GENERAL SERVICES ADMINISTRATION
FEDERAL SUPPLY SERVICE MULTIPLE AWARD SCHEDULE (MAS)
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 is available through GSA Advantage!, a menu-driven database system. The INTERNET address for GSA Advantage! is http://www.gsaadvantage.gov. Prices Shown Herein are Net (discount deducted).

CONTRACT No. 47QTCA18D00AG

For more information on ordering from Federal Supply Schedules click on the FSS Schedules button at fss.gsa.gov

Contractor          GCyber, LLC
                    241 18th ST S STE 504
                    Arlington, VA 22202
                    571-279-8270
                    www.gcycler.com

Contractor Point of Contact    Jeff Adams
                                Vice President
                                241 18th ST S STE 504
                                Arlington, VA 22202
                                571-279-8270
                                jeff@gcyber.com

Period of Performance 4/16/2018 – 4/15/2023
5 year option period 1 of 5

Business Size Small Business
CONTRACTOR INFORMATION

1. Schedule Information

1a. Table of Awarded Special Item Numbers
   - 54151S: Information Technology Professional Services
   - 54151HAC: Highly Adaptive Cybersecurity Services (HACS)
   - Ancillary: Ancillary Supplies and/or Services
   - OLM: Order Level Materials (OLM)

1b. Lowest Priced Model Number and Price for Each Awarded SIN
   See Appendix A

1c. Hourly Rates (Services Only)
   See Appendix A

1d. Labor Category Descriptions (Services Only)
   See Appendix C

2. Maximum Order Threshold
   - 54151S: $500,000
   - 54151S (ANCILLARY): $250,000
   - 54151HAC: $500,000

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

3. Minimum Order Threshold
   $100.00 (all SINs)

4. Geographic Coverage
   Continental US, Hawaii, Puerto Rico

5. Point(s) of Production
   Arlington, VA

6. Discount from Best Market Rate
   GSA Net Prices can be found in Pricing Matrixes (below). Negotiated discounts have been applied and the Industrial Funding Fee has been added.

7. Quantity Discounts
   None

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

9. Government Purchase Cards
   9a will be accepted at or below the micro-purchase threshold
   9b will not be accepted above the micro-purchase threshold.

10. Foreign Items
    None

11. Delivery
   11a. Time of Delivery
        Determined at Task Level
   11b. Expedited Delivery
        Determined at Task Level. Items available for expedited delivery are noted in this price list.
   11c. Overnight and 2-Day Delivery
        Determined at Task Level. Schedule Customers can contact the Contractor for rates for overnight and 2-day delivery.
   11d. Urgent Requirements
        Agencies can contact the Contractor’s representative to affect a faster delivery. Customers are encouraged to contact the Contractor for the purpose of requesting accelerated delivery.

12. FOB Point
    Destination

13. Ordering
   13a. Ordering Address
        GCyber, LLC
        241 18th ST S STE 504
        Arlington, VA 22202
   13b. Ordering Procedures
        Ordering activities shall use the ordering procedures described in Federal Acquisition Regulation 8.405-3 when placing an order or establishing a BPA for supplies or services. The ordering procedures, information on Blanket Purchase Agreements, and a sample BPA can be found at the GSA/FSS Schedule Homepage www.fss.gsa.gov/schedules.

14. Payment Address
    GCyber, LLC
    241 18th ST S STE 504
    Arlington, VA 22202

www.gcyber.com 3 sales@gcyber.com
15. Warranty Provision
   Standard Commercial

16. Export Packing Charges
   None

17. Terms and Conditions of Government Purchase Card Acceptance
   None

18. Terms and Conditions of Rental, Maintenance, and Repaid (if applicable)
   Not Applicable

19. Terms and Conditions of Installation (if applicable)
   Not Applicable

20. Terms and Conditions of Repaid Parts Indicating Date of Parts Price Lists and Any Discounts from List Prices (if available)
   Not Applicable

21a. Terms and Conditions for Any Other Services (if applicable)
   See Appendix B

21. List of Services and Distribution Points (if applicable)
   Not Applicable

22. List of Participating Dealers (if applicable)
   Not Applicable

23. Preventive Maintenance (if applicable)
   Not Applicable

24. Special Attributes
   24a. Environment Attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants)
        Not Applicable
   24b. Section 508 Compliance for Electronic and Information Technology (EIT)
        Compliant. EIT standards can be found at www.Section508.gov.

25. DUNS Number
    079386382

26. Notification Regarding Registration in System for Award Management (SAM) Database
    The Contractor has an active registration in the System for Award Management (SAM) database.
## APPENDIX A – Government Site Rates

<table>
<thead>
<tr>
<th>LCat #</th>
<th>Labor Category</th>
<th>2020 Rate</th>
<th>2021 Rate</th>
<th>2022 Rate</th>
<th>2023 Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001S</td>
<td>Applications Systems Analyst II</td>
<td>$57.37</td>
<td>$58.71</td>
<td>$60.08</td>
<td>$61.47</td>
</tr>
<tr>
<td>0002S</td>
<td>Applications Systems Analyst III</td>
<td>$71.68</td>
<td>$73.34</td>
<td>$75.05</td>
<td>$76.80</td>
</tr>
<tr>
<td>0003S</td>
<td>Business Process Consultant</td>
<td>$78.58</td>
<td>$80.42</td>
<td>$82.29</td>
<td>$84.20</td>
</tr>
<tr>
<td>0004S</td>
<td>Business Process Solutions Architect</td>
<td>$214.82</td>
<td>$219.83</td>
<td>$224.95</td>
<td>$230.19</td>
</tr>
<tr>
<td>0005S</td>
<td>Configuration Analyst II</td>
<td>$83.41</td>
<td>$85.35</td>
<td>$87.34</td>
<td>$89.37</td>
</tr>
<tr>
<td>0006S</td>
<td>Configuration Analyst III</td>
<td>$99.20</td>
<td>$101.52</td>
<td>$103.88</td>
<td>$106.30</td>
</tr>
<tr>
<td>0007S</td>
<td>Consultant</td>
<td>$150.78</td>
<td>$154.29</td>
<td>$157.88</td>
<td>$161.56</td>
</tr>
<tr>
<td>0008S</td>
<td>Data Security Analyst II</td>
<td>$75.61</td>
<td>$77.37</td>
<td>$79.18</td>
<td>$81.02</td>
</tr>
<tr>
<td>0009S</td>
<td>Data Security Analyst III</td>
<td>$92.53</td>
<td>$94.68</td>
<td>$96.89</td>
<td>$99.15</td>
</tr>
<tr>
<td>0010S</td>
<td>Data Security Analyst IV</td>
<td>$118.32</td>
<td>$121.07</td>
<td>$123.90</td>
<td>$126.78</td>
</tr>
<tr>
<td>0011S</td>
<td>Disaster Recovery Analyst</td>
<td>$72.02</td>
<td>$73.70</td>
<td>$75.42</td>
<td>$77.18</td>
</tr>
<tr>
<td>0012S</td>
<td>Enterprise Infrastructure Architect IV</td>
<td>$118.18</td>
<td>$120.93</td>
<td>$123.76</td>
<td>$126.64</td>
</tr>
<tr>
<td>0013S</td>
<td>Enterprise Solutions Engineer</td>
<td>$214.82</td>
<td>$219.83</td>
<td>$224.95</td>
<td>$230.19</td>
</tr>
<tr>
<td>0014S</td>
<td>Information Security Analyst II</td>
<td>$75.40</td>
<td>$77.16</td>
<td>$78.96</td>
<td>$80.79</td>
</tr>
<tr>
<td>0015S</td>
<td>Information Security Analyst III</td>
<td>$91.49</td>
<td>$93.62</td>
<td>$95.81</td>
<td>$98.04</td>
</tr>
<tr>
<td>0016S</td>
<td>Information Security Analyst IV</td>
<td>$101.42</td>
<td>$103.79</td>
<td>$106.21</td>
<td>$108.68</td>
</tr>
<tr>
<td>0017S</td>
<td>Information Security Analyst V</td>
<td>$120.97</td>
<td>$123.79</td>
<td>$126.68</td>
<td>$129.63</td>
</tr>
<tr>
<td>0018S</td>
<td>IT Project Manager III</td>
<td>$102.10</td>
<td>$104.48</td>
<td>$106.91</td>
<td>$109.41</td>
</tr>
<tr>
<td>0019S</td>
<td>IT Project Manager IV</td>
<td>$116.58</td>
<td>$119.30</td>
<td>$122.08</td>
<td>$124.93</td>
</tr>
<tr>
<td>0020S</td>
<td>Network Administrator I</td>
<td>$54.73</td>
<td>$56.01</td>
<td>$57.31</td>
<td>$58.65</td>
</tr>
<tr>
<td>0021S</td>
<td>Network Administrator III</td>
<td>$79.29</td>
<td>$81.14</td>
<td>$83.03</td>
<td>$84.96</td>
</tr>
<tr>
<td>0022S</td>
<td>Network Administrator IV</td>
<td>$98.66</td>
<td>$100.95</td>
<td>$103.31</td>
<td>$105.71</td>
</tr>
<tr>
<td>0023S</td>
<td>Program Manager III</td>
<td>$152.31</td>
<td>$155.86</td>
<td>$159.49</td>
<td>$163.21</td>
</tr>
<tr>
<td>0024S</td>
<td>Software Engineer V</td>
<td>$130.91</td>
<td>$133.97</td>
<td>$137.09</td>
<td>$140.28</td>
</tr>
<tr>
<td>0025S</td>
<td>Subject Matter Expert I</td>
<td>$83.80</td>
<td>$85.75</td>
<td>$87.75</td>
<td>$89.79</td>
</tr>
<tr>
<td>0026S</td>
<td>Subject Matter Expert III</td>
<td>$124.79</td>
<td>$127.70</td>
<td>$130.68</td>
<td>$133.73</td>
</tr>
<tr>
<td>0027S</td>
<td>Subject Matter Expert IV</td>
<td>$154.20</td>
<td>$157.79</td>
<td>$161.47</td>
<td>$165.23</td>
</tr>
<tr>
<td>0028S</td>
<td>Systems Administrator II</td>
<td>$63.68</td>
<td>$65.17</td>
<td>$66.68</td>
<td>$68.24</td>
</tr>
<tr>
<td>0029S</td>
<td>Systems Engineer II</td>
<td>$75.58</td>
<td>$77.34</td>
<td>$79.15</td>
<td>$80.99</td>
</tr>
<tr>
<td>0030S</td>
<td>Systems Engineer III</td>
<td>$108.18</td>
<td>$110.71</td>
<td>$113.29</td>
<td>$115.93</td>
</tr>
<tr>
<td>0031S</td>
<td>Systems Engineer IV</td>
<td>$118.53</td>
<td>$121.29</td>
<td>$124.12</td>
<td>$127.01</td>
</tr>
</tbody>
</table>

### Ancillary Supplies and/or Services (54151S) – Government Site Rates*

<table>
<thead>
<tr>
<th>LCat #</th>
<th>Labor Category</th>
<th>2020 Rate</th>
<th>2021 Rate</th>
<th>2022 Rate</th>
<th>2023 Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001A</td>
<td>Help Desk Support Assistant**</td>
<td>$39.61</td>
<td>$40.53</td>
<td>$41.47</td>
<td>$42.44</td>
</tr>
<tr>
<td>0002A</td>
<td>Help Desk Support**</td>
<td>$47.17</td>
<td>$48.27</td>
<td>$49.40</td>
<td>$50.55</td>
</tr>
</tbody>
</table>
### 54151HACS Highly Adaptive Cybersecurity Services (HACS) – Government Site Rates*

<table>
<thead>
<tr>
<th>LCat #</th>
<th>Labor Category</th>
<th>2020 Rate</th>
<th>2021 Rate</th>
<th>2022 Rate</th>
<th>2023 Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001H</td>
<td>Cybersecurity Applications Analyst II</td>
<td>$57.37</td>
<td>$58.71</td>
<td>$60.08</td>
<td>$61.47</td>
</tr>
<tr>
<td>0002H</td>
<td>Cybersecurity Applications Analyst III</td>
<td>$71.68</td>
<td>$73.34</td>
<td>$75.05</td>
<td>$76.80</td>
</tr>
<tr>
<td>0003H</td>
<td>Cybersecurity Process Consultant</td>
<td>$78.58</td>
<td>$80.42</td>
<td>$82.29</td>
<td>$84.20</td>
</tr>
<tr>
<td>0004H</td>
<td>Cybersecurity Solutions Architect</td>
<td>$214.82</td>
<td>$219.83</td>
<td>$224.95</td>
<td>$230.19</td>
</tr>
<tr>
<td>0005H</td>
<td>Cybersecurity Configuration Analyst II</td>
<td>$83.41</td>
<td>$85.35</td>
<td>$87.34</td>
<td>$89.37</td>
</tr>
<tr>
<td>0006H</td>
<td>Cybersecurity Configuration Analyst III</td>
<td>$99.20</td>
<td>$101.52</td>
<td>$103.88</td>
<td>$106.30</td>
</tr>
<tr>
<td>0007H</td>
<td>Cybersecurity Consultant</td>
<td>$150.78</td>
<td>$154.29</td>
<td>$157.88</td>
<td>$161.56</td>
</tr>
<tr>
<td>0008H</td>
<td>Data Security Analyst II</td>
<td>$75.61</td>
<td>$77.37</td>
<td>$79.18</td>
<td>$81.02</td>
</tr>
<tr>
<td>0009H</td>
<td>Data Security Analyst III</td>
<td>$92.53</td>
<td>$94.68</td>
<td>$96.89</td>
<td>$99.15</td>
</tr>
<tr>
<td>0010H</td>
<td>Data Security Analyst IV</td>
<td>$118.32</td>
<td>$121.07</td>
<td>$123.90</td>
<td>$126.78</td>
</tr>
<tr>
<td>0011H</td>
<td>Disaster Recovery Analyst</td>
<td>$72.02</td>
<td>$73.70</td>
<td>$75.42</td>
<td>$77.18</td>
</tr>
<tr>
<td>0012H</td>
<td>Enterprise Security Architect IV</td>
<td>$118.18</td>
<td>$120.93</td>
<td>$123.76</td>
<td>$126.64</td>
</tr>
<tr>
<td>0013H</td>
<td>Cybersecurity Enterprise Solutions Engineer</td>
<td>$214.82</td>
<td>$219.83</td>
<td>$224.95</td>
<td>$230.19</td>
</tr>
<tr>
<td>0014H</td>
<td>Information Security Analyst II</td>
<td>$75.40</td>
<td>$77.16</td>
<td>$78.96</td>
<td>$80.79</td>
</tr>
<tr>
<td>0015H</td>
<td>Information Security Analyst III</td>
<td>$91.49</td>
<td>$93.62</td>
<td>$95.81</td>
<td>$98.04</td>
</tr>
<tr>
<td>0016H</td>
<td>Information Security Analyst IV</td>
<td>$101.42</td>
<td>$103.79</td>
<td>$106.21</td>
<td>$108.68</td>
</tr>
<tr>
<td>0017H</td>
<td>Information Security Analyst V</td>
<td>$120.97</td>
<td>$123.79</td>
<td>$126.68</td>
<td>$129.63</td>
</tr>
<tr>
<td>0018H</td>
<td>Cybersecurity IT Project Manager III</td>
<td>$102.10</td>
<td>$104.48</td>
<td>$106.91</td>
<td>$109.41</td>
</tr>
<tr>
<td>0019H</td>
<td>Cybersecurity IT Project Manager IV</td>
<td>$116.58</td>
<td>$119.30</td>
<td>$122.08</td>
<td>$124.93</td>
</tr>
<tr>
<td>0020H</td>
<td>Cybersecurity Network Administrator I</td>
<td>$54.73</td>
<td>$56.01</td>
<td>$57.31</td>
<td>$58.65</td>
</tr>
<tr>
<td>0021H</td>
<td>Cybersecurity Network Administrator III</td>
<td>$79.29</td>
<td>$81.14</td>
<td>$83.03</td>
<td>$84.96</td>
</tr>
<tr>
<td>0022H</td>
<td>Cybersecurity Network Administrator IV</td>
<td>$98.66</td>
<td>$100.95</td>
<td>$103.31</td>
<td>$105.71</td>
</tr>
<tr>
<td>0023H</td>
<td>Cybersecurity Program Manager III</td>
<td>$152.31</td>
<td>$155.86</td>
<td>$159.49</td>
<td>$163.21</td>
</tr>
<tr>
<td>0024H</td>
<td>Cybersecurity Software Engineer V</td>
<td>$130.91</td>
<td>$133.97</td>
<td>$137.09</td>
<td>$140.28</td>
</tr>
<tr>
<td>0025H</td>
<td>Cybersecurity Subject Matter Expert I</td>
<td>$83.80</td>
<td>$85.75</td>
<td>$87.75</td>
<td>$89.79</td>
</tr>
<tr>
<td>0026H</td>
<td>Cybersecurity Subject Matter Expert III</td>
<td>$124.79</td>
<td>$127.70</td>
<td>$130.68</td>
<td>$133.73</td>
</tr>
<tr>
<td>0027H</td>
<td>Cybersecurity Subject Matter Expert IV</td>
<td>$154.20</td>
<td>$157.79</td>
<td>$161.47</td>
<td>$165.23</td>
</tr>
<tr>
<td>0028H</td>
<td>Cybersecurity Systems Administrator II</td>
<td>$63.68</td>
<td>$65.17</td>
<td>$66.68</td>
<td>$68.24</td>
</tr>
<tr>
<td>0029H</td>
<td>Cybersecurity Systems Engineer II</td>
<td>$75.58</td>
<td>$77.34</td>
<td>$79.15</td>
<td>$80.99</td>
</tr>
<tr>
<td>0030H</td>
<td>Cybersecurity Systems Engineer III</td>
<td>$108.18</td>
<td>$110.71</td>
<td>$113.29</td>
<td>$115.93</td>
</tr>
<tr>
<td>0031H</td>
<td>Cybersecurity Systems Engineer IV</td>
<td>$118.53</td>
<td>$121.29</td>
<td>$124.12</td>
<td>$127.01</td>
</tr>
</tbody>
</table>

* Rates shown above are inclusive of IFF fee.
** SCA labor categories are based on the U.S. Department of Labor Wage Determination Number 15-4281 Rev 7. The prices awarded are in line with the geographic scope of the contract.
## APPENDIX A – Contractor Site Rates

<table>
<thead>
<tr>
<th>LCat #</th>
<th>Labor Category</th>
<th>2020 Rate</th>
<th>2021 Rate</th>
<th>2022 Rate</th>
<th>2023 Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001S</td>
<td>Applications Systems Analyst II</td>
<td>$61.96</td>
<td>$63.41</td>
<td>$64.89</td>
<td>$66.39</td>
</tr>
<tr>
<td>0002S</td>
<td>Applications Systems Analyst III</td>
<td>$77.41</td>
<td>$79.21</td>
<td>$81.05</td>
<td>$82.94</td>
</tr>
<tr>
<td>0003S</td>
<td>Business Process Consultant</td>
<td>$84.87</td>
<td>$86.85</td>
<td>$88.87</td>
<td>$90.94</td>
</tr>
<tr>
<td>0004S</td>
<td>Business Process Solutions Architect</td>
<td>$232.01</td>
<td>$237.42</td>
<td>$242.95</td>
<td>$248.61</td>
</tr>
<tr>
<td>0005S</td>
<td>Configuration Analyst II</td>
<td>$90.08</td>
<td>$92.18</td>
<td>$94.33</td>
<td>$96.52</td>
</tr>
<tr>
<td>0006S</td>
<td>Configuration Analyst III</td>
<td>$107.14</td>
<td>$109.64</td>
<td>$112.19</td>
<td>$114.80</td>
</tr>
<tr>
<td>0007S</td>
<td>Consultant</td>
<td>$162.84</td>
<td>$166.63</td>
<td>$170.51</td>
<td>$174.48</td>
</tr>
<tr>
<td>0008S</td>
<td>Data Security Analyst II</td>
<td>$81.66</td>
<td>$83.56</td>
<td>$85.51</td>
<td>$87.50</td>
</tr>
<tr>
<td>0009S</td>
<td>Data Security Analyst III</td>
<td>$99.93</td>
<td>$102.25</td>
<td>$104.64</td>
<td>$107.08</td>
</tr>
<tr>
<td>0010S</td>
<td>Data Security Analyst IV</td>
<td>$127.79</td>
<td>$130.76</td>
<td>$133.81</td>
<td>$136.92</td>
</tr>
<tr>
<td>0011S</td>
<td>Disaster Recovery Analyst</td>
<td>$77.78</td>
<td>$79.60</td>
<td>$81.45</td>
<td>$83.35</td>
</tr>
<tr>
<td>0012S</td>
<td>Enterprise Infrastructure Architect IV</td>
<td>$127.63</td>
<td>$130.60</td>
<td>$133.66</td>
<td>$136.77</td>
</tr>
<tr>
<td>0013S</td>
<td>Enterprise Solutions Engineer</td>
<td>$232.01</td>
<td>$237.42</td>
<td>$242.95</td>
<td>$248.61</td>
</tr>
<tr>
<td>0014S</td>
<td>Information Security Analyst II</td>
<td>$81.43</td>
<td>$83.33</td>
<td>$85.28</td>
<td>$87.25</td>
</tr>
<tr>
<td>0015S</td>
<td>Information Security Analyst III</td>
<td>$98.81</td>
<td>$101.11</td>
<td>$103.47</td>
<td>$105.88</td>
</tr>
<tr>
<td>0016S</td>
<td>Information Security Analyst IV</td>
<td>$109.53</td>
<td>$112.09</td>
<td>$114.71</td>
<td>$117.37</td>
</tr>
<tr>
<td>0017S</td>
<td>Information Security Analyst V</td>
<td>$130.65</td>
<td>$133.69</td>
<td>$136.81</td>
<td>$140.00</td>
</tr>
<tr>
<td>0018S</td>
<td>IT Project Manager III</td>
<td>$110.27</td>
<td>$112.84</td>
<td>$115.46</td>
<td>$118.16</td>
</tr>
<tr>
<td>0019S</td>
<td>IT Project Manager IV</td>
<td>$125.91</td>
<td>$128.84</td>
<td>$131.85</td>
<td>$134.92</td>
</tr>
<tr>
<td>0020S</td>
<td>Network Administrator I</td>
<td>$59.11</td>
<td>$60.49</td>
<td>$61.89</td>
<td>$63.34</td>
</tr>
<tr>
<td>0021S</td>
<td>Network Administrator III</td>
<td>$85.63</td>
<td>$87.63</td>
<td>$89.67</td>
<td>$91.76</td>
</tr>
<tr>
<td>0022S</td>
<td>Network Administrator IV</td>
<td>$106.55</td>
<td>$109.03</td>
<td>$111.57</td>
<td>$114.17</td>
</tr>
<tr>
<td>0023S</td>
<td>Program Manager III</td>
<td>$164.49</td>
<td>$168.33</td>
<td>$172.25</td>
<td>$176.27</td>
</tr>
<tr>
<td>0024S</td>
<td>Software Engineer V</td>
<td>$141.38</td>
<td>$144.69</td>
<td>$148.06</td>
<td>$151.50</td>
</tr>
<tr>
<td>0025S</td>
<td>Subject Matter Expert I</td>
<td>$90.50</td>
<td>$92.61</td>
<td>$94.77</td>
<td>$96.97</td>
</tr>
<tr>
<td>0026S</td>
<td>Subject Matter Expert III</td>
<td>$134.77</td>
<td>$137.92</td>
<td>$141.13</td>
<td>$144.43</td>
</tr>
<tr>
<td>0027S</td>
<td>Subject Matter Expert IV</td>
<td>$166.54</td>
<td>$170.41</td>
<td>$174.39</td>
<td>$178.45</td>
</tr>
<tr>
<td>0028S</td>
<td>Systems Administrator II</td>
<td>$68.77</td>
<td>$70.38</td>
<td>$72.01</td>
<td>$73.70</td>
</tr>
<tr>
<td>0029S</td>
<td>Systems Engineer II</td>
<td>$81.63</td>
<td>$83.53</td>
<td>$85.48</td>
<td>$87.47</td>
</tr>
<tr>
<td>0030S</td>
<td>Systems Engineer III</td>
<td>$116.83</td>
<td>$119.57</td>
<td>$122.35</td>
<td>$125.20</td>
</tr>
<tr>
<td>0031S</td>
<td>Systems Engineer IV</td>
<td>$128.01</td>
<td>$130.99</td>
<td>$134.05</td>
<td>$137.17</td>
</tr>
</tbody>
</table>

## Ancillary Supplies and/or Services (54151S) – Contractor Site Rates*

<table>
<thead>
<tr>
<th>LCat #</th>
<th>Labor Category</th>
<th>2020 Rate</th>
<th>2021 Rate</th>
<th>2022 Rate</th>
<th>2023 Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001A</td>
<td>Help Desk Support Assistant**</td>
<td>$42.78</td>
<td>$43.77</td>
<td>$44.79</td>
<td>$45.84</td>
</tr>
<tr>
<td>0002A</td>
<td>Help Desk Support**</td>
<td>$50.94</td>
<td>$52.13</td>
<td>$53.35</td>
<td>$54.59</td>
</tr>
<tr>
<td>LCat #</td>
<td>Labor Category</td>
<td>2020 Rate</td>
<td>2021 Rate</td>
<td>2022 Rate</td>
<td>2023 Rate</td>
</tr>
<tr>
<td>-------</td>
<td>----------------------------------------</td>
<td>-----------</td>
<td>-----------</td>
<td>-----------</td>
<td>-----------</td>
</tr>
<tr>
<td>0001H</td>
<td>Cybersecurity Applications Analyst II</td>
<td>$61.96</td>
<td>$63.41</td>
<td>$64.89</td>
<td>$66.39</td>
</tr>
<tr>
<td>0002H</td>
<td>Cybersecurity Applications Analyst III</td>
<td>$77.41</td>
<td>$79.21</td>
<td>$81.05</td>
<td>$82.94</td>
</tr>
<tr>
<td>0003H</td>
<td>Cybersecurity Process Consultant</td>
<td>$84.87</td>
<td>$86.85</td>
<td>$88.87</td>
<td>$90.94</td>
</tr>
<tr>
<td>0004H</td>
<td>Cybersecurity Solutions Architect</td>
<td>$232.01</td>
<td>$237.42</td>
<td>$242.95</td>
<td>$248.61</td>
</tr>
<tr>
<td>0005H</td>
<td>Cybersecurity Configuration Analyst II</td>
<td>$90.08</td>
<td>$92.18</td>
<td>$94.33</td>
<td>$96.52</td>
</tr>
<tr>
<td>0006H</td>
<td>Cybersecurity Configuration Analyst III</td>
<td>$107.14</td>
<td>$109.64</td>
<td>$112.19</td>
<td>$114.80</td>
</tr>
<tr>
<td>0007H</td>
<td>Cybersecurity Consultant</td>
<td>$162.84</td>
<td>$166.63</td>
<td>$170.51</td>
<td>$174.48</td>
</tr>
<tr>
<td>0008H</td>
<td>Data Security Analyst II</td>
<td>$81.66</td>
<td>$83.56</td>
<td>$85.51</td>
<td>$87.50</td>
</tr>
<tr>
<td>0009H</td>
<td>Data Security Analyst III</td>
<td>$99.93</td>
<td>$102.25</td>
<td>$104.64</td>
<td>$107.08</td>
</tr>
<tr>
<td>0010H</td>
<td>Data Security Analyst IV</td>
<td>$127.79</td>
<td>$130.76</td>
<td>$133.81</td>
<td>$136.92</td>
</tr>
<tr>
<td>0011H</td>
<td>Disaster Recovery Analyst</td>
<td>$77.78</td>
<td>$79.60</td>
<td>$81.45</td>
<td>$83.35</td>
</tr>
<tr>
<td>0012H</td>
<td>Enterprise Security Architect IV</td>
<td>$127.63</td>
<td>$130.60</td>
<td>$133.66</td>
<td>$136.77</td>
</tr>
<tr>
<td>0013H</td>
<td>Cybersecurity Enterprise Solutions Engineer</td>
<td>$232.01</td>
<td>$237.42</td>
<td>$242.95</td>
<td>$248.61</td>
</tr>
<tr>
<td>0014H</td>
<td>Information Security Analyst II</td>
<td>$81.43</td>
<td>$83.33</td>
<td>$85.28</td>
<td>$87.25</td>
</tr>
<tr>
<td>0015H</td>
<td>Information Security Analyst III</td>
<td>$98.81</td>
<td>$101.11</td>
<td>$103.47</td>
<td>$105.88</td>
</tr>
<tr>
<td>0016H</td>
<td>Information Security Analyst IV</td>
<td>$109.53</td>
<td>$112.09</td>
<td>$114.71</td>
<td>$117.37</td>
</tr>
<tr>
<td>0017H</td>
<td>Information Security Analyst V</td>
<td>$130.65</td>
<td>$133.69</td>
<td>$136.81</td>
<td>$140.00</td>
</tr>
<tr>
<td>0018H</td>
<td>Cybersecurity IT Project Manager III</td>
<td>$110.27</td>
<td>$112.84</td>
<td>$115.46</td>
<td>$118.16</td>
</tr>
<tr>
<td>0019H</td>
<td>Cybersecurity IT Project Manager IV</td>
<td>$125.91</td>
<td>$128.84</td>
<td>$131.85</td>
<td>$134.92</td>
</tr>
<tr>
<td>0020H</td>
<td>Cybersecurity Network Administrator I</td>
<td>$59.11</td>
<td>$60.49</td>
<td>$61.89</td>
<td>$63.34</td>
</tr>
<tr>
<td>0021H</td>
<td>Cybersecurity Network Administrator III</td>
<td>$85.63</td>
<td>$87.63</td>
<td>$89.67</td>
<td>$91.76</td>
</tr>
<tr>
<td>0022H</td>
<td>Cybersecurity Network Administrator IV</td>
<td>$106.55</td>
<td>$109.03</td>
<td>$111.57</td>
<td>$114.17</td>
</tr>
<tr>
<td>0023H</td>
<td>Cybersecurity Program Manager III</td>
<td>$164.49</td>
<td>$168.33</td>
<td>$172.25</td>
<td>$176.27</td>
</tr>
<tr>
<td>0024H</td>
<td>Cybersecurity Software Engineer V</td>
<td>$141.38</td>
<td>$144.69</td>
<td>$148.06</td>
<td>$151.50</td>
</tr>
<tr>
<td>0025H</td>
<td>Cybersecurity Subject Matter Expert I</td>
<td>$90.50</td>
<td>$92.61</td>
<td>$94.77</td>
<td>$96.97</td>
</tr>
<tr>
<td>0026H</td>
<td>Cybersecurity Subject Matter Expert III</td>
<td>$134.77</td>
<td>$137.92</td>
<td>$141.13</td>
<td>$144.43</td>
</tr>
<tr>
<td>0027H</td>
<td>Cybersecurity Subject Matter Expert IV</td>
<td>$166.54</td>
<td>$170.41</td>
<td>$174.39</td>
<td>$178.45</td>
</tr>
<tr>
<td>0028H</td>
<td>Cybersecurity Systems Administrator II</td>
<td>$68.77</td>
<td>$70.38</td>
<td>$72.01</td>
<td>$73.70</td>
</tr>
<tr>
<td>0029H</td>
<td>Cybersecurity Systems Engineer II</td>
<td>$81.63</td>
<td>$83.53</td>
<td>$85.48</td>
<td>$87.47</td>
</tr>
<tr>
<td>0030H</td>
<td>Cybersecurity Systems Engineer III</td>
<td>$116.83</td>
<td>$119.57</td>
<td>$122.35</td>
<td>$125.20</td>
</tr>
<tr>
<td>0031H</td>
<td>Cybersecurity Systems Engineer IV</td>
<td>$128.01</td>
<td>$130.99</td>
<td>$134.05</td>
<td>$137.17</td>
</tr>
</tbody>
</table>

* Rates shown above are inclusive of IFF fee.
** SCA labor categories are based on the U.S. Department of Labor Wage Determination Number 15-4281 Rev 7. The prices awarded are in line with the geographic scope of the contract.
APPENDIX B

Terms and Conditions Applicable to Information Technology (IT) Professional Services
(Special Item Number 54151S, formerly 132-51)

All offerors must follow the evaluation criteria and instructions outlined in the MAS solicitation, including in SCP-FSS-001. The Information Technology Category Attachment outlines additional evaluation criteria, requirements, and information specific to this category only. For a list of required Schedule templates and attachments, please visit www.gsa.gov/mascategoryrequirements.

1 SCOPE

a. The prices, terms, and conditions stated under Special Item Number 132-51 Information Technology Professional. Services apply exclusively to IT Professional Services within the scope of this Information Technology Schedule.

b. The Contractor shall provide services at the Contractor’s facility and/or at the ordering activity location, as agreed to by the Contractor and the ordering activity.

2 PERFORMANCE INCENTIVES I-FSS-60 Performance Incentives (April 2000)

a. Performance incentives may be agreed upon between the Contractor and the ordering activity on individual fixed price orders or Blanket Purchase Agreements under this contract.

b. The ordering activity must establish a maximum performance incentive price for these services and/or total solutions on individual orders or Blanket Purchase Agreements.

c. Incentives should be designed to relate results achieved by the contractor to specified targets. To the maximum extent practicable, ordering activities shall consider establishing incentives where performance is critical to the ordering activity’s mission and incentives are likely to motivate the contractor. Incentives shall be based on objectively measurable tasks.

3 ORDER

a. Agencies may use written orders, EDI orders, blanket purchase agreements, individual purchase orders, or task orders for ordering services under this contract. Blanket Purchase Agreements shall not extend beyond the end of the contract period; all services and delivery shall be made, and the contract terms and conditions shall continue in effect until the completion of the order. Orders for tasks which extend beyond the fiscal year for which funds are available shall include FAR 52.232-19 (Deviation – May 2003) Availability of Funds for the Next Fiscal Year. The purchase order shall specify the availability of funds and the period for which funds are available.

b. All task orders are subject to the terms and conditions of the contract. In the event of a conflict between a task order and the contract, the contract will take precedence.

4 PERFORMANCE OF SERVICES

www.gcyber.com

B-1

sales@gcyber.com
a. The Contractor shall commence the performance of services on the date agreed to by the Contractor and the ordering activity.

b. The Contractor agrees to render services only during normal working hours unless otherwise agreed to by the Contractor and the ordering activity.

c. The ordering activity should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner.

Any Contractor travel required in the performance of IT Services must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel. Contractors cannot use GSA city pair contracts.

5 STOP-WORK ORDER (FAR 52.242-15) (AUG 1989)

a. The Contracting Officer may, at any time, by written order to the Contractor, require the Contractor to stop all, or any part, of the work called for by this contract for a period of 90 days after the order is delivered to the Contractor, and for any further period to which the parties may agree. The order shall be specifically identified as a stop-work order issued under this clause. Upon receipt of the order, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the order during the period of the work stoppage. Within a period of 90 days after a stop-work is delivered to the Contractor, or within any extension of that period to which the parties shall have agreed, the Contracting Officer shall either-

   i. Cancel the stop-work order; or

   ii. Terminate the work covered by the order as provided in the Default, or the Termination for Convenience of the Government, clause of this contract.

b. If a stop-work order issued under this clause is canceled or the period of the order or any extension thereof expires, the Contractor shall resume work. The Contracting Officer shall make an equitable adjustment in the delivery schedule, contract price, or both, and the contract shall be modified, in writing, accordingly, if-

   i. The stop-work order results in an increase in the time required for, or in the Contractor’s cost properly allocable to, the performance of any part of this contract; and

   ii. The Contractor asserts its right to the adjustment within 30 days after the end of the period of work stoppage; provided, that, if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon the claim submitted at any time before final payment under this contract.

c. If a stop-work order is not canceled and the work covered by the order is terminated for the convenience of the Government, the Contracting Officer shall allow reasonable costs resulting from the stop-work order in arriving at the termination settlement.
d. If a stop-work order is not canceled and the work covered by the order is terminated for default, the Contracting Officer shall allow, by equitable adjustment or otherwise, reasonable costs resulting from the stop-work order.

6 INSPECTION OF SERVICES


7 RESPONSIBILITIES OF THE CONTRACTOR

The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character. If the end product of a task order is software, then FAR 52.227-14 (Dec 2007) Rights in Data – General, may apply.

8 RESPONSIBILITIES OF THE ORDERING ACTIVITY

Subject to security regulations, the ordering activity shall permit Contractor access to all facilities necessary to perform the requisite IT Professional Services.

9 INDEPENDENT CONTRACTOR

All IT Professional Services performed by the Contractor under the terms of this contract shall be as an independent Contractor, and not as an agent or employee of the ordering activity.

10 ORGANIZATIONAL CONFLICTS OF INTEREST

a. Definitions.

“Contractor” means the person, firm, unincorporated association, joint venture, partnership, or corporation that is a party to this contract.

“Contractor and its affiliates” and “Contractor or its affiliates” refers to the Contractor, its chief executives, directors, officers, subsidiaries, affiliates, subcontractors at any tier, and consultants and any joint venture involving the Contractor, any entity into or with which the Contractor subsequently merges or affiliates, or any other successor or assignee of the Contractor.

An “Organizational conflict of interest“ exists when the nature of the work to be performed under a proposed ordering activity contract, without some restriction on ordering activities by the Contractor and its affiliates, may either (i) result in an unfair competitive advantage to the Contractor or its affiliates or (ii) impair the Contractor’s or its affiliates’ objectivity in performing contract work.

b. To avoid an organizational or financial conflict of interest and to avoid prejudicing the best interests of the ordering activity, ordering activities may place restrictions on the Contractors, its affiliates, chief executives, directors, subsidiaries and subcontractors at any tier when placing orders against schedule contracts. Such restrictions shall be consistent with FAR 9.505 and shall

www.gcyber.com

B-3

sales@gcyber.com
be designed to avoid, neutralize, or mitigate organizational conflicts of interest that might otherwise exist in situations related to individual orders placed against the schedule contract. Examples of situations, which may require restrictions, are provided at FAR 9.508.

11 INVOICES
The Contractor, upon completion of the work ordered, shall submit invoices for IT Professional Services. Progress payments may be authorized by the ordering activity on individual orders if appropriate. Progress payments shall be based upon completion of defined milestones or interim products. Invoices shall be submitted monthly for recurring services performed during the preceding month.

12 PAYMENTS
For firm-fixed price orders the ordering activity shall pay the Contractor, upon submission of proper invoices or vouchers, the prices stipulated in this contract for service rendered and accepted. Progress payments shall be made only when authorized by the order. For time and materials orders, the Payments under Time and Materials and Labor Hour Contracts at FAR 52.212-4 (MAR 2009) (ALTERNATE I – OCT 2008) (DEVIAITION I – FEB 2007) applies to time and materials orders placed under this contract. For labor hour orders, the Payment under Time and Materials and Labor Hour Contracts at FAR 52.212-4 (MAR 2009) (ALTERNATE I – OCT 2008) (DEVIAITION I – FEB 2007) applies to labor hour orders placed under this contract. 52.216-31(Feb 2007) Time-and-Materials/Labor-Hour Proposal Requirements—Commercial Item Acquisition. As prescribed in 16.601(e)(3), insert the following provision:

a. The Government contemplates award of a Time-and-Materials or Labor-Hour type of contract resulting from this solicitation.

b. The offeror must specify fixed hourly rates in its offer that include wages, overhead, general and administrative expenses, and profit. The offeror must specify whether the fixed hourly rate for each labor category applies to labor performed by—

   i. The offeror.

   ii. Subcontractors; and/or

   iii. Divisions, subsidiaries, or affiliates of the offeror under a common control.

13 RESUMES
Resumes shall be provided to the GSA Contracting Officer or the user ordering activity upon request.

14 INCIDENTAL SUPPORT COSTS
Incidental support costs are available outside the scope of this contract. The costs will be negotiated separately with the ordering activity in accordance with the guidelines set forth in the FAR.

15 APPROVAL OF SUBCONTRACTS
The ordering activity may require that the Contractor receive, from the ordering activity’s Contracting Officer, written consent before placing any subcontract for furnishing any of the work called for in a task order.

16 DESCRIPTION OF IT PROFESSIONAL SERVICES AND PRICING

a. The Contractor shall provide a description of each type of IT Service offered under Special Item Numbers 132-51 IT Professional Services should be presented in the same manner as the Contractor sells to its commercial and other ordering activity customers. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles (labor categories) for those individuals who will perform the service should be provided.

b. Pricing for all IT Professional Services shall be in accordance with the Contractor’s customary commercial practices, e.g., hourly rates, monthly rates, term rates, and/or fixed prices, minimum general experience, and minimum education.
Terms and Conditions Applicable to Highly Adaptive Cybersecurity Services (HACS)
(Special Item Number 54151HACS, formerly 132-45)

All offerors must follow the evaluation criteria and instructions outlined in the MAS solicitation, including in SCP-FSS-001. The Information Technology Category Attachment outlines additional evaluation criteria, requirements, and information specific to this category only. For a list of required Schedule templates and attachments, please visit www.gsa.gov/mascategoryrequirements.
For additional guidance and information for Schedule buyers and sellers, please visit our general guidance page at www.gsa.gov/schedules.

54151HACS includes a wide range of fields such as the seven-step Risk Management Framework services, information assurance, virus detection, network management, situational awareness and incident response, secure web hosting, and backup, security services, and, Security Operations Center (SOC) services. HACS vendors are cataloged under the 5 subcategories of High Value Asset Assessments; Risk and Vulnerability Assessments, Cyber Hunt, Incident Response, and Penetration Testing.

NOTE: Subject to Cooperative Purchasing

Instructions:
Additional SIN Description: Includes proactive and reactive cybersecurity services that improve customer enterprise-level security posture. Services to identify and protect a customer’s information resources, detect and respond to cybersecurity events or incidents, and recover capabilities or services impaired by any incidents that emerge.

It encompasses a wide range of fields that include, but are not limited to, Risk Management Framework (RMF) services, information assurance (IA), virus detection, network management, situational awareness and incident response, secure web hosting, and backup and security services.

The seven-step RMF includes preparation, information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. RMF activities may also include Information Security Continuous Monitoring Assessment (ISCMCA), which evaluate organization-wide ISCM implementations, and also Federal Incident Response Evaluations (FIREs), which assess an organization’s incident management functions.

It also includes Security Operations Center (SOC) services. The SOC scope includes services such as: 24x7x365 monitoring and analysis, traffic analysis, incident response and coordination, penetration testing, anti-virus management, intrusion detection and prevention, and information sharing.

1) Specific Instructions for SIN 54151HACS – Highly Adaptive Cybersecurity Services (HACS)

a) Offerers may request to be placed in the following subcategories.

i) High Value Asset (HVA) Assessments include Risk and Vulnerability Assessment (RVA) which assesses threats and vulnerabilities, determines deviations from acceptable configurations,
enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations. The services offered in the RVA sub-category include Network Mapping, Vulnerability Scanning, Phishing Assessment, Wireless Assessment, Web Application Assessment, Operating System Security Assessment (OSSA), Database Assessment, and Penetration Testing. Security Architecture Review (SAR) evaluates a subset of the agency’s HVA security posture to determine whether the agency has properly architected its cybersecurity solutions and ensures that agency leadership fully understands the risks inherent in the implemented cybersecurity solution. The SAR process utilizes in-person interviews, documentation reviews, and leading practice evaluations of the HVA environment and supporting systems. SAR provides a holistic analysis of how an HVA’s individual security components integrate and operate, including how data is protected during operations. Systems Security Engineering (SSE) identifies security vulnerabilities and minimizes or contains risks associated with these vulnerabilities spanning the Systems Development Life Cycle. SSE focuses on but is not limited to the following security areas: perimeter security, network security, endpoint security, application security, physical security, and data security.

ii) Risk and Vulnerability Assessment (RVA) assesses threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations. The services offered in the RVA sub-category include Network Mapping, Vulnerability Scanning, Phishing Assessment, Wireless Assessment, Web Application Assessment, Operating System Security Assessment (OSSA), Database Assessment, and Penetration Testing.

iii) Penetration Testing is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network.

iv) Incident Response services help organizations impacted by a cybersecurity compromise determine the extent of the incident, remove the adversary from their systems, and restore their networks to a more secure state.

v) Cyber Hunt activities respond to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Cyber Hunts start with the premise that threat actors known to target some organizations in a specific industry or with specific systems are likely to also target other organizations in the same industry or with the same systems.

b) Services offered SIN 54151HACS shall be in accordance with the following laws and standards when applicable to the specific task orders, including but not limited to:

Federal Acquisition Regulation (FAR) Part 52.204-21
OMB Memorandum M-17-12 - Preparing for and Responding to a Breach of Personally Identifiable Information (PII)
OMB Memorandum M-19-03 - Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program
2017 Report to the President on Federal IT Modernization
The Cybersecurity National Action Plan (CNAP)
NIST SP 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems
NIST SP 800-27A - Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
NIST SP 800-30 - Guide for Conducting Risk Assessments
NIST SP 800-35 - Guide to Information Technology Security Services
NIST SP 800-44 - Guidelines on Securing Public Web Servers
NIST SP 800-48 - Guide to Securing Legacy IEEE 802.11 Wireless Networks
NIST SP 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations
NIST SP 800-61 - Computer Security Incident Handling Guide
NIST SP 800-64 - Security Considerations in the System Development Life Cycle
NIST SP 800-82 - Guide to Industrial Control Systems (ICS) Security
NIST SP 800-86 - Guide to Integrating Forensic Techniques into Incident Response
NIST SP 800-115 - Technical Guide to Information Security Testing and Assessment
NIST SP 800-137 - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
NIST SP 800-153 - Guidelines for Securing Wireless Local Area Networks (WLANs)
NIST SP 800-160 - Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
NIST SP 800-171 - Protecting Controlled Unclassified Information in non-federal Information Systems and Organizations.

c) All professional labor categories under SIN 54151S Information Technology Professional Services may remain there unless the labor categories are specific to SIN 54151HACS

2) Oral Technical Evaluation for SIN 54151HACS - Highly Adaptive Cybersecurity Services (HACS)

a) Unless otherwise specified, the offeror shall participate in an oral technical evaluation that will be conducted by a Technical Evaluation Board (TEB). The oral technical evaluation will be held at the unclassified level and will be scheduled by the TEB. The oral technical evaluation will be used to assess the offeror’s capability to successfully perform the services within the scope of each subcategory as set forth in this solicitation, excepting those service components awarded through the submission of the Service Self-Attestation. The Self-Attestation form is available at gsa.gov/hacs.
An offeror may only be awarded SIN 54151HACS upon successful completion of the Highly Adaptive Cybersecurity Services oral technical evaluation. If the offeror elects to be cataloged under the "Cyber Hunt" and/or "Incident Response" subcategories, additional questions related to those areas will be asked during the HACS Oral Technical Evaluation.

i) **ORAL TECHNICAL EVALUATION CONSTRAINTS:** The offeror shall identify up to five key personnel, by name and association with the offeror, who will field questions during the oral technical evaluation. The HACS SIN consists of 5 subcategories. The base HACS Oral Technical Evaluation consists of questions related to the 3 subcategories of, High Value Asset Assessments, Risk and Vulnerability Assessments and Penetration Testing. One (1) hour and 40 minutes is allotted for the base HACS Oral Technical Evaluation. The evaluation will be stopped precisely after 1 hour and 40 minutes. Should the offer elect to be considered for the additional subcategories of Incident Response and Cyber Hunt, an additional 10 minutes will be allotted for each of those subcategories. The total base evaluation session is expected to last up to 1 hour and 40 minutes, depending on the number of subcategories the offeror is proposing. The TEB Chairperson will be responsible for ensuring the schedule is met and that

ii) **ORAL TECHNICAL EVALUATION SCHEDULING:** The TEB will contact the offeror's authorized negotiator or the signatory of the SF 1449 via email to schedule the oral technical evaluation. Evaluation time slots will be assigned on a first-come-first-served basis. The Government reserves the right to reschedule any offeror's oral technical evaluation at its sole discretion. The oral technical evaluation will be held at facilities designated by the TEB. The exact location, seating capacity, and any other relevant information will be provided when the evaluations are scheduled. The Government may also make accommodations for vendors to participate in the oral evaluations virtually.

iii) **PROHIBITION OF ELECTRONIC RECORDING OF THE ORAL TECHNICAL EVALUATION:** The offeror may not record or transmit any of the oral evaluation process. All offeror's electronic devices shall be removed from the room during the evaluation. The offeror is permitted to have a timer in the room during the evaluation, provided by the TEB.

iv) **RESUBMISSION RESTRICTIONS FOR UNSUCCESSFUL VENDORS UNDER THIS EVALUATION FACTOR:** The TEB will afford the offeror multiple opportunities to achieve the "pass" criteria under this evaluation factor through "clarification" questioning, during the Oral Technical Evaluation. Any offeror whom the TEB has found to have not passed under this evaluation factor shall be failed and shall be ineligible to re-submit under the SIN to participate in this evaluation factor for a period of six (6) months following the date of failure.

v) **HIGH VALUE ASSET (HVA) ASSESSMENTS SUBCATEGORY PLACEMENT:** Any offeror previously awarded all of the following four SINS: 132-45A Penetration Testing, 132-45B Incident Response, 132-45C Cyber Hunt, and 132-45D Risk and Vulnerability Assessment, shall not be subject to a Highly Adaptive Cybersecurity Services oral technical evaluation, so long as they provide in the modification package to the GSA contracting officer a Service Self-Attestation acknowledging their ability to perform Security Architecture Review (SAR) and Systems Evaluation.
Security Engineering (SSE) services in their entirety. The Self-Attestation form is available at gsa.gov/hacs.

b) Oral Technical Evaluation Procedures: The offeror will be evaluated on their knowledge of the proposed services. The oral technical evaluation will require the offeror to respond to a specific scenario and general questions to assess the offeror’s expertise. The competencies, criteria and evaluation minimums for the questions are below: All new offerors and modifications must participate in and PASS the HACS Oral Technical Evaluation. The Oral Technical Evaluation will include, at a minimum, questions on Risk and Vulnerability Assessment (RVA), Security Architecture Review (SAR), Systems Security Engineering (SSE), and Penetration Testing. At the time of submission, all new offerors and modifications can also elect to be cataloged in one or both of the additional subcategories of Cyber Hunt or Incident Response (IR). Should this election be taken, additional questions related to these subcategories will be included in their HACS evaluation and these additional subcategory topics must be passed as well.

c) Oral Technical Evaluation Criteria: The offeror’s responses to the government’s questions during the oral technical evaluation session shall be used to determine whether the offeror has the requisite experience and expertise to perform tasks expected to be performed within the scope of the SIN. The oral technical proposal will be evaluated and rated on a pass/fail basis. The rating definitions provided below will be used for the evaluation of the offeror’s responses to questions during the oral evaluation.

<table>
<thead>
<tr>
<th>TECHNICAL RATINGS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rating</td>
</tr>
<tr>
<td>Acceptable</td>
</tr>
<tr>
<td>Unacceptable</td>
</tr>
</tbody>
</table>
Terms and Conditions Applicable to Ancillary Supplies and/or Services
(Special Item Number 54151S, Formerly 132-100)

Ancillary supplies and/or services are support supplies and services which are not within the scope of any ITC SIN, and shall be offered under the ANCILLARY SIN, which is offered under the Miscellaneous large category.

Non-professional labor categories must be incidental to and used solely to support hardware, software and/or professional services, and cannot be purchased separately. Non-professional labor categories shall be offered under the ANCILLARY SIN, which is offered under the Miscellaneous large category.

Energy Star or Electronic Product Environmental Assessment Tool (EPEAT) programs. Commercially available products under this solicitation may be covered by the Energy Star or Electronic Product Environmental Assessment Tool (EPEAT) programs. For applicable products, offerors are encouraged to offer Energy Star-qualified products and EPEAT-registered products, at the Bronze level or higher. If offerors opt to offer Energy Star or Electronic Product Environmental Assessment Tool (EPEAT) products then they shall identify by model which products offered are Energy Star-qualified and EPEAT-registered, broken out by registration level of bronze, silver, or gold. Visit the Green Procurement Compilation, sftool.gov/greenprocurement for a complete list of products covered by these programs.

Instructions: The work performed under this SIN shall be associated with existing SIN(s) under the contract. Ancillary supplies and/or services shall not be the primary purpose of the work ordered, but be an integral part of the total solution offered. Ancillary supplies and/or services may only be ordered in conjunction with or in support of supplies or services purchased under another SIN(s). Offerors may be required to provide additional information to support a determination that their proposed ancillary supplies and/or services are commercially offered in support of one or more SIN(s).

The Miscellaneous Category Attachment outlines additional evaluation criteria, requirements, and information specific to this category only. For a list of required Schedule templates and attachments, please visit www.gsa.gov/mascategoryrequirements

Note: When used in conjunction with a Cooperative Purchasing eligible SIN, this SIN is Cooperative Purchasing Eligible.

Regulation Number Regulation Title/Comments
52.222-46 EVALUATION OF COMPENSATION FOR PROFESSIONAL EMPLOYEES (FEB 1993)
52.222-48 EXEMPTION FROM APPLICATION OF THE SERVICE CONTRACT LABOR STANDARDS TO CONTRACTS FOR MAINTENANCE, CALIBRATION, OR REPAIR OF CERTAIN EQUIPMENT CERTIFICATION (MAY 2014)
52.223-2 AFFIRMATIVE PROCUREMENT OF BIOBASED PRODUCTS UNDER SERVICE AND CONSTRUCTION CONTRACTS (SEP 2013)
52.228-5 INSURANCE - WORK ON A GOVERNMENT INSTALLATION (JAN 1997)
52.229-1 STATE AND LOCAL TAXES (APR 1984)
52.247-68 REPORT OF SHIPMENT (REPSHIP) (FEB 2006)
52.222-62 PAID SICK LEAVE UNDER EXECUTIVE ORDER 13706 (JAN 2017)

www.gcyber.com B-11 sales@gcyber.com
52.222-52 EXEMPTION FROM APPLICATION OF THE SERVICE CONTRACT LABOR STANDARDS TO CONTRACTS FOR CERTAIN SERVICES - CERTIFICATION (MAY 2014)

52.223-11 OZONE-DEPLETING SUBSTANCES AND HIGH GLOBAL WARMING POTENTIAL HYDROFLUOROCARBONS (JUN 2016)

52.225-18 PLACE OF MANUFACTURE (AUG 2018)

552.238-105 DELIVERIES BEYOND THE CONTRACTUAL PERIOD - PLACING OF ORDERS (MAY 2019)
552.238-107 TRAFFIC RELEASE (SUPPLIES) (MAY 2019)
552.238-86 DELIVERY SCHEDULE (MAY 2019)
552.238-89 DELIVERIES TO THE U.S. POSTAL SERVICE (MAY 2019)
552.238-90 CHARACTERISTICS OF ELECTRIC CURRENT (MAY 2019)
552.238-91 MARKING AND DOCUMENTATION REQUIREMENTS FOR SHIPPING (MAY 2019)
552.238-92 VENDOR MANAGED INVENTORY (VMI) PROGRAM (MAY 2019)
552.238-93 ORDER ACKNOWLEDGMENT (MAY 2019)
552.238-94 ACCELERATED DELIVERY REQUIREMENTS (MAY 2019)
552.238-95 SEPARATE CHARGE FOR PERFORMANCE ORIENTED PACKAGING (POP) (MAY 2019)
552.238-96 SEPARATE CHARGE FOR DELIVERY WITHIN CONSIGNEE'S PREMISES (MAY 2019)
552.238-111 ENVIRONMENTAL PROTECTION AGENCY REGISTRATION REQUIREMENT (MAY 2019)
APPENDIX C

54151S Labor Category Descriptions

Applications Systems Analyst II
Experience: 2 to 4 years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non- degreed = 6 yrs. of experience)
Job Duties: Researches, analyzes, and modifies programming systems including encoding, testing, debugging, and installing to support an organization’s application systems. Consults with users to identify current operating procedures and to clarify program objectives. Writes manuals for users to describe installation and operating procedures. May write documentation to describe program development, logic, coding, and corrections. Typically reports to a project leader or manager. Gaining exposure to some of the complex tasks within the job function. Occasionally directed in several aspects of the work.

Applications Systems Analyst III
Experience: 4 to 7 years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non- degreed = 6 yrs. of experience)
Job Duties: Researches, analyzes, and modifies programming systems including encoding, testing, debugging, and installing to support an organization’s application systems. Consults with users to identify current operating procedures and to clarify program objectives. Writes manuals for users to describe installation and operating procedures. May write documentation to describe program development, logic, coding, and corrections. Typically reports to a project leader or manager. Contributes to moderately complex aspects of a project. Work is generally independent and collaborative in nature.

Business Process Consultant
Experience: 10+ years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non- degreed = 6 yrs. of experience)
Job Duties: Researches and analyzes basic and complex issues surrounding the business processes of an organization. Makes recommendations surrounding improving processes, efficiency and practices. Simulates and tests process improvements. Communicates changes and may provide training to impacted business units. Typically reports to top management. Works on advanced, complex technical projects or business issues requiring state of the art technical or industry knowledge. Works autonomously. Goals are generally communicated in solution" or project goal terms.

Business Process Solutions Architect
Experience: 10+ years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non- degreed = 6 yrs. of experience)
Job Duties: Researches and analyzes complex, enterprise wide issues surrounding the business processes of an organization. Makes recommendations surrounding improving security
processes, efficiency and practices. Consults at the highest level of agency management and serve as trusted advisors providing the highest level of security process guidance and advice to senior executives in government. Assist overall security strategy development at the agency level.

Configuration Analyst II
Experience: 2 to 4 years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degreed = 6 yrs. of experience)
Job Duties: Analyzes changes of product design to determine the effect on the end product design and function and determines and prepares documentation necessary for change. Coordinates with customers and manufacturers to determine a process for change reporting. Reviews released engineering change data and changes documenting activities to ensure adherence to configuration management procedures and policies. Typically reports to a supervisor. Gaining exposure to some of the complex tasks within the job function. Occasionally directed in several aspects of the work.

Configuration Analyst III
Experience: 4 to 7 years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degreed = 6 yrs. of experience)
Job Duties: Analyzes changes of product design to determine the effect on the end product design and function and determines and prepares documentation necessary for change. Coordinates with customers and manufacturers to determine a process for change reporting. Reviews released engineering change data and changes documenting activities to ensure adherence to configuration management procedures and policies. Typically reports to a supervisor or manager. Contributes to moderately complex aspects of a project. Work is generally independent and collaborative in nature.

Consultant
Experience: 5+ years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degreed = 6 yrs. of experience)
Job Duties: Provides consulting to managers, supervisors and workforce on automated business processes or techniques such as Client Resource Management, Enterprise Resource Planning or Supply Chain Management. Facilitates workshops and analysis sessions. Conducts and assists with benchmarking and surveys. Facilitates process improvement efforts.

Data Security Analyst II
Experience: 2 to 4 years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degreed = 6 yrs. of experience)
Job Duties: Designs, implements, and enforces security policies that protect systems and data from access by unauthorized users. Creates procedures for data access, protection, and backup. Investigates security violations and modifies procedures to prevent future incursions. Reviews changes to information systems to ensure compliance with security standards. Typically reports to a supervisor or manager. Gaining exposure to some of
the complex tasks within the job function. Occasionally directed in several aspects of the work.

Data Security Analyst III
Experience: 4 to 7 years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degreed = 6 yrs. of experience)
Job Duties: Designs, implements, and enforces security policies that protect systems and data from access by unauthorized users. Creates procedures for data access, protection, and backup. Investigates security violations and modifies procedures to prevent future incursions. Reviews changes to information systems to ensure compliance with security standards. Typically reports to a supervisor or manager. Contributes to moderately complex aspects of a project. Work is generally independent and collaborative in nature

Data Security Analyst IV
Experience: 7+ years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degreed = 6 yrs. of experience)
Job Duties: Designs, implements, and enforces security policies that protect systems and data from access by unauthorized users. Creates procedures for data access, protection, and backup. Investigates security violations and modifies procedures to prevent future incursions. Reviews changes to information systems to ensure compliance with security standards. May supervise and guide the work of lower-level data security analysts. Typically reports to a manager or head of a unit/department. A specialist on complex technical and business matters. Work is highly independent. May assume a team lead role for the work group.

Disaster Recovery Analyst
Experience: 2 to 4 years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degreed = 6 yrs. of experience)
Job Duties: Assists in developing, implementing, and maintaining policies, procedures, and programs for ensuring the security and integrity of company data, databases, information systems, and technology. Participates in risk management analysis and assists with the creation of business continuity, contingency, and disaster recovery plans. Develops and executes the testing processes utilized to validate the disaster recovery plans. May implement and administer a database and tools used to track and manage event response and recovery process. Typically reports to a manager. Gaining exposure to some of the complex tasks within the job function. Occasionally directed in several aspects of the work.

Enterprise Infrastructure Architect IV
Experience: 7+ years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degreed = 6 yrs. of experience)
Job Duties: Responsible for designing and implementing information systems that will adequately support the enterprise infrastructure of the organization. Analyzes system requirements and defines system architecture that will meet business needs, including
server infrastructure, capacity planning, storage requirements, and networking protocols. Ensures that architecture project rollouts meet security standards and be effectively integrated with current applications. Typically reports to Manager. A specialist on complex technical and business matters. Work is highly independent. May assume a team lead role for the work group.

**Enterprise Solutions Engineer**

**Experience:** 10+ years of related experience  
**Education:** Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non- degree = 6 yrs. of experience)  
**Job Duties:** Researches and analyzes complex, enterprise wide issues surrounding the technological strategies of an organization. Consults at the highest level of agency management and serves as trusted advisors providing the highest level of technical guidance, strategies, and roadmaps to senior executives in government. Assists overall technological strategy development at the agency level.

**Help Desk Support Assistant**

**Experience:** May require 0-2 year of general work experience  
**Education:** Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non- degree = 6 yrs. of experience)  
**Job Duties:** Provides support to end users for basic computer, application, system, device, access and hardware issues. Identifies, researches and resolves routine technical problems of low complexity. Responds to telephone, email and on-line requests for technical support. Documents, tracks, and monitors the problem using applicable systems and tools. May coordinate with other teams or departments to resolve user problems. May perform password re-sets for users. Typically reports to a supervisor. Possesses a moderate understanding of general aspects of the job. Works under the close direction of senior personnel in the functional area.

**Help Desk Support**

**Experience:** 2-4 years of related experience  
**Education:** Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non- degree = 6 yrs. of experience)  
**Job Duties:** Provides support to end users for computer, application, system, device, access and hardware issues. Identifies, researches and resolves technical problems of moderate complexity. Responds to telephone, email and on-line requests for technical support. Documents, tracks, and monitors the problem using applicable systems and tools. May coordinate with other teams or departments to resolve user problems. Typically reports to a supervisor or manager. Gaining or has attained full proficiency in a specific area of discipline. Works under moderate supervision.

**Information Security Analyst II**

**Experience:** 2 to 4 years of related experience  
**Education:** Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non- degree = 6 yrs. of experience)  
**Job Duties:** Completes tasks designed to ensure security of the organization's systems and information assets. Protects against unauthorized access, modification, or destruction and develops IT security policies and standards. Works with end users to determine
needs of individual departments. Implements policies or procedures and tracks compliance throughout the organization. Typically reports to a manager. Gaining exposure to some of the complex tasks within the job function. Occasionally directed in several aspects of the work.

**Information Security Analyst III**

**Experience:** 4 to 7 years of related experience  
**Education:** Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degreed = 6 yrs. of experience)  
**Job Duties:** Completes tasks designed to ensure security of the organization's systems and information assets. Protects against unauthorized access, modification, or destruction and develops IT security policies and standards. Works with end users to determine needs of individual departments. Understands internet architecture and firewall configuration to protect system security. May need to authorize user access and familiar with domain structures and digital signatures. Typically reports to a manager. Contributes to moderately complex aspects of a project. Work is generally independent and collaborative in nature.

**Information Security Analyst IV**

**Experience:** 7+ years of related experience  
**Education:** Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degreed = 6 yrs. of experience)  
**Job Duties:** Designs and implements information security standards for applications and databases. Collaborates with a team of information security analysts to provide subject matter expertise on application development, database design, and network maintenance. Researches and advocates the latest technologies and solutions to support the security requirements of internal and external customers. Assesses client needs against security concerns and resolves information security risk issues. Trains security awareness to business partners and IT staff. Typically reports to a manager. A specialist on complex technical and business matters. Work is highly independent. May assume a team lead role for the work group.

**Information Security Analyst V**

**Experience:** 10+ years of related experience  
**Education:** Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degreed = 6 yrs. of experience)  
**Job Duties:** Identifies potential information and network or internet security vulnerabilities. Designs and implements information security standards for applications and databases. Conducts analysis, investigates and recommends security technologies. Ensures site security and provides consultation on security issues staying abreast of current malware and other potential internet security threats. Typically reports to a manager. Works on advanced, complex technical projects or business issues requiring state of the art technical or industry knowledge. Works autonomously. Goals are generally communicated in solution or project goal terms.

**IT Project Manager III**

**Experience:** 4 to 7 years of related experience
**IT Project Manager IV**

**Experience:** 7+ years of related experience

**Education:** Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degree = 6 yrs. of experience)

**Job Duties:** Provides technical/management leadership on major tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Decision making and domain knowledge may have a critical impact on overall project implementation. Leads team on large projects or significant segment of large complex projects. Analyzes new and complex project related problems and creates innovative solutions involving finance, scheduling, technology, methodology, tools, and solution components. Provides applications systems analysis and programming activities for a Government site, facility or multiple locations. Prepares long and short-range plans for application selection, systems development, systems maintenance, and production activities and for necessary support resources. Oversees all aspects of projects.

**Network Administrator I**

**Experience:** 0-2 years of related experience

**Education:** Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degree = 6 yrs. of experience)

**Job Duties:** Assists with the daily administration of a network/server environment. Monitors network performance and performs testing to provide diagnosis of issues and to assist with deployment of solutions. Performs routine updates and maintenance tasks. May be responsible for tracking the parts inventory and maintenance of documentation. Emphasis is on learning the key aspects of the job to be performed and supporting more senior administrators. Typically reports to supervisor or manager. May require Network Administrator certification. Works on projects/matters of limited complexity in a support role. Work is closely managed.

**Network Administrator III**

**Experience:** 4 to 7 years of related experience

**Education:** Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degree = 6 yrs. of experience)

**Job Duties:** Responsible for daily administration of a network/server environment. Installs, configures, and maintains system software. Monitors network performance troubleshoots issues and deploys solutions. Plans and implements upgrades, patches, and installation of new applications and equipment. Creates and maintains a disaster recovery, security and backup and restore plan. May assist with evaluating new
networks to optimize network efficiency and performance. Typically reports to
manager or head of a unit/department. May require Network Administrator
certification. Contributes to moderately complex aspects of a project. Work is generally
independent and collaborative in nature.

**Network Administrator IV**

**Experience:** 7+ years of related experience
**Education:** Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 
1 yr. of College (non-degreed = 6 yrs. of experience)
**Job Duties:** Responsible for daily administration of a network/server environment. Installs,
configures and maintains system software. Monitors network performance
troubleshoots more complex issues and deploys solutions. Plans and implements
upgrades, patches, and installation of new applications and equipment. Creates and
maintains a disaster recovery, security and backup and restore plan and policy. May
conduct evaluation of new technologies to optimize network efficiency and
performance. Typically reports to manager or head of a unit/department. May require
Network Administration certification. A specialist on complex technical and business
matters. Work is highly independent. May assume a team lead role for the work group.

**Program Manager III**

**Experience:** 10+ years of related experience
**Education:** Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 
1 yr. of College (non-degreed = 6 yrs. of experience)
**Job Duties:** Provides management and technical direction to project managers or other program or
project personnel. Exercises independent judgment and a high level of analytical skills in
solving technical, administrative and managerial problems. Accountable for project
planning, execution and performance.

**Software Engineer V**

**Experience:** 10+ years of related experience
**Education:** Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 
1 yr. of College (non-degreed = 6 yrs. of experience)
**Job Duties:** Designs and develops software applications. Performs coding, debugging, testing and
troubleshooting throughout the application development process. May provide
consultation on complex projects. Typically reports to a manager. Works on advanced,
complex technical projects or business issues requiring state of the art technical or
industry knowledge. Works autonomously. Goals are generally communicated in
solution or project goal terms. May provide a leadership role for the work group
through knowledge in the area of specialization.

**Subject Matter Expert I**

**Experience:** 2 to 4 years of related experience
**Education:** Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 
1 yr. of College (non-degreed = 6 yrs. of experience)
**Job Duties:** Possesses and applies expertise on multiple complex work assignments. Assignments
may be broad in nature, requiring originality and innovation in determining how to
accomplish tasks. Operates with appreciable latitude in developing methodology and
presenting solutions to problems. Contributes to deliverables and performance metrics
where applicable. Serves as subject matter expert, possessing in-depth knowledge of a particular area, such as business, computer science, engineering, mathematics, or the various sciences. Provides technical knowledge and analysis of highly specialized applications and operational environments, high-level functional systems analysis, design, integration, documentation and implementation advice on exceptionally complex problems that need extensive knowledge of the subject matter for effective implementation. Participates as needed in all phases of software development with emphasis on the planning, analysis, testing, integration, documentation, and presentation phases. Applies principles, methods and knowledge of the functional area of capability to specific task order requirements, advanced mathematical principles and methods to exceptionally difficult and narrowly defined technical problems in engineering and other scientific applications to arrive at automated solutions.

Subject Matter Expert III
Experience: 7+ years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degreed = 6 yrs. of experience)
Job Duties: Possesses and applies a comprehensive knowledge across key tasks and high impact assignments. Functions as a technical expert across multiple project assignments. Serves as subject matter expert, possessing in-depth knowledge of a particular area, such as business, computer science, engineering, mathematics, or the various sciences. Provides technical knowledge and analysis of highly specialized applications and operational environments, high-level functional systems analysis, design, integration, documentation and implementation advice on exceptionally complex problems that need extensive knowledge of the subject matter for effective implementation. Participates as needed in all phases of software development with emphasis on the planning, analysis, testing, integration, documentation, and presentation phases. Applies principles, methods and knowledge of the functional area of capability to specific task order requirements, advanced mathematical principles and methods to exceptionally difficult and narrowly defined technical problems in engineering and other scientific applications to arrive at automated solutions.

Subject Matter Expert IV
Experience: 10+ years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degreed = 6 yrs. of experience)
Job Duties: Provides technical/management leadership on major tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Decision making and domain knowledge may have a critical impact on overall project implementation. Serves as subject matter expert, possessing in-depth knowledge of a particular area, such as business, computer science, engineering, mathematics, or the various sciences. Provides technical knowledge and analysis of highly specialized applications and operational environments, high-level functional systems analysis, design, integration, documentation and implementation advice on exceptionally complex problems that need extensive knowledge of the subject matter for effective implementation. Participates as needed in all phases of software development with emphasis on the planning, analysis, testing, integration, documentation, and presentation phases. Applies principles, methods and knowledge...
of the functional area of capability to specific task order requirements, advanced mathematical principles and methods to exceptionally difficult and narrowly defined technical problems in engineering and other scientific applications to arrive at automated solutions.

**Systems Administrator II**

**Experience:** 2 to 4 years of related experience

**Education:** Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degreed = 6 yrs. of experience)

**Job Duties:** Maintains and supports the integrity of the operating system environment and various computer systems. Administers, installs and troubleshoots a variety of operating systems. Performs systems maintenance tasks, such as system back-up, recovery and file maintenance. Schedules, installs, and tests system software upgrades. Configures software and resolves technical problems. Monitors and maintains software licensing and maintenance agreements. Typically reports to a project leader or manager. Gaining exposure to some of the complex tasks within the job function. Occasionally directed in several aspects of the work.

**Systems Engineer II**

**Experience:** 2 to 4 years of related experience

**Education:** Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degreed = 6 yrs. of experience)

**Job Duties:** Designs, develops, supports, and maintains the organization's systems infrastructure, including the implementation and design of hardware and software. Reviews previous documents and prepares up-to-date documents/modes/reports to meet consumer requests. Performs end-user support. Typically reports to a manager. Gaining exposure to some of the complex tasks within the job function. Occasionally directed in several aspects of the work.

**Systems Engineer III**

**Experience:** 4 to 7 years of related experience

**Education:** Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degreed = 6 yrs. of experience)

**Job Duties:** Designs, develops, supports, and maintains the organization's systems infrastructure, including the implementation and design of hardware and software. Analyzes, develops, modifies, tests and maintains the system. Reviews previous documents and prepares up-to-date documents/modes/reports to meet consumer requests. Typically reports to a manager. Contributes to moderately complex aspects of a project. Work is generally independent and collaborative in nature.

**Systems Engineer IV**

**Experience:** 7+ years of related experience

**Education:** Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degreed = 6 yrs. of experience)

**Job Duties:** Plans and designs an organization's systems infrastructure, including the implementation and design of hardware and software. Analyzes, develops, modifies, tests and maintains the system. Verifies and validates systems and meets internal and external requirements. Diagnoses problems and provides recommendations for
improvement on existing and new systems. Typically reports to a manager. A specialist on complex technical and business matters. Work is highly independent. May assume a team lead role for the work group.

**54151HACS Labor Category Descriptions**

**Cybersecurity Applications Analyst II**  
Experience: 2 to 4 years of related experience  
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degree = 6 yrs. of experience)  
Job Duties: Researches, analyzes, and modifies programming systems including encoding, testing, debugging, and installing to support an organization's application systems with an emphasis on risk and vulnerability as well as compliance. Consults with users to identify current operating procedures and to clarify program objectives. Writes manuals for users to describe installation and operating procedures. May write documentation to describe program development, logic, coding, and corrections. Typically reports to a project leader or manager. Gaining exposure to some of the complex tasks within the job function. Occasionally directed in several aspects of the work. Specialized tasks may include but are not limited to ethical hacking, penetration testing or risk and vulnerability assessment (RVA), whether related to potential or actual threats, attacks, incidents, forensics, intrusions, and/or responses/remediations.

**Cybersecurity Applications Analyst III**  
Experience: 4 to 7 years of related experience  
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degree = 6 yrs. of experience)  
Job Duties: Researches, analyzes, and modifies programming systems including encoding, testing, debugging, and installing to support an organization's application systems with an emphasis on risk and vulnerability as well as compliance. Consults with users to identify current operating procedures and to clarify program objectives. Writes manuals for users to describe installation and operating procedures. May write documentation to describe program development, logic, coding, and corrections. Typically reports to a project leader or manager. Contributes to moderately complex aspects of a project. Work is generally independent and collaborative in nature. Specialized tasks may include but are not limited to ethical hacking, penetration testing or risk and vulnerability assessment (RVA), whether related to potential or actual threats, attacks, incidents, forensics, intrusions, and/or responses/remediations.

**Cybersecurity Process Consultant**  
Experience: 10+ years of related experience  
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degree = 6 yrs. of experience)  
Job Duties: Researches and analyzes basic and complex issues surrounding the business processes of an organization. Makes recommendations surrounding improving processes, efficiency and practices. Simulates and tests process improvements. Communicates changes and may provide training to impacted business units. Typically reports to top management. Works on advanced, complex technical projects or business issues requiring state of the art technical or industry knowledge. Works autonomously. Goals
are generally communicated in solution” or project goal terms. Specialized tasks may include but are not limited to ethical hacking, penetration testing or risk and vulnerability assessment (RVA), whether related potential or actual threats, attacks, incidents, forensics, intrusions, and/or responses/remediations.

**Cybersecurity Solutions Architect**

**Experience:** 10+ years of related experience

**Education:** Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degreed = 6 yrs. of experience)

**Job Duties:** Researches and analyzes complex, enterprise wide issues surrounding the business processes of an organization. Makes recommendations surrounding improving security processes, efficiency and practices. Consults at the highest level of agency management and serve as trusted advisors providing the highest level of security process guidance and advice to senior executives in government. Assist overall security strategy development at the agency level.

**Cybersecurity Configuration Analyst II**

**Experience:** 2 to 4 years of related experience

**Education:** Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degreed = 6 yrs. of experience)

**Job Duties:** Analyzes changes of product design to determine the effect on the end product design and function and determines and prepares documentation necessary for change. Coordinates with customers and manufacturers to determine a process for change reporting. Reviews released engineering change data and changes documenting activities to ensure adherence to configuration management procedures and policies. Typically reports to a supervisor. Gaining exposure to some of the complex tasks within the job function. Occasionally directed in several aspects of the work. Specialized tasks may include but are not limited to ethical hacking, penetration testing or risk and vulnerability assessment (RVA), whether related to potential or actual threats, attacks, incidents, forensics, intrusions, and/or responses/remediations.

**Cybersecurity Configuration Analyst III**

**Experience:** 4 to 7 years of related experience

**Education:** Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degreed = 6 yrs. of experience)

**Job Duties:** Analyzes changes of product design to determine the effect on the end product design and function and determines and prepares documentation necessary for change. Coordinates with customers and manufacturers to determine a process for change reporting. Reviews released engineering change data and changes documenting activities to ensure adherence to configuration management procedures and policies. Typically reports to a supervisor or manager. Contributes to moderately complex aspects of a project. Work is generally independent and collaborative in nature. Specialized tasks may include but are not limited to ethical hacking, penetration testing or risk and vulnerability assessment (RVA), whether related to potential or actual threats, attacks, incidents, forensics, intrusions, and/or responses/remediations.

**Cybersecurity Consultant**

**Experience:** 5+ years of related experience

---

[www.gcyber.com](http://www.gcyber.com)  
C-11  
[sales@gcyber.com](mailto:sales@gcyber.com)
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non- degreed = 6 yrs. of experience)

Job Duties: Provides consulting to managers, supervisors and workforce on automated business processes or techniques such as Client Resource Management, Enterprise Resource Planning or Supply Chain Management. Facilitates workshops and analysis sessions. Conducts and assists with benchmarking and surveys. Facilitates process improvement efforts.

**Data Security Analyst II**

Experience: 2 to 4 years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non- degreed = 6 yrs. of experience)

Job Duties: Designs, implements, and enforces security policies that protect systems and data from access by unauthorized users with a focus on Risk and Vulnerability Analyst, Vulnerability Manager, Ethical Hacker, Computer Network Defense (CND) Auditor, Compliance Manager, and Information Security Engineer. Creates procedures for data access, protection, and backup. Investigates security violations and modifies procedures to prevent future incursions and ensures whether related to potential or actual threats, attacks, incidents, forensics, intrusions, and/or responses/remediations. Reviews changes to information systems to ensure compliance with security standards. Typically reports to a supervisor or manager. Gaining exposure to some of the complex tasks within the job function. Occasionally directed in several aspects of the work.

**Data Security Analyst III**

Experience: 4 to 7 years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non- degreed = 6 yrs. of experience)

Job Duties: Designs, implements, and enforces security policies that protect systems and data from access by unauthorized users with a focus on Risk/Vulnerability Analyst, Vulnerability Manager, Ethical Hacker, Computer Network Defense (CND) Auditor, Compliance Manager, and Information Security Engineer. Creates procedures for data access, protection, and backup. Investigates security violations and modifies procedures to prevent future incursions. Reviews changes to information systems to ensure compliance with security standards. Typically reports to a supervisor or manager. Contributes to moderately complex aspects of a project. Work is generally independent and collaborative in nature but also continuous regarding whether related to potential or actual threats, attacks, incidents, forensics, intrusions, and/or responses/remediations.

**Data Security Analyst IV**

Experience: 7+ years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non- degreed = 6 yrs. of experience)

Job Duties: Designs, implements, and enforces security policies that protect systems and data from access by unauthorized users with a focus on Risk/Vulnerability Analyst, Vulnerability Manager, Ethical Hacker, Computer Network Defense (CND) Auditor, Compliance Manager, and Information Security Engineer. Creates procedures for data access, protection, and backup. Investigates security violations and modifies procedures to
prevent future incursions. Reviews changes to information systems to ensure compliance with security standards. May supervise and guide the work of lower-level data security analysts. Typically reports to a manager or head of a unit/department. A specialist on complex technical and business matters. Work is highly independent. May assume a team lead role for the work group constantly analyzing data of whether there are related to potential or actual threats, attacks, incidents, forensics, intrusions, and/or responses/remediations.

Disaster Recovery Analyst
Experience: 2 to 4 years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non- degree = 6 yrs. of experience)
Job Duties: Helps organizations impacted by a Cybersecurity compromise i.e. potential or actual threats, attacks, incidents, forensics, intrusions, and/or responses/remediations. The individual also determines the extent of the incident, remove the adversary from their systems, and restore their networks to a more secure state. Assists in developing, implementing, and maintaining policies, procedures, and programs for ensuring the security and integrity of company data, databases, information systems, and technology. Participates in risk management analysis and assists with the creation of business continuity, contingency, and disaster recovery plans. Develops and executes the testing processes utilized to validate the disaster recovery plans. May implement and administer a database and tools used to track and manage event response and recovery process. Typically reports to a manager. Gaining exposure to some of the complex tasks within the job function. Occasionally directed in several aspects of the work.

Enterprise Security Architect IV
Experience: 7+ years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non- degree = 6 yrs. of experience)
Job Duties: Responsible for designing and implementing information systems that will adequately support the enterprise infrastructure of the organization with an emphasis on the cybersecurity posture such as potential or actual threats, attacks, incidents, forensics, intrusions, and/or responses/remediations. Analyzes system requirements and defines system architecture that will meet business needs, including server infrastructure, capacity planning, storage requirements, and networking protocols. Ensures that architecture project rollouts meet security standards and be effectively integrated with current applications. Typically reports to Manager. A specialist on complex technical and business matters. Work is highly independent. May assume a team lead role for the work group.

Cybersecurity Enterprise Solutions Engineer
Experience: 10+ years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non- degree = 6 yrs. of experience)
Job Duties: Researches and analyzes complex, enterprise wide issues surrounding the security related strategies of an organization. Consults at the highest level of agency

www.gcyber.com  C-13  sales@gcyber.com
management and serves as trusted advisors providing the highest level of technical
guidance as it relates to security strategies, and roadmaps to senior executives in
government. Assists overall technological strategy development and implementation at
the agency level.

Information Security Analyst II
Experience:  2 to 4 years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience =
           1 yr. of College (non- degree = 6 yrs. of experience)
Job Duties: Completes tasks designed to ensure security of the organization’s systems and
           information assets with an emphasis on risk/vulnerability analysis and compliance to
           prevent potential threats, attacks, incidents, forensics, intrusions, and/or
           responses/remediations. Protects against unauthorized access, modification, or
           destruction and develops IT security policies and standards. Works with end users to
determine needs of individual departments. Implements policies or procedures and
tracks compliance throughout the organization. Typically reports to a manager. Gaining
exposure to some of the complex tasks within the job function. Occasionally directed in
several aspects of the work.

Information Security Analyst III
Experience:  4 to 7 years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience =
           1 yr. of College (non- degree = 6 yrs. of experience)
Job Duties: Completes tasks designed to ensure security of the organization’s systems and
           information assets with an emphasis on risk/vulnerability analysis and compliance to
           prevent potential threats, attacks, incidents, forensics, intrusions, and/or
           responses/remediations. Protects against unauthorized access, modification, or
           destruction and develops IT security policies and standards. Works with end users to
determine needs of individual departments. Understands internet architecture and
firewall configuration to protect system security. May need to authorize user access
and familiar with domain structures and digital signatures. Typically reports to a
manager. Contributes to moderately complex aspects of a project. Work is generally
independent and collaborative in nature.

Information Security Analyst IV
Experience:  7+ years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience =
           1 yr. of College (non- degree = 6 yrs. of experience)
Job Duties: Designs and implements information security standards for applications and databases.
           Collaborates with a team of information security analysts to provide subject matter
           expertise on application development, database design, and network maintenance; with
           an emphasis on risk/vulnerability analysis and compliance to prevent potential threats,
           attacks, incidents, forensics, intrusions, and/or responses/remediations. Researches and
           advocates the latest technologies and solutions to support the security requirements of
           internal and external customers. Assesses client needs against security concerns and
           resolves information security risk issues. Trains security awareness to business partners
           and IT staff. Typically reports to a manager. A specialist on complex
technical and business matters. Work is highly independent. May assume a team lead role for the work group.

Information Security Analyst V
Experience: 10+ years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degreeted = 6 yrs. of experience)
Job Duties: Identifies potential information and network or internet security vulnerabilities. Designs and implements information security standards for applications and databases with an emphasis on risk/vulnerability analysis and compliance to prevent potential threats, attacks, incidents, forensics, intrusions, and/or responses/remediations. Conducts analysis, investigates and recommends security technologies. Ensures site security and provides consultation on security issues staying abreast of current malware and other potential internet security threats. Typically reports to a manager. Works on advanced, complex technical projects or business issues requiring state of the art technical or industry knowledge. Works autonomously. Goals are generally communicated in solution or project goal terms.

Cybersecurity IT Project Manager III
Experience: 4 to 7 years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degreeted = 6 yrs. of experience)
Job Duties: Manages and oversees all aspects of a technology project to ensure it is completed on-time and within budget. Has overall responsibility for managing scope, cost, schedule, internal staffing and outside vendors, and contractual deliverable. Prepares reports for upper management regarding status of project including but not limited to preventing potential threats, attacks, incidents, forensics, intrusions, and/or responses/remediations. Possesses strong knowledge of technology. Typically reports to a manager. A specialist on complex technical and business matters. Work is highly independent. May assume a team lead role for the work group.

Cybersecurity IT Project Manager IV
Experience: 7+ years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degreeted = 6 yrs. of experience)
Job Duties: Provides technical/management leadership on major tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Decision making and domain knowledge may have a critical impact on overall project implementation. Leads team on large projects or significant segment of large complex projects but also emphasizes on preventing potential threats, attacks, incidents, forensics, intrusions, and/or responses/remediations. Analyzes new and complex project related problems and creates innovative solutions involving finance, scheduling, technology, methodology, tools, and solution components. Provides applications systems analysis and programming activities for a Government site, facility or multiple locations. Prepares long and short-range plans for application selection, systems development, systems maintenance, and production activities and for necessary support resources. Oversees all aspects of projects.
Cybersecurity Network Administrator I
Experience: 0-2 years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non- degreed = 6 yrs. of experience)
Job Duties: Assists with the daily administration of a network/server environment with an emphasis on network security and compliance including but not limited to detecting potential threats, attacks, incidents, forensics, intrusions, and/or responses/remediations within the network. Monitors network performance and performs testing to provide diagnosis of issues and to assist with deployment of solutions. Performs routine updates and maintenance tasks. May be responsible for tracking the parts inventory and maintenance of documentation. Emphasis is on learning the key aspects of the job to be performed and supporting more senior administrators. Typically reports to supervisor or manager. May require Network Administrator certification. Works on projects/matters of limited complexity in a support role. Work is closely managed.

Cybersecurity Network Administrator III
Experience: 4 to 7 years of related experience
Education: Bachelor’s in engineering, Computer Science or another related field. 1.5 yrs. experience = 1 yr. of College (non- degreed = 6 yrs. of experience)
Job Duties: Responsible for daily administration of a network/server environment with an emphasis on network security and compliance. Installs, configures, and maintains system software. Monitors network performance troubleshoots issues and deploys solutions including but not limited to detecting potential threats, attacks, incidents, forensics, intrusions, and/or responses/remediations within the network. Plans and implements upgrades, patches, and installation of new applications and equipment. Creates and maintains a disaster recovery, security and backup and restore plan. May assist with evaluating new technologies to optimize network efficiency and performance. Typically reports to manager or head of a unit/department. May require Network Administrator certification. Contributes to moderately complex aspects of a project. Work is generally independent and collaborative in nature.

Cybersecurity Network Administrator IV
Experience: 7+ years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non- degreed = 6 yrs. of experience)
Job Duties: Responsible for daily administration of a network/server environment with an emphasis on network security and compliance. Installs, configures and maintains system software. Monitors network performance troubleshoots more complex issues and deploys solutions including but not limited to detecting potential threats, attacks, incidents, forensics, intrusions, and/or responses/remediations within the network. Plans and implements upgrades, patches, and installation of new applications and equipment. Creates and maintains a disaster recovery, security and backup and restore plan and policy. May conduct evaluation of new technologies to optimize network efficiency and performance. Typically reports to manager or head of a unit/department. May require Network Administration certification. A specialist on complex technical and business matters. Work is highly independent. May assume a team lead role for the work group.

www.gcyber.com
C-16
sales@gcyber.com
Cybersecurity Program Manager III
Experience: 10+ years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience =
1 yr. of College (non- degree = 6 yrs. of experience)
Job Duties: Provides management and technical direction to project managers or other program or project personnel. Exercises independent judgment and a high level of analytical skills in solving technical, administrative and managerial problems solutions including but not limited to detecting potential threats, attacks, incidents, forensics, intrusions, and/or responses/remediations within the program. Accountable for project planning, execution and performance.

Cybersecurity Software Engineer V
Experience: 10+ years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience =
1 yr. of College (non- degree = 6 yrs. of experience)
Job Duties: Designs and develops software applications. Performs coding, debugging, testing and troubleshooting throughout the application development process with an emphasis on cybersecurity solutions including but not limited to detecting potential threats, attacks, incidents, forensics, intrusions, and/or responses/remediations within the software. May provide consultation on complex projects. Typically reports to a manager. Works on advanced, complex technical projects or business issues requiring state of the art technical or industry knowledge. Works autonomously. Goals are generally communicated in solution or project goal terms. May provide a leadership role for the work group through knowledge in the area of specialization.

Cybersecurity Subject Matter Expert I
Experience: 2 to 4 years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience =
1 yr. of College (non- degree = 6 yrs. of experience)
Job Duties: Possesses and applies expertise on multiple complex work assignments. Assignments may be broad in nature, requiring originality and innovation in determining how to accomplish tasks while focusing on cybersecurity and compliance. Operates with appreciable latitude in developing methodology and presenting solutions to problems. Contributes to deliverables and performance metrics where applicable. Serves as subject matter expert, possessing in-depth knowledge of a particular area, such as business, computer science, engineering, mathematics, or the various sciences. Provides technical knowledge and analysis of highly specialized applications and operational environments, high-level functional systems analysis, design, integration, documentation and implementation advice on exceptionally complex problems that need extensive knowledge of the subject matter for effective implementation including but not limited to detecting potential threats, attacks, incidents, forensics, intrusions, and/or responses/remediations within the subject matter. Participates as needed in all phases of software development with emphasis on the planning, analysis, testing, integration, documentation, and presentation phases. Applies principles, methods and knowledge of the functional area of capability to specific task order requirements, advanced mathematical principles and methods to exceptionally difficult and narrowly defined technical problems in engineering and other scientific applications to arrive at automated solutions.
Cybersecurity Subject Matter Expert III
Experience: 7+ years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non- degree = 6 yrs. of experience)
Job Duties: Possesses and applies a comprehensive knowledge across key tasks and high impact assignments. Functions as a technical expert across multiple project assignments. Serves as subject matter expert, possessing in-depth knowledge of a particular area, such as business, computer science, engineering, mathematics, or the various sciences. Provides technical knowledge and analysis of highly specialized applications and operational environments, high-level functional systems analysis, design, integration, documentation and implementation advice on exceptionally complex problems that need extensive knowledge of the subject matter for effective implementation including but not limited to detecting potential threats, attacks, incidents, forensics, intrusions, and/or responses/remediations within the subject matter. Participates as needed in all phases of software development with emphasis on the planning, analysis, testing, integration, documentation, and presentation phases. Applies principles, methods and knowledge of the functional area of capability to specific task order requirements, advanced mathematical principles and methods to exceptionally difficult and narrowly defined technical problems in engineering and other scientific applications to arrive at automated solutions.

Cybersecurity Subject Matter Expert IV
Experience: 10+ years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non- degree = 6 yrs. of experience)
Job Duties: Provides technical/management leadership on major tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Decision making and domain knowledge may have a critical impact on overall project implementation. Serves as subject matter expert, possessing in-depth knowledge of a particular area, such as business, computer science, engineering, mathematics, or the various sciences. Provides technical knowledge and analysis of highly specialized applications and operational environments, high-level functional systems analysis, design, integration, documentation and implementation advice on exceptionally complex problems that need extensive knowledge of the subject matter for effective implementation including but not limited to detecting potential threats, attacks, incidents, forensics, intrusions, and/or responses/remediations within the subject matter. Participates as needed in all phases of software development with emphasis on the planning, analysis, testing, integration, documentation, and presentation phases. Applies principles, methods and knowledge of the functional area of capability to specific task order requirements, advanced mathematical principles and methods to exceptionally difficult and narrowly defined technical problems in engineering and other scientific applications to arrive at automated solutions.

Cybersecurity Systems Administrator II
Experience: 2 to 4 years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non- degree = 6 yrs. of experience)
Job Duties: Maintains and supports the integrity of the operating system environment and various computer systems with an emphasis on cybersecurity and compliance. Administers, installs and troubleshoots a variety of operating systems. Performs systems maintenance tasks, such as system back-up, recovery and file maintenance including but not limited to detecting potential threats, attacks, incidents, forensics, intrusions, and/or responses/remediations within the system. Schedules, installs, and tests system software upgrades. Configures software and resolves technical problems. Monitors and maintains software licensing and maintenance agreements. Typically reports to a project leader or manager. Gaining exposure to some of the complex tasks within the job function. Occasionally directed in several aspects of the work.

Cybersecurity Systems Engineer II
Experience: 2 to 4 years of related experience
Education: Bachelor’s in engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degreed = 6 yrs. of experience)
Job Duties: Designs, develops, supports, and maintains the organization's systems infrastructure, including the implementation and design of hardware and software with an emphasis on cyber security, risk/vulnerability analysis and compliance to prevent potential threats, attacks, incidents, forensics, intrusions, and/or responses/remediations within the system. Reviews previous documents and prepares up-to-date documents/modes/reports to meet consumer requests. Performs end-user support. Typically reports to a project leader or manager. Gaining exposure to some of the complex tasks within the job function. Occasionally directed in several aspects of the work.

Cybersecurity Systems Engineer III
Experience: 4 to 7 years of related experience
Education: Bachelors in Engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degreed = 6 yrs. of experience)
Job Duties: Designs, develops, supports, and maintains the organization's systems infrastructure, including the implementation and design of hardware and software with an emphasis on cybersecurity, risk/vulnerability analysis and compliance to prevent potential threats, attacks, incidents, forensics, intrusions, and/or responses/remediations within the system. Analyzes, develops, modifies, tests and maintains the system. Reviews previous documents and prepares up-to-date documents/modes/reports to meet consumer requests. Typically reports to a manager. Contributes to moderately complex aspects of a project. Work is generally independent and collaborative in nature.

Cybersecurity Systems Engineer IV
Experience: 7+ years of related experience
Education: Bachelors in Engineering, Computer Science or other related field. 1.5 yrs. experience = 1 yr. of College (non-degreed = 6 yrs. of experience)
Job Duties: Plans and designs an organization's systems infrastructure, including the implementation and design of hardware and software with an emphasis on cybersecurity, risk/vulnerability analysis and compliance to prevent potential threats, attacks, incidents, forensics, intrusions, and/or responses/remediations within the system. Analyzes, develops, modifies, tests and maintains the system. Verifies and validates systems and meets internal and external requirements. Diagnoses problems and provides recommendations for improvement on existing and new systems. Typically reports to a manager. A specialist on complex technical and business matters. Work is highly independent. May assume a team lead role for the work group.