Recommends
solutions to meet security requirements. Gathers and organizes technical information about an
organization’s mission goals and needs, and makes recommendations to improve existing
security posture. Demonstrated experience and ability to provide enterprise-wide technical
analysis and direction for problem definition, analysis and remediation for complex systems and
enclaves. Ability to provide workable recommendations and advice to client executive
management on system security posture and process improvements, optimization and
maintenance. Develops and maintains cybersecurity plans, strategy, and policy to support and
align with organizational cybersecurity initiatives and regulatory compliance. Reviews,
consolidates, develops and/or implements cybersecurity policy in accordance with agency/client
and NIST security requirements and assess IT policies, standards, guidelines or procedures to
ensure a balance of security and operational requirements.

Education: Associate’s Degree

**Information Assurance Analyst - Intermediate**
Minimum Experience: five years

Functional Responsibilities: Conducts comprehensive assessments of the management,
operational, and technical security controls and control enhancements employed within or
inherited by an information technology (IT) system to determine the overall effectiveness of the
controls (as defined in NIST SP 800-53 and/or SP 800-37). Demonstrated ability to independently
perform complex security analysis of applications and systems for compliance with security
requirements. Performs cybersecurity vulnerability evaluations. Uses a variety of security
techniques, technologies, and tools to evaluate security posture in highly complex computer
systems and networks. Analyzes and
defines security requirements for systems, applications and infrastructure. Recommends
solutions to meet security requirements. Gathers and organizes technical information about an
organization’s mission goals and needs, and makes recommendations to improve existing

---

**FEDERAL SUPPLY SCHEDULE PRICE LIST**
Wise Technical Innovations LLC
Contract Number: 47QTC20D0072
security posture. Demonstrated experience and ability to provide enterprise-wide technical analysis and direction for problem definition, analysis and remediation for complex systems and enclaves. Ability to provide workable recommendations and advice to client executive management on system security posture and process improvements, optimization and maintenance. Develops and maintains cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance. Reviews, consolidates, develops and/or implements cybersecurity policy in accordance with agency/client and NIST security requirements and assess IT policies, standards, guidelines or procedures to ensure a balance of security and operational requirements.

Education: Bachelor’s Degree

Information Assurance Analyst - Senior
Minimum Experience: seven years

Functional Responsibilities: Conducts comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-53 and/or SP 800-37). Demonstrated ability to independently perform complex security analysis of applications and systems for compliance with security requirements. Performs cybersecurity vulnerability evaluations. Uses a variety of security techniques, technologies, and tools to evaluate security posture in highly complex computer systems and networks. Analyzes and defines security requirements for systems, applications and infrastructure. Recommends solutions to meet security requirements. Gathers and organizes technical information about an organization's mission goals and needs, and makes recommendations to improve existing security posture. Demonstrated experience and ability to provide enterprise-wide technical analysis and direction for problem definition, analysis and remediation for complex systems and enclaves. Ability to provide workable recommendations and advice to client executive management on system security posture and process improvements, optimization and maintenance. Develops and maintains cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance. Reviews, consolidates, develops and/or implements cybersecurity policy in accordance with agency/client and NIST security requirements and assess IT policies, standards, guidelines or procedures to ensure a balance of security and operational requirements.

Education: Bachelor’s Degree

Penetration Tester - Intermediate
Minimum Experience: three years

Functional Responsibilities: Demonstrated ability to independently perform penetration testing of applications, systems and enclaves belonging to or managed by clients. Identifies security flaws in computing platforms and applications and devise strategies and techniques to mitigate identified cybersecurity risks. Perform application and network penetration testing and wireless security assessments. Apply offensive cybersecurity testing techniques, coordinate testing projects with internal and external
system owners. Reports the nature of identified cyber security risks and recommends risk mitigation measures to improve the cyber security posture of the enterprise.
• Proven proficiency in performing extensive vulnerability assessment and penetration testing.
• Experience with testing tools, including NESSUS, METASPLOIT, CANVAS, NMAP, Burp Suite, and Kismet
• Experience with network vulnerability assessments and penetration testing methods
• Experience with writing testing assessment reports
• Knowledge of open security testing standards and projects, including OWASP

Education: Bachelor’s Degree

Penetration Tester - Senior
Minimum Experience: six years

Functional Responsibilities: Demonstrated ability to independently perform penetration testing of applications, systems and enclaves belonging to or managed by clients. Identifies security flaws in computing platforms and applications and devise strategies and techniques to mitigate identified cybersecurity risks.
Performs application and network penetration testing and wireless security assessments. Apply offensive cybersecurity testing techniques, coordinate testing projects with internal and external system owners. Reports the nature of identified cyber security risks and recommends risk mitigation measures to improve the cyber security posture of the enterprise.
• Proven proficiency in performing extensive vulnerability assessment and penetration testing.
• Experience with testing tools, including NESSUS, METASPLOIT, CANVAS, NMAP, Burp Suite, and Kismet
• Experience with network vulnerability assessments and penetration testing methods
• Experience with writing testing assessment reports
• Knowledge of open security testing standards and projects, including OWASP

Education: Bachelor’s Degree

Cybersecurity Engineer - Senior
Minimum Experience: seven years

Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats. Identifies and mitigates vulnerabilities using alternate or compensating controls if necessary. Supports, monitors, tests, and troubleshoots IA software issues in conjunction with other IA staff to ensure timely response actions to security incidents. Recognizes potential security violations, takes appropriate action to report the incident as required by regulation and mitigates any adverse impact. Implements applicable patches including vulnerabilities from the National Vulnerability Database, US CERT alerts, IA vulnerability alerts (IAVA), IA vulnerability bulletins (IAVB), and technical advisories (TA) for assigned operating system(s). Under technical supervision, performs information assurance...
activities in data center environments. Supports Security Operations Center (SOC). Assists with
the installation, daily operation, and maintenance of IA systems to include technical support,
troubleshooting, and system testing. Conducts and/or supports authorized penetration testing on
enterprise network assets. Performs a variety of routine project tasks applied to specialized
Cybersecurity problems. Tasks
involve integration of tools and processes or methodologies to resolve total system problems, or
technology problems as they relate to cybersecurity requirements. Analyzes information security
requirements. Applies analytical and systematic approaches in the resolution of problems of
work flow, organization, and planning. Provides security engineering support for planning,
design, development, testing, demonstration, integration of information systems. Experienced
with security tools such as SIEM tools, vulnerability scanners, monitoring tools and incident
response processes and tools

Education: Bachelor's Degree

Cybersecurity Assessment and Authorization (A&A) Analyst - Junior
Minimum Experience: two years

Functional Responsibilities:
Serves as a cybersecurity Subject Matter Expert (SME) with regards to Authorization of
information systems and all associated cybersecurity policies and procedures. Fully versed in the
general tenets supporting the overall organization implementation of its authorization process, to
include supporting cybersecurity policy, procedures and processes. Performs a cybersecurity
process while either authorizing an information system or serving as a SME for an information
system undergoing authorization. Possess an understanding of how the security controls
identified in the NIST 800-53 apply to the process of assessing and authorizing a large
organization’s IT infrastructure, in which there is a compilation of large and small enclaves,
applications and IT processes. Determines the applicable severity value for an identified
vulnerability (e.g., non-compliant security control), and determines the possible ramifications on
the system’s current or future authorization. Required to brief senior management on the
progress or results of an information system undergoing the authorization process. Prepares,
reviews, and evaluates documentation of compliance. Verifies that application
software/network/system security postures are implemented as stated, document deviations, and
recommend required actions to correct those deviations. Reviews IA and IA enabled software,
hardware, and firmware for compliance with appropriate security configuration guidelines,
policies, and procedures. Developed, reviews or updates IA security plans and A&A
documentation. Identifies alternative functional IA security strategies to address organizational
security concerns. Perform security reviews and identify security gaps in security architecture
resulting in recommendations for inclusion in the risk mitigation strategy. Prepares,
recommendations for the Designated Approving Authority (DAA) or Authorizing Official (AO).
• Relevant A&A (formerly known as C&A) experience
• Risk Management Framework (RMF) and NIST A&A experience
• Experience in assessing security controls and conducting authorization
reviews for large, complex organizations.

Education: Associate's Degree

Cybersecurity Assessment and Authorization (A&A) Analyst - Intermediate
Minimum Experience: five years

Functional Responsibilities:
Serves as a cybersecurity Subject Matter Expert (SME) with regards to Authorization of information systems and all associated cybersecurity policies and procedures. Fully versed in the general tenets supporting the overall organization implementation of its authorization process, to include supporting cybersecurity policy, procedures and processes. Performs a cybersecurity process while either authorizing an information system or serving as a SME for an information system undergoing authorization. Possess an understanding of how the security controls identified in the NIST 800-53 apply to the process of assessing and authorizing a large organization’s IT infrastructure, in which there is a compilation of large and small enclaves, applications and IT processes. Determines the applicable severity value for an identified vulnerability (e.g., non-compliant security control), and determines the possible ramifications on the system’s current or future authorization. Required to brief senior management on the progress or results of an information system undergoing the authorization process. Prepares, reviews, and evaluates documentation of compliance. Verifies that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations. Reviews IA and IA enabled software, hardware, and firmware for compliance with appropriate security configuration guidelines, policies, and procedures. Developed, reviews or updates IA security plans and A&A documentation. Identifies alternative functional IA security strategies to address organizational security concerns. Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy. Prepares, recommendations for the Designated Approving Authority (DAA) or Authorizing Official (AO).
  - Relevant A&A (formerly known as C&A) experience
  - Risk Management Framework (RMF) and NIST A&A experience
  - Experience in assessing security controls and conducting authorization reviews for large, complex organizations.

Education: Bachelor’s Degree

Cybersecurity Assessment and Authorization (A&A) Analyst - Senior
Minimum Experience: seven years

Functional Responsibilities:
Serves as a cybersecurity Subject Matter Expert (SME) with regards to Authorization of information systems and all associated cybersecurity policies and procedures. Fully versed in the general tenets supporting the overall organization implementation of its authorization process, to include supporting cybersecurity policy, procedures and processes. Performs a cybersecurity process while either authorizing an information system or serving as a SME for an information system undergoing authorization. Possess an understanding of how the security controls identified in the NIST 800-53 apply to the process of assessing and authorizing a large organization’s IT infrastructure, in which there is a compilation of large and small enclaves, applications and IT processes. Determines the applicable severity value for an identified vulnerability (e.g., non-compliant security control), and determines the possible ramifications on the system’s current or future authorization. Required to brief senior management on the progress or results of an information system undergoing the authorization process. Prepares, reviews, and evaluates documentation of compliance. Verifies that application
software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations. Reviews IA and IA enabled software, hardware, and firmware for compliance with appropriate security configuration guidelines, policies, and procedures. Developed, reviews or updates IA security plans and A&A documentation. Identifies alternative functional IA security strategies to address organizational security concerns. Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy. Prepares, recommendations for the Designated Approving Authority (DAA) or Authorizing Official (AO).

- Relevant A&A (formerly known as C&A) experience
- Risk Management Framework (RMF) and NIST A&A experience
- Experience in assessing security controls and conducting authorization reviews for large, complex organizations.

Education: Bachelor’s Degree

Cybersecurity Technical Writer - Junior

Minimum Experience: two years

Functional Responsibilities:
Under general supervision, edits and rewrites documents for grammatical, syntactical, and usage errors, spelling, punctuation, and adherence to standards. Proofreads documentation and graphics for accuracy and adherence to original content provides quality control checking for documents received from photocopying and word processing; assembles Master copies, including graphics, appendices, table of contents, and title pages; assists in scheduling printing, and copying. Assists in document tracking and logging, and consults with technical staff to determine format, contents, and the organization of technical reports and proposals. Assists in collecting and organizing information required for preparation of user’s manuals, training materials, installation guides, proposals, and reports. Edits functional descriptions, system specifications, user’s manuals, special reports, or any other customer deliverables and documents.

- Relevant Technical Writing experience

Education: Associate’s Degree

Cybersecurity Technical Writer - Intermediate

Minimum Experience: five years

Functional Responsibilities:
Under general supervision, edits and rewrites documents for grammatical, syntactical, and usage errors, spelling, punctuation, and adherence to standards. Proofreads documentation and graphics for accuracy and adherence to original content provides quality control checking for documents received from photocopying and word processing; assembles Master copies, including graphics, appendices, table of contents, and title pages; assists in scheduling printing, and copying. Assists in document tracking and logging, and consults with technical staff to determine format, contents, and the organization of technical reports and proposals. Assists in collecting and organizing information required for preparation of user’s manuals, training
Cloud Computing Security Specialist (CCSS) – Staff
Minimum Experience: three years
Functional Responsibilities:
Serves as an Information Assurance and Cloud computing SME with regards to Assessment and Authorization (A&A) (formerly known as C&A) and a broad coverage of the application of the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) standards and guidance as outlined in the NIST Special Publication(s) (SP) 800-53 and 800-37 (Current versions). Possesses the ability to work independently with substantial cloud computing security knowledge. The assessor must have the essential skill sets to identify, manage and resolve cloud computing security risk and implement “best practices” as applied within a cloud environment (across all the different deployment and service models, and derivatives). The CCSS must be well versed in FedRAMP assessment methodology of security and privacy controls deployed in cloud information systems to include six (6) domain areas. The six domains include:

- Architectural Concepts & Design Requirements
- Cloud Data Security
- Cloud Platform & Infrastructure Security
- Cloud Application Security
- Operations
- Legal & Compliance
- Relevant A&A experience; Risk Management Framework (RMF) and NIST A&A experience
- Experience in assessing IA Controls and conducting A&A reviews for large, complex Information systems

Education: Bachelor’s Degree

Cloud Computing Security Specialist (CCSS) – Intermediate
Minimum Experience: five years
Functional Responsibilities:
Serves as an Information Assurance and Cloud computing SME with regards to Assessment and Authorization (A&A) (formerly known as C&A) and a broad coverage of the application of the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) standards and guidance as outlined in the NIST Special Publication(s) (SP) 800-53 and 800-37 (Current versions). Possesses the ability to work independently with substantial cloud computing security knowledge. The assessor must have the essential skill sets to identify, manage and resolve cloud computing security risk and implement “best practices” as applied within a cloud environment (across all the different deployment and service models, and derivatives). The CCSS must be well versed in FedRAMP assessment methodology of security and privacy controls deployed in cloud information systems to include six (6) domain areas. The six domains include:
• Architectural Concepts & Design Requirements
• Cloud Data Security
• Cloud Platform & Infrastructure Security
• Cloud Application Security
• Operations
• Legal & Compliance
• Relevant A&A experience; Risk Management Framework (RMF) and NIST A&A experience
• Experience in assessing IA Controls and conducting A&A reviews for large, complex Information systems

Education: Bachelor’s Degree

Cloud Computing Security Specialist (CCSS) – Senior
Minimum Experience: seven years
Functional Responsibilities:
Serves as an Information Assurance and Cloud computing SME with regards to Assessment and Authorization (A&A) (formerly known as C&A) and a broad coverage of the application of the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) standards and guidance as outlined in the NIST Special Publication(s) (SP) 800-53 and 800-37 (Current versions). Possesses the ability to work independently with substantial cloud computing security knowledge. The assessor must have the essential skill sets to identify, manage and resolve cloud computing security risk and implement “best practices” as applied within a cloud environment (across all the different deployment and service models, and derivatives). The CCSS must be well versed in FedRAMP assessment methodology of security and privacy controls deployed in cloud information systems to include six (6) domain areas. The six domains include:
• Architectural Concepts & Design Requirements
• Cloud Data Security
• Cloud Platform & Infrastructure Security
• Cloud Application Security
• Operations
• Legal & Compliance
• Relevant A&A experience; Risk Management Framework (RMF) and NIST A&A experience
• Experience in assessing IA Controls and conducting A&A reviews for large, complex Information systems

Education: Bachelor’s Degree

Information Security Analyst (Data Protection) - Junior
Minimum Experience: two years

Functional Responsibilities:
Serves as information security analyst performing incident response (identification, containment, eradication, recovery) for Personally Identifiable Information (PII) incidents and PII-related data breaches. Investigates, analyzes, and responds to cyber incidents within the network environment

FEDERAL SUPPLY SCHEDULE PRICE LIST
Wise Technical Innovations LLC
Contract Number: 47QTCA20D0072
or enclave. Utilizes data loss prevention (DLP) tools to identify improperly stored PII data at rest and improperly transmitted PII data. Performs the quarantining of improperly stored PII data. Recommends appropriate actions to mitigate the risk of unauthorized access to PII data and ensures the implementation of appropriate security controls to safeguard PII data. Engages with stakeholders and mission partners to facilitate containment, eradication, and recovery for PII incidents. Validates remedial actions and ensures compliance with NIST and agency specific information security and privacy policy.

• Hands-on experience performing computer security incident handling
• Hands-on experience with data loss prevention software/tools

Education: Associate’s Degree

Information Security Analyst (Data Protection) - Intermediate
Minimum Experience: five years

Functional Responsibilities:
Serves as information security analyst performing incident response (identification, containment, eradication, recovery) for Personally Identifiable Information (PII) incidents and PII-related data breaches. Investigates, analyzes, and responds to cyber incidents within the network environment or enclave. Utilizes data loss prevention (DLP) tools to identify improperly stored PII data at rest and improperly transmitted PII data. Performs the quarantining of improperly stored PII data. Recommends appropriate actions to mitigate the risk of unauthorized access to PII data and ensures the implementation of appropriate security controls to safeguard PII data. Engages with stakeholders and mission partners to facilitate containment, eradication, and recovery for PII incidents. Validates remedial actions and ensures compliance with NIST and agency specific information security and privacy policy.

• Hands-on experience performing computer security incident handling
• Hands-on experience with data loss prevention software/tools

Education: Bachelor’s Degree

Information Security Analyst (Data Protection) - Senior
Minimum Experience: seven years

Functional Responsibilities:
Serves as information security analyst performing incident response (identification, containment, eradication, recovery) for Personally Identifiable Information (PII) incidents and PII-related data breaches. Investigates, analyzes, and responds to cyber incidents within the network environment or enclave. Utilizes data loss prevention (DLP) tools to identify improperly stored PII data at rest and improperly transmitted PII data. Performs the quarantining of improperly stored PII data. Recommends appropriate actions to mitigate the risk of unauthorized access to PII data and ensures the implementation of appropriate security controls to safeguard PII data. Engages with stakeholders and mission partners to facilitate containment, eradication, and recovery for PII incidents. Validates remedial actions and ensures compliance with NIST and agency specific information security and privacy policy.

• Hands-on experience performing computer security incident handling
• Hands-on experience with data loss prevention software/tools

Education: Bachelor’s Degree

Operational Technology Security Engineer – Junior
Minimum Experience: two years
Functional Responsibilities:
Performs a variety of routine project tasks applied to specialized information assurance problems with IT systems. Tasks involve integration of processes or methodologies with information systems to resolve total system problems, or technology problems as they relate to IA requirements. Analyzes information security requirements. Applies analytical and systematic approaches in the resolution of problems of work flow, organization, and planning. Provides security engineering support for planning, design, development, testing, demonstration, integration of IT systems.
Provides expert support, analysis and research into exceptionally complex cyber security problems, and processes relating to the subject matter. Serves as technical expert on project teams providing technical direction, interpretation and alternatives.
Applies extensive technical expertise in the field of cybersecurity, and has full knowledge of other related disciplines. Guides the successful completion of major programs and may function in a project leadership role. Develops technical solutions to complex problems that require the regular use of ingenuity and creativity. Expertise is in an area of Information Technology (e.g., Product SME, Information Systems Architecture, Telecommunications Systems Design, Architecture, Implementation, Information Systems Integration, Software Development Methodologies, Security Engineering, Security Compliance, Cognitive Security, Analytics, Privacy, Communications and Network Systems Management), or a specific functional area (e.g., finance, logistics, and operations research).
Education: Associate’s Degree

Operational Technology Security Engineer – Intermediate
Minimum Experience: five years
Functional Responsibilities:
Performs a variety of routine project tasks applied to specialized information assurance problems with IT systems. Tasks involve integration of processes or methodologies with information systems to resolve total system problems, or technology problems as they relate to IA requirements. Analyzes information security requirements. Applies analytical and systematic approaches in the resolution of problems of work flow, organization, and planning. Provides security engineering support for planning, design, development, testing, demonstration, integration of IT systems.
Provides expert support, analysis and research into exceptionally complex cyber security problems, and processes relating to the subject matter. Serves as technical expert on project teams providing technical direction, interpretation and alternatives.
Applies extensive technical expertise in the field of cybersecurity, and has full knowledge of other related disciplines. Guides the successful completion of major programs and may function in a project leadership role. Develops technical solutions to complex problems that require the regular use of ingenuity and creativity. Expertise is in an area of Information Technology (e.g., Product SME, Information Systems Architecture, Telecommunications Systems Design, Architecture, Implementation, Information Systems Integration, Software Development Methodologies, Security Engineering, Security Compliance,
Cognitive Security, Analytics, Privacy, Communications and Network Systems Management), or a specific functional area (e.g., finance, logistics, and operations research).

Education: Bachelor’s Degree

**Operational Technology Security Engineer – Senior**

Minimum Experience: seven years

Functional Responsibilities:

Performs a variety of routine project tasks applied to specialized information assurance problems with IT systems. Tasks involve integration of processes or methodologies with information systems to resolve total system problems, or technology problems as they relate to IA requirements. Analyzes information security requirements. Applies analytical and systematic approaches in the resolution of problems of work flow, organization, and planning. Provides security engineering support for planning, design, development, testing, demonstration, integration of IT systems. Provides expert support, analysis and research into exceptionally complex cyber security problems, and processes relating to the subject matter. Serves as technical expert on project teams providing technical direction, interpretation and alternatives. Applies extensive technical expertise in the field of cybersecurity, and has full knowledge of other related disciplines. Guides the successful completion of major programs and may function in a project leadership role. Develops technical solutions to complex problems that require the regular use of ingenuity and creativity. Expertise is in an area of Information Technology (e.g., Product SME, Information Systems Architecture, Telecommunications Systems Design, Architecture, Implementation, Information Systems Integration, Software Development Methodologies, Security Engineering, Security Compliance, Cognitive Security, Analytics, Privacy, Communications and Network Systems Management), or a specific functional area (e.g., finance, logistics, and operations research).

Education: Bachelor’s Degree

**Vulnerability Management Analyst – Junior**

Minimum Experience: two years

Functional Responsibilities:

Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities. Serves as vulnerability management analyst for assigned applications. Analyzes vulnerabilities and characterizes risk. Engages with stakeholders and mission partners to facilitate application, infrastructure and/or web vulnerability assessments. Performs code review, software assurance testing, and application vulnerability scanning. Facilitates the coordination of remediation efforts, prioritizing remediation efforts based on risk. Recommends appropriate actions to remediate vulnerabilities and mitigate risks and ensures the implementation of appropriate security settings to include those required by NIST and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG). Tracks and reports security and compliance issues. Validates remedial actions and ensures compliance with NIST and agency specific information security policy.

Qualifications:
- Hands-on experience working with application vulnerability scanners
- Understanding of application vulnerabilities and remediation techniques

Education: Associate’s Degree

FEDERAL SUPPLY SCHEDULE PRICE LIST
Wise Technical Innovations LLC
Contract Number: 47QTCA20D0072
Vulnerability Management Analyst – Intermediate
Minimum Experience: five years
Functional Responsibilities:
Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities. Serves as vulnerability management analyst for assigned applications. Analyzes vulnerabilities and characterizes risk. Engages with stakeholders and mission partners to facilitate application, infrastructure and/or web vulnerability assessments. Performs code review, software assurance testing, and application vulnerability scanning. Facilitates the coordination of remediation efforts, prioritizing remediation efforts based on risk. Recommends appropriate actions to remediate vulnerabilities and mitigate risks and ensures the implementation of appropriate security settings to include those required by NIST and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG). Tracks and reports security and compliance issues. Validates remedial actions and ensures compliance with NIST and agency specific information security policy.
Qualifications:
• Hands-on experience working with application vulnerability scanners
• Understanding of application vulnerabilities and remediation techniques
Education: Bachelor’s Degree

Vulnerability Management Analyst – Senior
Minimum Experience: seven years
Functional Responsibilities:
Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities. Serves as vulnerability management analyst for assigned applications. Analyzes vulnerabilities and characterizes risk. Engages with stakeholders and mission partners to facilitate application, infrastructure and/or web vulnerability assessments. Performs code review, software assurance testing, and application vulnerability scanning. Facilitates the coordination of remediation efforts, prioritizing remediation efforts based on risk. Recommends appropriate actions to remediate vulnerabilities and mitigate risks and ensures the implementation of appropriate security settings to include those required by NIST and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG). Tracks and reports security and compliance issues. Validates remedial actions and ensures compliance with NIST and agency specific information security policy.
Qualifications:
• Hands-on experience working with application vulnerability scanners
• Understanding of application vulnerabilities and remediation techniques
Education: Bachelor’s Degree