GENERAL SERVICES ADMINISTRATION
Federal Supply Service
Authorized Federal Supply Schedule Price List

Multiple Award Schedule
Information Technology Category

Contract Number: GS-35F-0456V
Contract Period: May 18, 2019 – May 17, 2024
Pricelist Effective: August 20, 2020    Mod: A824

Contract Admin: Abhai Johri
Email: gsastar2@e2zintegral.com
Tel: 240-907-2570
Fax: 301-294-4673
Website: http://www.e2zintegral.com/

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

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

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

<table>
<thead>
<tr>
<th>SIN</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S</td>
<td>Information Technology Professional Services</td>
</tr>
<tr>
<td>541611</td>
<td>Management and Financial Consulting, Acquisition and Grants Management Support, and Business Program and Project Management Services</td>
</tr>
<tr>
<td>541990L</td>
<td>Professional Law Enforcement Services</td>
</tr>
<tr>
<td>OLM</td>
<td>Order Level Materials</td>
</tr>
</tbody>
</table>

1b. Identification of the lowest priced model number and lowest unit price for that model for each special item number awarded in the contract. **Not Applicable to services**

1c. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles, experience, functional responsibility and education for those types of employees or subcontractors who will perform services shall be provided.

Please see...

2. Maximum order.

<table>
<thead>
<tr>
<th>SIN</th>
<th>Maximum Order Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S</td>
<td>$500,000</td>
</tr>
<tr>
<td>541611</td>
<td>$1,000,000</td>
</tr>
<tr>
<td>541990L</td>
<td>$250,000</td>
</tr>
</tbody>
</table>

3. Minimum order **$100.00**

4. Geographic coverage (delivery area). **Domestic (CONUS only)**

5. Point(s) of production. **USA**

6. Discount from list prices or statement of net price. **5-37.6%, Prices shown herein are net (discount deducted)**

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**

9a. Notification that Government purchase cards are accepted at or below the micro- purchase threshold. **YES, Government Purchase Cards are accepted below the micro-purchase threshold.**

9b. Notification whether Government purchase cards are accepted or not accepted above the micro-
purchase threshold. **YES, Government Purchase Cards are accepted above the micro-purchase threshold.**

10. Foreign items. **None**

11a. Time of delivery. **Determined at task order days**

11b. Expedited Delivery. **Contact Contractor**

11c. Overnight and 2-day delivery. **Contact Contractor**

11d. Urgent Requirements. **Contact Contractor.**

12. F.O.B. point(s). **FOB Destination**

13a. Ordering address(es). **Same as contractor’s address.**

13b. Ordering procedures: For supplies and services, the ordering procedures, information on Blanket Purchase Agreements (BPA’s) are found in Federal Acquisition Regulation (FAR) 8.405-3.

14. Payment address(es) **Same as contractor’s address.**

15. Warranty provision. **Standard Commercial Warranty.**

16. Export packing charges, if applicable. **N/A**

17. Terms and conditions of Government purchase card acceptance (any thresholds above the micro-purchase level). **YES, Government Purchase Cards are accepted above the micro-purchase threshold.**

18. Terms and conditions of rental, maintenance, and repair (if applicable). **N/A**

19. Terms and conditions of installation (if applicable). **N/A**

20. Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices (if applicable). See Warranty for Repair Parts, If Applicable. **N/A**

20a. Terms and conditions for any other services (if applicable) **N/A**

21. List of service and distribution points (if applicable). **N/A**

22. List of participating dealers (if applicable). **N/A**

23. Preventive maintenance (if applicable). **N/A**

24a. Special attributes such as environmental attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants). **None**

24b. If applicable, indicate that Section 508 compliance information is available on Electronic and Information Technology (EIT) supplies and services and show where full details can be found. The EIT standards can be found at: [https://www.section508.gov/](https://www.section508.gov/) **N/A**

25. Data Universal Number System (DUNS) number. **018193669**

Contractor is Active in SAM  
Exp Date: 06/13/2021

**GSA Pricelist**

Prices shown include Industrial Funding Fee (IFF)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S</td>
<td>Administrative Specialists II</td>
<td>Associates</td>
<td>2</td>
<td>$42.00</td>
<td>$43.05</td>
<td>$44.13</td>
<td>$45.23</td>
<td>$46.36</td>
<td>$42.00</td>
</tr>
<tr>
<td>54151S</td>
<td>Application Developer II</td>
<td>Associates</td>
<td>2</td>
<td>$51.82</td>
<td>$53.11</td>
<td>$54.44</td>
<td>$55.80</td>
<td>$57.20</td>
<td>$51.82</td>
</tr>
<tr>
<td>54151S</td>
<td>Application Developer III</td>
<td>Bachelor's</td>
<td>5</td>
<td>$62.45</td>
<td>$64.02</td>
<td>$65.62</td>
<td>$67.26</td>
<td>$68.94</td>
<td>$62.45</td>
</tr>
<tr>
<td>54151S</td>
<td>Application Developer IV</td>
<td>Masters</td>
<td>6</td>
<td>$84.40</td>
<td>$86.51</td>
<td>$88.67</td>
<td>$90.89</td>
<td>$93.16</td>
<td>$84.40</td>
</tr>
<tr>
<td>54151S</td>
<td>Applications Engineer II</td>
<td>Associates</td>
<td>2</td>
<td>$63.39</td>
<td>$64.97</td>
<td>$66.59</td>
<td>$68.26</td>
<td>$69.97</td>
<td>$63.39</td>
</tr>
<tr>
<td>54151S</td>
<td>Applications Engineer III</td>
<td>Associates</td>
<td>2</td>
<td>$63.16</td>
<td>$64.74</td>
<td>$66.36</td>
<td>$68.02</td>
<td>$69.72</td>
<td>$63.16</td>
</tr>
<tr>
<td>54151S</td>
<td>Applications Engineer IV</td>
<td>Masters</td>
<td>6</td>
<td>$75.66</td>
<td>$77.56</td>
<td>$79.49</td>
<td>$81.48</td>
<td>$83.52</td>
<td>$75.66</td>
</tr>
<tr>
<td>54151S</td>
<td>Architecture Specialist III</td>
<td>Bachelor's</td>
<td>5</td>
<td>$97.73</td>
<td>$100.17</td>
<td>$102.67</td>
<td>$105.24</td>
<td>$107.87</td>
<td>$97.73</td>
</tr>
<tr>
<td>54151S</td>
<td>Architecture Specialist IV</td>
<td>Masters</td>
<td>6</td>
<td>$101.55</td>
<td>$104.09</td>
<td>$106.69</td>
<td>$109.36</td>
<td>$112.09</td>
<td>$101.55</td>
</tr>
<tr>
<td>54151S</td>
<td>Business Process Engineering Specialist III</td>
<td>Bachelor's</td>
<td>5</td>
<td>$102.58</td>
<td>$105.14</td>
<td>$107.77</td>
<td>$110.46</td>
<td>$113.22</td>
<td>$102.58</td>
</tr>
<tr>
<td>54151S</td>
<td>Business Process Engineering Specialist IV</td>
<td>Masters</td>
<td>6</td>
<td>$116.05</td>
<td>$118.95</td>
<td>$121.92</td>
<td>$124.97</td>
<td>$128.09</td>
<td>$116.05</td>
</tr>
<tr>
<td>54151S</td>
<td>Network Engineer III</td>
<td>Bachelor's</td>
<td>5</td>
<td>$66.69</td>
<td>$68.36</td>
<td>$70.07</td>
<td>$71.82</td>
<td>$73.62</td>
<td>$66.69</td>
</tr>
<tr>
<td>54151S</td>
<td>Network Engineer IV</td>
<td>Masters</td>
<td>6</td>
<td>$84.34</td>
<td>$86.45</td>
<td>$88.61</td>
<td>$90.82</td>
<td>$93.09</td>
<td>$84.34</td>
</tr>
<tr>
<td>54151S</td>
<td>Database Specialist III</td>
<td>Bachelor's</td>
<td>5</td>
<td>$74.20</td>
<td>$76.06</td>
<td>$77.96</td>
<td>$79.91</td>
<td>$81.90</td>
<td>$74.20</td>
</tr>
<tr>
<td>54151S</td>
<td>Database Specialist IV</td>
<td>Masters</td>
<td>6</td>
<td>$78.40</td>
<td>$80.36</td>
<td>$82.37</td>
<td>$84.43</td>
<td>$86.54</td>
<td>$78.40</td>
</tr>
<tr>
<td>54151S</td>
<td>Deployment Engineer III</td>
<td>Bachelor's</td>
<td>5</td>
<td>$69.14</td>
<td>$70.86</td>
<td>$72.64</td>
<td>$74.45</td>
<td>$76.31</td>
<td>$69.14</td>
</tr>
<tr>
<td>54151S</td>
<td>IT Security Specialist III</td>
<td>Bachelor's</td>
<td>5</td>
<td>$77.74</td>
<td>$79.68</td>
<td>$81.67</td>
<td>$83.71</td>
<td>$85.81</td>
<td>$77.74</td>
</tr>
<tr>
<td>54151S</td>
<td>IT Security Specialist IV</td>
<td>Masters</td>
<td>6</td>
<td>$84.24</td>
<td>$86.34</td>
<td>$88.50</td>
<td>$90.72</td>
<td>$92.98</td>
<td>$84.24</td>
</tr>
<tr>
<td>54151S</td>
<td>Project Control Specialist III</td>
<td>Bachelor's</td>
<td>5</td>
<td>$68.77</td>
<td>$70.48</td>
<td>$72.25</td>
<td>$74.05</td>
<td>$75.90</td>
<td>$68.77</td>
</tr>
<tr>
<td>54151S</td>
<td>Program Manager III</td>
<td>Bachelor's</td>
<td>5</td>
<td>$94.73</td>
<td>$97.09</td>
<td>$99.52</td>
<td>$102.01</td>
<td>$104.56</td>
<td>$94.73</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------------------------------------</td>
<td>-----------</td>
<td>------------</td>
<td>--------------</td>
<td>--------------</td>
<td>--------------</td>
<td>--------------</td>
<td>--------------</td>
<td>--------------</td>
</tr>
<tr>
<td>54151S</td>
<td>Program Manager IV</td>
<td>Masters</td>
<td>6</td>
<td>$105.64</td>
<td>$108.28</td>
<td>$110.99</td>
<td>$113.76</td>
<td>$116.61</td>
<td>$105.64</td>
</tr>
<tr>
<td>54151S</td>
<td>Project Manager III</td>
<td>Bachelor's</td>
<td>5</td>
<td>$89.17</td>
<td>$91.40</td>
<td>$93.68</td>
<td>$96.02</td>
<td>$98.42</td>
<td>$89.17</td>
</tr>
<tr>
<td>54151S</td>
<td>Project Manager IV</td>
<td>Masters</td>
<td>6</td>
<td>$94.15</td>
<td>$96.50</td>
<td>$98.92</td>
<td>$101.39</td>
<td>$103.92</td>
<td>$94.15</td>
</tr>
<tr>
<td>54151S</td>
<td>Quality Assurance Specialist II</td>
<td>Bachelor's</td>
<td>5</td>
<td>$74.20</td>
<td>$76.06</td>
<td>$77.96</td>
<td>$79.91</td>
<td>$81.90</td>
<td>$74.20</td>
</tr>
<tr>
<td>54151S</td>
<td>Quality Assurance Specialist III</td>
<td>Bachelor's</td>
<td>5</td>
<td>$74.20</td>
<td>$76.06</td>
<td>$77.96</td>
<td>$79.91</td>
<td>$81.90</td>
<td>$74.20</td>
</tr>
<tr>
<td>54151S</td>
<td>Requirements Analyst IV</td>
<td>Masters</td>
<td>6</td>
<td>$84.34</td>
<td>$86.45</td>
<td>$88.61</td>
<td>$90.82</td>
<td>$93.09</td>
<td>$84.34</td>
</tr>
<tr>
<td>54151S</td>
<td>Subject Matter Expert II</td>
<td>Associates</td>
<td>2</td>
<td>$105.41</td>
<td>$108.04</td>
<td>$110.74</td>
<td>$113.51</td>
<td>$116.35</td>
<td>$105.41</td>
</tr>
<tr>
<td>54151S</td>
<td>Subject Matter Expert III</td>
<td>Bachelor's</td>
<td>5</td>
<td>$124.84</td>
<td>$127.96</td>
<td>$131.16</td>
<td>$134.44</td>
<td>$137.80</td>
<td>$124.84</td>
</tr>
<tr>
<td>54151S</td>
<td>Systems Administrator II</td>
<td>Associates</td>
<td>2</td>
<td>$63.25</td>
<td>$64.83</td>
<td>$66.45</td>
<td>$68.11</td>
<td>$69.81</td>
<td>$63.25</td>
</tr>
<tr>
<td>54151S</td>
<td>Systems Administrator III</td>
<td>Bachelor's</td>
<td>5</td>
<td>$72.31</td>
<td>$74.12</td>
<td>$75.98</td>
<td>$77.87</td>
<td>$79.82</td>
<td>$72.31</td>
</tr>
<tr>
<td>54151S</td>
<td>Systems Administrator IV</td>
<td>Masters</td>
<td>6</td>
<td>$81.78</td>
<td>$83.82</td>
<td>$85.92</td>
<td>$88.06</td>
<td>$90.27</td>
<td>$81.78</td>
</tr>
<tr>
<td>54151S</td>
<td>Systems Engineer III</td>
<td>Bachelor's</td>
<td>5</td>
<td>$75.77</td>
<td>$77.66</td>
<td>$79.61</td>
<td>$81.60</td>
<td>$83.64</td>
<td>$75.77</td>
</tr>
<tr>
<td>54151S</td>
<td>Test Engineer IV</td>
<td>Bachelor's</td>
<td>5</td>
<td>$90.44</td>
<td>$92.70</td>
<td>$95.02</td>
<td>$97.40</td>
<td>$99.83</td>
<td>$90.44</td>
</tr>
<tr>
<td>54151S</td>
<td>Test Engineer IV</td>
<td>Masters</td>
<td>6</td>
<td>$80.94</td>
<td>$82.97</td>
<td>$85.04</td>
<td>$87.17</td>
<td>$89.35</td>
<td>$80.94</td>
</tr>
<tr>
<td>54151S</td>
<td>Web Designer III</td>
<td>Bachelor's</td>
<td>5</td>
<td>$65.29</td>
<td>$66.92</td>
<td>$68.59</td>
<td>$70.31</td>
<td>$72.07</td>
<td>$65.29</td>
</tr>
<tr>
<td>54151S</td>
<td>Web Designer IV</td>
<td>Masters</td>
<td>6</td>
<td>$76.12</td>
<td>$78.03</td>
<td>$79.98</td>
<td>$81.98</td>
<td>$84.03</td>
<td>$76.12</td>
</tr>
<tr>
<td>541611,</td>
<td>Junior Knowledge Manager - SharePoint Administrator</td>
<td>Bachelor's</td>
<td>3</td>
<td>$98.31</td>
<td>$100.77</td>
<td>$103.29</td>
<td>$105.87</td>
<td>$108.52</td>
<td>$98.31</td>
</tr>
<tr>
<td>541990L</td>
<td>Journeyman Knowledge Manager - SharePoint - Administrator</td>
<td>Bachelor's</td>
<td>6</td>
<td>$112.26</td>
<td>$115.06</td>
<td>$117.94</td>
<td>$120.89</td>
<td>$123.91</td>
<td>$112.26</td>
</tr>
<tr>
<td>541611,</td>
<td>Senior Knowledge Manager - SharePoint - Administrator</td>
<td>Masters</td>
<td>8</td>
<td>$120.35</td>
<td>$123.36</td>
<td>$126.44</td>
<td>$129.60</td>
<td>$132.84</td>
<td>$120.35</td>
</tr>
<tr>
<td>541990L</td>
<td>Junior Linguist</td>
<td>Bachelor's</td>
<td>3</td>
<td>$67.26</td>
<td>$68.94</td>
<td>$70.67</td>
<td>$72.43</td>
<td>$74.24</td>
<td>$67.26</td>
</tr>
<tr>
<td>541990L</td>
<td>Journeyman Linguist</td>
<td>Bachelor's</td>
<td>3</td>
<td>$75.43</td>
<td>$77.32</td>
<td>$79.25</td>
<td>$81.23</td>
<td>$83.26</td>
<td>$75.43</td>
</tr>
<tr>
<td>541990L</td>
<td>Senior Linguist</td>
<td>Masters</td>
<td>8</td>
<td>$80.23</td>
<td>$82.24</td>
<td>$84.30</td>
<td>$86.40</td>
<td>$88.56</td>
<td>$80.23</td>
</tr>
<tr>
<td>541990L</td>
<td>Junior Intelligence Analyst</td>
<td>Bachelor's</td>
<td>3</td>
<td>$74.59</td>
<td>$76.45</td>
<td>$78.36</td>
<td>$80.32</td>
<td>$82.33</td>
<td>$74.59</td>
</tr>
<tr>
<td>541990L</td>
<td>Journeyman Intelligence Analyst</td>
<td>Bachelor's</td>
<td>8</td>
<td>$84.02</td>
<td>$86.12</td>
<td>$88.27</td>
<td>$90.48</td>
<td>$92.74</td>
<td>$84.02</td>
</tr>
<tr>
<td>541990L</td>
<td>Senior Intelligence Analyst</td>
<td>Masters</td>
<td>8</td>
<td>$89.61</td>
<td>$91.85</td>
<td>$94.14</td>
<td>$96.49</td>
<td>$98.91</td>
<td>$89.61</td>
</tr>
<tr>
<td>541990L</td>
<td>Junior Maritime Domain Analyst (MDA)</td>
<td>Bachelor's</td>
<td>3</td>
<td>$80.91</td>
<td>$82.93</td>
<td>$85.00</td>
<td>$87.13</td>
<td>$89.31</td>
<td>$80.91</td>
</tr>
<tr>
<td>541990L</td>
<td>Journeyman Maritime Domain Analyst (MDA)</td>
<td>Bachelor's</td>
<td>8</td>
<td>$90.11</td>
<td>$92.37</td>
<td>$94.68</td>
<td>$97.04</td>
<td>$99.47</td>
<td>$90.11</td>
</tr>
<tr>
<td>541990L</td>
<td>Senior Maritime Domain Analyst (MDA)</td>
<td>Masters</td>
<td>8</td>
<td>$95.66</td>
<td>$98.05</td>
<td>$100.50</td>
<td>$103.01</td>
<td>$105.59</td>
<td>$95.66</td>
</tr>
<tr>
<td>541990L</td>
<td>Junior Cyber Intelligence Analyst</td>
<td>Bachelor's</td>
<td>3</td>
<td>$85.74</td>
<td>$87.88</td>
<td>$90.08</td>
<td>$92.33</td>
<td>$94.64</td>
<td>$85.74</td>
</tr>
<tr>
<td>-------</td>
<td>--------------------------------------</td>
<td>-----------</td>
<td>------------</td>
<td>----------</td>
<td>----------</td>
<td>----------</td>
<td>----------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>541990L</td>
<td>Journeyman Cyber Intelligence Analyst</td>
<td>Bachelor</td>
<td>6</td>
<td>$97.59</td>
<td>$100.03</td>
<td>$102.53</td>
<td>$105.09</td>
<td>$107.72</td>
<td></td>
</tr>
<tr>
<td>541990L</td>
<td>Senior Cyber Intelligence Analyst</td>
<td>Masters</td>
<td>6</td>
<td>$104.76</td>
<td>$107.38</td>
<td>$110.07</td>
<td>$112.82</td>
<td>$115.64</td>
<td></td>
</tr>
<tr>
<td>541990L</td>
<td>Junior Information Security Analyst</td>
<td>Bachelor</td>
<td>3</td>
<td>$81.37</td>
<td>$83.41</td>
<td>$85.49</td>
<td>$87.63</td>
<td>$89.82</td>
<td></td>
</tr>
<tr>
<td>541990L</td>
<td>Journeyman Information Security Analyst</td>
<td>Bachelor</td>
<td>6</td>
<td>$90.07</td>
<td>$92.32</td>
<td>$94.63</td>
<td>$96.99</td>
<td>$99.42</td>
<td></td>
</tr>
<tr>
<td>541990L</td>
<td>Senior Information Security Analyst</td>
<td>Masters</td>
<td>8</td>
<td>$95.46</td>
<td>$97.85</td>
<td>$100.30</td>
<td>$102.80</td>
<td>$105.37</td>
<td></td>
</tr>
<tr>
<td>541611L, 541990L</td>
<td>Journeyman Project Manager/Program Manager</td>
<td>Bachelor</td>
<td>6</td>
<td>$147.45</td>
<td>$151.13</td>
<td>$154.91</td>
<td>$158.78</td>
<td>$162.75</td>
<td></td>
</tr>
<tr>
<td>541611L, 541990L</td>
<td>Senior Project Manager/Program Manager</td>
<td>Masters</td>
<td>8</td>
<td>$156.84</td>
<td>$160.76</td>
<td>$164.78</td>
<td>$168.90</td>
<td>$173.13</td>
<td></td>
</tr>
<tr>
<td>541611L, 541990L</td>
<td>Senior Executive Strategist</td>
<td>Masters</td>
<td>8</td>
<td>$166.67</td>
<td>$170.84</td>
<td>$175.11</td>
<td>$179.49</td>
<td>$183.98</td>
<td></td>
</tr>
<tr>
<td>541611L, 541990L</td>
<td>Senior Subject Matter Expert (SME)</td>
<td>Masters</td>
<td>8</td>
<td>$164.73</td>
<td>$168.85</td>
<td>$173.07</td>
<td>$177.40</td>
<td>$181.83</td>
<td></td>
</tr>
<tr>
<td>541611L, 541990L</td>
<td>Subject Matter Expert (SME)</td>
<td>Masters</td>
<td>12</td>
<td>$190.46</td>
<td>$195.22</td>
<td>$200.10</td>
<td>$205.10</td>
<td>$210.23</td>
<td></td>
</tr>
<tr>
<td>541611L, 541990L</td>
<td>Junior Knowledge Manager - SharePoint - Developer</td>
<td>Bachelor</td>
<td>3</td>
<td>$92.54</td>
<td>$94.86</td>
<td>$97.23</td>
<td>$99.66</td>
<td>$102.15</td>
<td></td>
</tr>
<tr>
<td>541611L, 541990L</td>
<td>Journeyman Knowledge Manager - SharePoint - Developer</td>
<td>Bachelor</td>
<td>6</td>
<td>$102.53</td>
<td>$105.09</td>
<td>$107.72</td>
<td>$110.41</td>
<td>$113.17</td>
<td></td>
</tr>
<tr>
<td>541611L, 541990L</td>
<td>Senior Knowledge Manager - SharePoint - Developer</td>
<td>Masters</td>
<td>8</td>
<td>$108.54</td>
<td>$111.26</td>
<td>$114.04</td>
<td>$116.89</td>
<td>$119.81</td>
<td></td>
</tr>
<tr>
<td>541611L, 541990L</td>
<td>Junior Data Analyst</td>
<td>Bachelor</td>
<td>3</td>
<td>$91.18</td>
<td>$93.46</td>
<td>$95.80</td>
<td>$98.19</td>
<td>$100.65</td>
<td></td>
</tr>
<tr>
<td>541611L, 541990L</td>
<td>Journeyman Data Analyst</td>
<td>Bachelor</td>
<td>6</td>
<td>$103.25</td>
<td>$105.83</td>
<td>$108.47</td>
<td>$111.19</td>
<td>$113.96</td>
<td></td>
</tr>
<tr>
<td>541611L, 541990L</td>
<td>Senior Data Analyst</td>
<td>Masters</td>
<td>8</td>
<td>$110.28</td>
<td>$113.04</td>
<td>$115.86</td>
<td>$118.76</td>
<td>$121.73</td>
<td></td>
</tr>
<tr>
<td>541611L, 541990L</td>
<td>Junior Research Analyst</td>
<td>Bachelor</td>
<td>3</td>
<td>$81.01</td>
<td>$83.04</td>
<td>$85.11</td>
<td>$87.24</td>
<td>$89.42</td>
<td></td>
</tr>
<tr>
<td>541611L, 541990L</td>
<td>Journeyman Research Analyst</td>
<td>Bachelor</td>
<td>6</td>
<td>$91.33</td>
<td>$93.61</td>
<td>$95.95</td>
<td>$98.35</td>
<td>$100.81</td>
<td></td>
</tr>
<tr>
<td>541611L, 541990L</td>
<td>Senior Research Analyst</td>
<td>Masters</td>
<td>8</td>
<td>$96.97</td>
<td>$99.39</td>
<td>$101.87</td>
<td>$104.42</td>
<td>$107.03</td>
<td></td>
</tr>
<tr>
<td>541611L, 541990L</td>
<td>Junior Acquisition Analyst</td>
<td>Bachelor</td>
<td>3</td>
<td>$98.31</td>
<td>$100.77</td>
<td>$103.29</td>
<td>$105.87</td>
<td>$108.52</td>
<td></td>
</tr>
<tr>
<td>541611L, 541990L</td>
<td>Journeyman Acquisition Analyst</td>
<td>Bachelor</td>
<td>6</td>
<td>$112.26</td>
<td>$115.06</td>
<td>$117.94</td>
<td>$120.89</td>
<td>$123.91</td>
<td></td>
</tr>
<tr>
<td>541611L, 541990L</td>
<td>Senior Acquisition Analyst</td>
<td>Masters</td>
<td>8</td>
<td>$120.35</td>
<td>$123.36</td>
<td>$126.44</td>
<td>$129.60</td>
<td>$132.84</td>
<td></td>
</tr>
<tr>
<td>541611L, 541990L</td>
<td>Junior Procurement Analyst</td>
<td>Bachelor</td>
<td>3</td>
<td>$77.04</td>
<td>$78.96</td>
<td>$80.94</td>
<td>$82.96</td>
<td>$85.03</td>
<td></td>
</tr>
<tr>
<td>541611L, 541990L</td>
<td>Journeyman Procurement Analyst</td>
<td>Bachelor</td>
<td>6</td>
<td>$85.95</td>
<td>$88.10</td>
<td>$90.30</td>
<td>$92.56</td>
<td>$94.87</td>
<td></td>
</tr>
<tr>
<td>541611L, 541990L</td>
<td>Senior Procurement Analyst</td>
<td>Masters</td>
<td>8</td>
<td>$91.33</td>
<td>$93.62</td>
<td>$95.96</td>
<td>$98.36</td>
<td>$100.82</td>
<td></td>
</tr>
<tr>
<td>SIN</td>
<td>Title</td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 541611,   | **Junior Knowledge Manager - SharePoint    | **Required Licenses or Certifications:** None  
**Security Clearance:** Variable  
Knowledge Manager – SharePoint administrator is responsible for current and future knowledge systems, data and management of information for client focused environment.  
**Brief Description of Duties:**  
• Manages SharePoint Knowledge Management (KM) Portals and the day to day operations of the portal.  
• Manages the Portal Change Request process for their respective portal(s).  
• Maintains training material and trains users for their respective SharePoint portal.  
• Provides SharePoint user experience and interface (UX/UI) expertise.  
• Assist with the maintenance of the customer’s acquisition and personnel databases.  
• Monitors the professional appearance of SharePoint pages. |
| 541990L  | Administrator** | Bachelors 3 |
| 541611,   | **Journeyman Knowledge Manager - SharePoint** | **Required Licenses or Certifications:** None  
**Security Clearance:** Variable  
Knowledge Manager – SharePoint administrator is responsible for current and future knowledge systems, data and management of information for client focused environment.  
**Brief Description of Duties:**  
• Manages SharePoint Knowledge Management (KM) Portals and the day to day operations of the portal.  
• Manages the Portal Change Request process for their respective portal(s).  
• Maintains training material and trains users for their respective SharePoint portal.  
• Provides SharePoint user experience and interface (UX/UI) expertise.  
• Assist with the maintenance of the customer’s acquisition and personnel databases.  
• Monitors the professional appearance of SharePoint pages. |
| 541990L  | Administrator** | Bachelors 6 |
| 541611,   | **Senior Knowledge Manager - SharePoint**  | **Required Licenses or Certifications:** None  
**Security Clearance:** Variable  
Knowledge Manager – SharePoint administrator is responsible for current and future knowledge systems, data and management of information for client focused environment.  
**Brief Description of Duties:**  
• Manages SharePoint Knowledge Management (KM) Portals and the day to day operations of the portal.  
• Manages the Portal Change Request process for their respective portal(s).  
• Maintains training material and trains users for their respective SharePoint portal.  
• Provides SharePoint user experience and interface (UX/UI) expertise.  
• Assist with the maintenance of the customer’s acquisition and personnel databases.  
• Monitors the professional appearance of SharePoint pages. |
<p>| 541990L  | Administrator** | Masters 8 |</p>
<table>
<thead>
<tr>
<th>SIN</th>
<th>Title</th>
<th>Description</th>
<th>Min. Edu.</th>
<th>Years Exp.</th>
</tr>
</thead>
</table>
| 541990L  | Junior Linguist     | **Required Licenses or Certifications:** Certified by a competent and accredited independent state, or federal language translation certification authority. **Security Clearance:** Variable  
- Reads and identifies if foreign documents contain any Personal Identifiable Information (PII). Documents include: Business Licenses, Tax Licenses, Article of Association, Official Picture Identification, Financial documents, company portfolios  
- Translates PII found during OSINT or supplied company documents from languages within Central Command to English. Languages include: Dari, Pashtu, Arabic, Turkish and Kurdish  
- Records translated information in a vendor vetting translation template supplied by the Vendor Threat Mitigation branch.  
- Able to fluently read, write and understand English and the language requiring translation at a high-school level or its equivalent or above.  
- Certified by a competent and accredited independent state, or federal language translation certification authority. | Bachelors | 3         |
| 541990L  | Journeyman Linguist | **Required Licenses or Certifications:** Certified by a competent and accredited independent state, or federal language translation certification authority. **Security Clearance:** Variable  
- Reads and identifies if foreign documents contain any Personal Identifiable Information (PII). Documents include: Business Licenses, Tax Licenses, Article of Association, Official Picture Identification, Financial documents, company portfolios  
- Translates PII found during OSINT or supplied company documents from languages within Central Command to English. Languages include: Dari, Pashtu, Arabic, Turkish and Kurdish  
- Records translated information in a vendor vetting translation template supplied by the Vendor Threat Mitigation branch.  
- Able to fluently read, write and understand English and the language requiring translation at a high-school level or its equivalent or above.  
- Certified by a competent and accredited independent state, or federal language translation certification authority. | Bachelors | 6         |
| 541990L  | Senior Linguist     | **Required Licenses or Certifications:** Certified by a competent and accredited independent state, or federal language translation certification authority. **Security Clearance:** Variable  
- Reads and identifies if foreign documents contain any Personal Identifiable Information (PII). Documents include: Business Licenses, Tax Licenses, Article of Association, Official Picture Identification, Financial documents, company portfolios  
- Translates PII found during OSINT or supplied company documents from languages within Central Command to English. Languages include: Dari, Pashtu, Arabic, Turkish and Kurdish  
- Records translated information in a vendor vetting translation template supplied by the Vendor Threat Mitigation branch.  
- Able to fluently read, write and understand English and the language requiring translation at a high-school level or its equivalent or above.  
- Certified by a competent and accredited independent state, or federal language translation certification authority. | Masters   | 8         |
<table>
<thead>
<tr>
<th>SIN</th>
<th>Title</th>
<th>Description</th>
<th>Min. Edu.</th>
<th>Years Exp.</th>
</tr>
</thead>
</table>
| 541990L | **Junior Intelligence Analyst** | **Required Licenses or Certifications:** None  
**Security Clearance:** Variable  
Perform collection, control and dissemination of intelligence/counterintelligence information.  
- Develop and maintain criminal network link analysis in FALCON/Palantir and/or Analyst Notebook  
- Incorporate classified foreign intelligence information into criminal network analyses.  
- Conduct risk assessments and develop criteria from which to establish risk.  
- Conduct network analysis and targeting efforts.  
- Perform systematic reviews, exploitations, in depth analysis, coordinates, monitors, and disseminates national and international intelligence/counterintelligence, law enforcement developments and trends.  
- Utilize intelligence information to produce and disseminate strategic, operational and tactical intelligence products.  
- Independently draft intelligence reports or sections of more complex intelligence assessments.  
- Be knowledgeable of and understand how to implement the standards described in Intelligence Community Directives 203 (Analytic Standards), 206 (Sourcing Requirements) and 208 (Writing for Maximum Utility).  
- Interpret and evaluate intelligence analyses and draft critical interagency intelligence assessments.  
- Locate, acquire, review, select and organize intelligence materials for use in briefings, reports and other analytic products.  
- Analyze the significance and policy implications of issues under investigation.  
- Apprise intelligence officials at all levels, within and outside the organization, on emerging issues by preparing intelligence reports and presenting oral briefings.  
- Plan, develop, organize and conduct special research studies providing comprehensive assessments of broad, exceptionally complex or highly sensitive issues.  
- Utilize agency and industry standards to evaluate the validity, accuracy and reliability of a broad array and high volume of information for translation into intelligence relevant to ICE.  
- Initiate contact with key personnel, fellow intelligence analysts and experts to validate and ascertain the reliability and urgency of information.  
- Monitor intelligence trends to anticipate and formulate new operations requirements.  
- Maintain liaison and operational relationships with JTF personnel and facilitate a collaborative effort. | Bachelors | 3          |
<table>
<thead>
<tr>
<th>SIN</th>
<th>Title</th>
<th>Description</th>
<th>Min. Edu.</th>
<th>Years Exp.</th>
</tr>
</thead>
</table>
| 541990L| Journeyman Intelligence Analyst | **Required Licenses or Certifications:** None  
**Security Clearance:** Variable  
Perform collection, control and dissemination of intelligence/counterintelligence information.  
• Develop and maintain criminal network link analysis in FALCON/Palantir and/or Analyst Notebook  
• Incorporate classified foreign intelligence information into criminal network analyses.  
• Conduct risk assessments and develop criteria from which to establish risk.  
• Conduct network analysis and targeting efforts.  
• Perform systematic reviews, exploitations, in depth analysis, coordinates, monitors, and disseminates national and international intelligence/counterintelligence, law enforcement developments and trends.  
• Utilize intelligence information to produce and disseminate strategic, operational and tactical intelligence products.  
• Independently draft intelligence reports or sections of more complex intelligence assessments.  
• Be knowledgeable of and understand how to implement the standards described in Intelligence Community Directives 203 (Analytic Standards), 206 (Sourcing Requirements) and 208 (Writing for Maximum Utility).  
• Interpret and evaluate intelligence analyses and draft critical interagency intelligence assessments.  
• Locate, acquire, review, select and organize intelligence materials for use in briefings, reports and other analytic products.  
• Analyze the significance and policy implications of issues under investigation.  
• Apprise intelligence officials at all levels, within and outside the organization, on emerging issues by preparing intelligence reports and presenting oral briefings.  
• Plan, develop, organize and conduct special research studies providing comprehensive assessments of broad, exceptionally complex or highly sensitive issues.  
• Utilize agency and industry standards to evaluate the validity, accuracy and reliability of a broad array and high volume of information for translation into intelligence relevant to ICE.  
• Initiate contact with key personnel, fellow intelligence analysts and experts to validate and ascertain the reliability and urgency of information.  
• Monitor intelligence trends to anticipate and formulate new operations requirements.  
• Maintain liaison and operational relationships with JTF personnel and facilitate a collaborative effort. | Bachelors | 6          |
<table>
<thead>
<tr>
<th>SIN</th>
<th>Title</th>
<th>Description</th>
<th>Min. Edu.</th>
<th>Years Exp.</th>
</tr>
</thead>
</table>
| 541990L  | Senior Intelligence Analyst | **Required Licenses or Certifications:** None  
*Security Clearance:* Variable  
Perform collection, control and dissemination of intelligence/counterintelligence information.  
• Develop and maintain criminal network link analysis in FALCON/Palantir and/or Analyst Notebook  
• Incorporate classified foreign intelligence information into criminal network analyses.  
• Conduct risk assessments and develop criteria from which to establish risk.  
• Conduct network analysis and targeting efforts.  
• Perform systematic reviews, exploitations, in depth analysis, coordinates, monitors, and disseminates national and international intelligence/counterintelligence, law enforcement developments and trends.  
• Utilize intelligence information to produce and disseminate strategic, operational and tactical intelligence products.  
• Independently draft intelligence reports or sections of more complex intelligence assessments.  
• Be knowledgeable of and understand how to implement the standards described in Intelligence Community Directives 203 (Analytic Standards), 206 (Sourcing Requirements) and 208 (Writing for Maximum Utility).  
• Interpret and evaluate intelligence analyses and draft critical interagency intelligence assessments.  
• Locate, acquire, review, select and organize intelligence materials for use in briefings, reports and other analytic products.  
• Analyze the significance and policy implications of issues under investigation.  
• Apprise intelligence officials at all levels, within and outside the organization, on emerging issues by preparing intelligence reports and presenting oral briefings.  
• Plan, develop, organize and conduct special research studies providing comprehensive assessments of broad, exceptionally complex or highly sensitive issues  
• Utilize agency and industry standards to evaluate the validity, accuracy and reliability of a broad array and high volume of information for translation into intelligence relevant to ICE.  
• Initiate contact with key personnel, fellow intelligence analysts and experts to validate and ascertain the reliability and urgency of information.  
• Monitor intelligence trends to anticipate and formulate new operations requirements.  
• Maintain liaison and operational relationships with JTF personnel and facilitate a collaborative effort. | Masters  | 8           |
<table>
<thead>
<tr>
<th>SIN</th>
<th>Title</th>
<th>Description</th>
<th>Min. Edu.</th>
<th>Years Exp.</th>
</tr>
</thead>
</table>
| 541990L | **Junior Maritime Domain Analyst (MDA)**   | **Required Licenses or Certifications:** None  
**Security Clearance:** Variable  
• Identify and report to respective Chain of Command on system problem reports/change requests, and services.  
• Perform data exploitation, improve JIATF West’s understanding of counter-threat capabilities and TTPs, and develop best practices to improve MDA for JIATF West J3, law enforcement agencies and partner nation counterparts.  
• Attend technical exchange meetings to provide assistance, coordination, and collaboration with Government leads as needed.  
• Conduct Multi-Int maritime fusion analysis through use of the Joint Worldwide Intelligence Communications System (JWICS) as it relates to the JIATF West counterdrug mission, including phone toll analysis and vessel target development.  
• Conduct initial Signal Development (SIGDEV) & Electronic Intelligence (ELINT) analysis to enhance the JIATF West counterdrug maritime intelligence picture and conduct analysis on real-world counterdrug vessels of interest through standardized intelligence community tools.  
• Produce weekly maritime Vessels of Interest lists to be shared with US and interagency partners, providing greater MDA to the ITC.  
• Assist with maintenance of MDA standing operating procedures, guides, checklists, concept of operations (CONOPs) and other documentation required to improve and professionalize command operational MDA capabilities.  
• Create and provide briefings for flag and executive-level leadership on MDA events, cases, capabilities, and analysis and assessments.  
• Participate in and document After-Action Reports, lessons learned, and observations from operational events conducted. | Bachelors | 3          |
| 541990L | **Journeyman Maritime Domain Analyst (MDA)** | **Required Licenses or Certifications:** None  
**Security Clearance:** Variable  
• Identify and report to respective Chain of Command on system problem reports/change requests, and services.  
• Perform data exploitation, improve JIATF West’s understanding of counter-threat capabilities and TTPs, and develop best practices to improve MDA for JIATF West J3, law enforcement agencies and partner nation counterparts.  
• Attend technical exchange meetings to provide assistance, coordination, and collaboration with Government leads as needed.  
• Conduct Multi-Int maritime fusion analysis through use of the Joint Worldwide Intelligence Communications System (JWICS) as it relates to the JIATF West counterdrug mission, including phone toll analysis and vessel target development.  
• Conduct initial Signal Development (SIGDEV) & Electronic Intelligence (ELINT) analysis to enhance the JIATF West counterdrug maritime intelligence picture and conduct analysis on real-world counterdrug vessels of interest through standardized intelligence community tools.  
• Produce weekly maritime Vessels of Interest lists to be shared with US and interagency partners, providing greater MDA to the ITC.  
• Assist with maintenance of MDA standing operating procedures, guides, checklists, concept of operations (CONOPs) and other documentation required to improve and professionalize command operational MDA capabilities.  
• Create and provide briefings for flag and executive-level leadership on MDA events, cases, capabilities, and analysis and assessments.  
• Participate in and document After-Action Reports, lessons learned, and observations from operational events conducted. | Bachelors | 6          |
<table>
<thead>
<tr>
<th>SIN</th>
<th>Title</th>
<th>Description</th>
<th>Min. Edu.</th>
<th>Years Exp.</th>
</tr>
</thead>
</table>
| 541990L | **Senior Maritime Domain Analyst (MDA)** | **Required Licenses or Certifications:** None  
**Security Clearance:** Variable  
- Identify and report to respective Chain of Command on system problem reports/change requests, and services.  
- Perform data exploitation, improve JIATF West’s understanding of counter-threat capabilities and TTPs, and develop best practices to improve MDA for JIATF West J3, law enforcement agencies and partner nation counterparts.  
- Attend technical exchange meetings to provide assistance, coordination, and collaboration with Government leads as needed.  
- Conduct Multi-Int maritime fusion analysis through use of the Joint Worldwide Intelligence Communications System (JWICS) as it relates to the JIATF West counterdrug mission, including phone toll analysis and vessel target development.  
- Conduct initial Signal Development (SIGDEV) & Electronic Intelligence (ELINT) analysis to enhance the JIATF West counterdrug maritime intelligence picture and conduct analysis on real-world counterdrug vessels of interest through standardized intelligence community tools.  
- Produce weekly maritime Vessels of Interest lists to be shared with US and interagency partners, providing greater MDA to the ITC.  
- Assist with maintenance of MDA standing operating procedures, guides, checklists, concept of operations (CONOPs) and other documentation required to improve and professionalize command operational MDA capabilities.  
- Create and provide briefings for flag and executive-level leadership on MDA events, cases, capabilities, and analysis and assessments.  
- Participate in and document After-Action Reports, lessons learned, and observations from operational events conducted. | Masters   | 8          |
<table>
<thead>
<tr>
<th>SIN</th>
<th>Title</th>
<th>Description</th>
<th>Min. Edu.</th>
<th>Years Exp.</th>
</tr>
</thead>
</table>
| 541990L | Junior Cyber Intelligence Analyst | **Required Licenses or Certifications:** None  
**Security Clearance:** TS/SCI Security Clearance  
Analyst will work as a cyber all-source intelligence threat analyst, as an integral part of a diverse contract team supporting a DoD Scientific and Technical Intelligence (S&T) client. Provide the required experience and expertise to perform in-depth technical research, analysis, and assessment of foreign cyber technologies, capabilities, and threats to US ground force systems, combat support systems, and operations in response to Production Requirements and Requests for Information from DoD or Service Combatant, Functional, Acquisition, and Research & Development Commands.  
**Basic Qualifications:**  
• TS/SCI Security Clearance  
• Ability and experience authoring concise, in-depth, well-sourced intelligence assessments and RFI responses in conformance with intelligence community (IC) analytic standards  
• Ability to research, create, develop, and deliver professional briefings and multimedia presentations  
• Knowledge of the intelligence cycle, and the process for all-source intelligence research, analysis and production  
• Knowledge of current and emerging cyber threat technologies, capabilities and methodologies  
• Knowledge of current and emerging cybersecurity technologies and methodologies  
• Knowledge of current and emerging computer, computer networks, and communications networks technologies, designs and programs  
• Ability to interact, collaborate and coordinate with small groups on intelligence data and information requirements, and research, analysis and production  
• Possession of excellent oral and written communication skills  
• Familiarity with, and experience utilizing, all intelligence sources (Cyber, IMINT, SIGINT, OSINT, and HUMINT, etc.)  
• Familiarity with, and experience utilizing, current intelligence databases, networks, libraries, and exploitation/analysis tools (such as, WEBTAS, Analytical Notebook, DCSG-A, GIS tools and M3)  
• Knowledge of USG intelligence organizations (DIA, NSA, CIA, Service Intelligence Centers, USCYBERCOM, ARCYBER), programs, and products | Bachelors | 3          |
<table>
<thead>
<tr>
<th>SIN</th>
<th>Title</th>
<th>Description</th>
<th>Min. Edu.</th>
<th>Years Exp.</th>
</tr>
</thead>
</table>
| 541990L | Journeyman Cyber Intelligence Analyst | **Required Licenses or Certifications:** None  
**Security Clearance:** TS/SCI Security Clearance  
Analyst will work as a cyber all-source intelligence threat analyst, as an integral part of a diverse contract team supporting a DoD Scientific and Technical Intelligence (S&TI) client. Provide the required experience and expertise to perform in-depth technical research, analysis, and assessment of foreign cyber technologies, capabilities, and threats to US ground force systems, combat support systems, and operations in response to Production Requirements and Requests for Information from DoD or Service Combatant, Functional, Acquisition, and Research & Development Commands.  
Basic Qualifications:  
• TS/SCI Security Clearance  
• Ability and experience authoring concise, in-depth, well-sourced intelligence assessments and RFI responses in conformance with intelligence community (IC) analytic standards  
• Ability to research, create, develop, and deliver professional briefings and multimedia presentations  
• Knowledge of the intelligence cycle, and the process for all-source intelligence research, analysis and production  
• Knowledge of current and emerging cyber threat technologies, capabilities and methodologies  
• Knowledge of current and emerging cybersecurity technologies and methodologies  
• Knowledge of current and emerging computer, computer networks, and communications networks technologies, designs and programs  
• Ability to interact, collaborate and coordinate with small groups on intelligence data and information requirements, and research, analysis and production  
• Possession of excellent oral and written communication skills  
• Familiarity with, and experience utilizing, all intelligence sources (Cyber, IMINT, SIGINT, OSINT, and HUMINT, etc.)  
• Familiarity with, and experience utilizing, current intelligence databases, networks, libraries, and exploitation/analysis tools (such as, WEBTAS, Analytical Notebook, DCSG-A, GIS tools and M3)  
• Knowledge of USG intelligence organizations (DIA, NSA, CIA, Service Intelligence Centers, USCYBERCOM, ARCYBER), programs, and products | Bachelors | 6          |
<table>
<thead>
<tr>
<th>SIN</th>
<th>Title</th>
<th>Description</th>
<th>Min. Edu.</th>
<th>Years Exp.</th>
</tr>
</thead>
</table>
| 541990L | Senior Cyber Intelligence Analyst          | **Required Licenses or Certifications:** None  
**Security Clearance:** TS/SCI Security Clearance  
Analyst will work as a cyber all-source intelligence threat analyst, as an integral part of a diverse contract team supporting a DoD Scientific and Technical Intelligence (S&TI) client. Provide the required experience and expertise to perform in-depth technical research, analysis, and assessment of foreign cyber technologies, capabilities, and threats to US ground force systems, combat support systems, and operations in response to Production Requirements and Requests for Information from DoD or Service Combatant, Functional, Acquisition, and Research & Development Commands.  
**Basic Qualifications:**  
• TS/SCI Security Clearance  
• Ability and experience authoring concise, in-depth, well-sourced intelligence assessments and RFI responses in conformance with intelligence community (IC) analytic standards  
• Ability to research, create, develop, and deliver professional briefings and multimedia presentations  
• Knowledge of the intelligence cycle, and the process for all-source intelligence research, analysis and production  
• Knowledge of current and emerging cyber threat technologies, capabilities and methodologies  
• Knowledge of current and emerging cybersecurity technologies and methodologies  
• Knowledge of current and emerging computer, computer networks, and communications networks technologies, designs and programs  
• Ability to interact, collaborate and coordinate with small groups on intelligence data and information requirements, and research, analysis and production  
• Possession of excellent oral and written communication skills  
• Familiarity with, and experience utilizing, all intelligence sources (Cyber, IMINT, SIGINT, OSINT, and HUMINT, etc.)  
• Familiarity with, and experience utilizing, current intelligence databases, networks, libraries, and exploitation/analysis tools (such as, WEBTAS, Analytical Notebook, DCSG-A, GIS tools and M3)  
• Knowledge of USG intelligence organizations (DIA, NSA, CIA, Service Intelligence Centers, USCYBERCOM, ARCYBER), programs, and products |
<p>|         |                                            | Masters 8                                                                                           | Masters   | 8          |</p>
<table>
<thead>
<tr>
<th>SIN</th>
<th>Title</th>
<th>Description</th>
<th>Min. Edu.</th>
<th>Years Exp.</th>
</tr>
</thead>
</table>
| 541990L | Junior Information Security Analyst | **Required Licenses or Certifications:** IAT Level II/III certified (Security+, CISSP, CISA, CEH, etc.) Preferred – CISSP -ISSEP/ISSAP  
**Security Clearance:** Variable  
  • Implement and document analysis, testing, and evaluations activities necessary to ensure that the systems and networks obtain and maintain full accreditation with NIST 800-53 controls and RMF standards  
  • Perform patch management and execute system vulnerability scans and anti-malware software using approved processes.  
  • Use approved tools to collect IAVAs, determine which are relevant to ABIS systems, categorize them in terms of severity, prioritize them on the watch-list based on category, schedule patches based on priorities but no less frequently than monthly, verify system logs that patches were installed correctly, and support system scans to verify the remediation.  
  • Implement industry standard operating system and application hardening practices, including strong user access controls and authentication, robust roles and privileges management, disciplined patching and scanning, firewall and boundary protection, and IDS/IPS capabilities.  
  • Conduct system assessments and the development/implementation of a continuous monitoring program, configuration changes, policy compliance as well as user and network activity auditing.  
  • Develop and implement a Continuous Diagnostics and Mitigation (CDM) plan to assess the CS posture of all ABIS systems, and ensure compliance with FISMA standards, and address evolving threats.  
  • Ability to periodically perform vulnerability assessments and penetration testing to secure systems and networks  
  • Support Incident Response/Disaster Recovery - containment, assessment, and risk remediation techniques  
  • Support holistic and integrated Cybersecurity approach ensures information confidentiality, integrity, and availability of AABIS/IABIS systems  
  • Participates in enterprise architecture planning activities  
  • Creates information security system requirements  
  • Creates and maintains information security architecture diagrams and control catalogs  
  • Participates in information security system and control testing activities  
  • Partners with other IT teams in business continuity and disaster recovery planning activities  
  • Collaborates with risk and compliance functions to ensure controls meet regulatory requirements and adequately reduce risk  
  • Supporting Identification, Credential, and Access Management (ICAM) requirements  
  • Supporting Continuous Diagnostics and Mitigation (CDM) Implementation and Management  
  • Developing and conducting security training - Performing compliance management functions  
  • Supporting IV&V (Independent Verification and Validation) / Auditing  
  • Conducting Assessment and Authorization (A&A)  
  • Conducting penetration testing  
  • Supporting security incident remediation services  
  • Development and deployment of security architecture and engineering changes  
  • Support advanced network security engineering  
  • Enhancing security operations capabilities and operating a full security operations center (SOC) to include Monitoring, Incident Response, Vulnerability Management, and O&M of all security tools  
  • Working knowledge of risk management concepts  
  • Certifications - IAT Level II/III certified (Security+, CISSP, CISA, CEH, etc.) Preferred – CISSP -ISSEP/ISSAP | Bachelors | 3          |
<table>
<thead>
<tr>
<th>SIN</th>
<th>Title</th>
<th>Description</th>
<th>Min. Edu.</th>
<th>Years Exp.</th>
</tr>
</thead>
</table>
| 541990L| **Journeyman Information Security Analyst** | **Required Licenses or Certifications:** None  
**Security Clearance:** Variable  
- Implement and document analysis, testing, and evaluations activities necessary to ensure that the systems and networks obtain and maintain full accreditation with NIST 800-53 controls and RMF standards  
- Perform patch management and execute system vulnerability scans and anti-malware software using approved processes.  
- Use approved tools to collect IAVAs, determine which are relevant to ABIS systems, categorize them in terms of severity, prioritize them on the watch-list based on category, schedule patches based on priorities but no less frequently than monthly, verify system logs that patches were installed correctly, and support system scans to verify the remediation.  
- Implement industry standard operating system and application hardening practices, including strong user access controls and authentication, robust roles and privileges management, disciplined patching and scanning, firewall and boundary protection, and IDS/IPS capabilities.  
- Conduct system assessments and the development/implementation of a continuous monitoring program, configuration changes, policy compliance as well as user and network activity auditing.  
- Develop and implement a Continuous Diagnostics and Mitigation (CDM) plan to assess the CS posture of all ABIS systems, and ensure compliance with FISMA standards, and address evolving threats.  
- Ability to periodically perform vulnerability assessments and penetration testing to secure systems and networks  
- Support Incident Response/Disaster Recovery - containment, assessment, and risk remediation techniques  
- Support holistic and integrated Cybersecurity approach ensures information confidentiality, integrity, and availability of AABIS/IABIS systems  
- Participates in enterprise architecture planning activities  
- Creates information security system requirements  
- Creates and maintains information security architecture diagrams and control catalogs  
- Participates in information security system and control testing activities  
- Partners with other IT teams in business continuity and disaster recovery planning activities  
- Collaborates with risk and compliance functions to ensure controls meet regulatory requirements and adequately reduce risk  
- Supporting Identification, Credential, and Access Management (ICAM) requirements  
- Supporting Continuous Diagnostics and Mitigation {Monitoring} (CDM) Implementation and Management  
- Developing and conducting security training - Performing compliance management functions  
- Supporting IV&V (Independent Verification and Validation) / Auditing  
- Conducting Assessment and Authorization (A&A)  
- Conducting penetration testing  
- Supporting security incident remediation services  
- Development and deployment of security architecture and engineering changes  
- Support advanced network security engineering  
- Enhancing security operations capabilities and operating a full security operations center (SOC) to include Monitoring, Incident Response, Vulnerability Management, and O&M of all security tools  
- Working knowledge of risk management concepts  
- **Certifications - IAT Level II/III certified** (Security+, CISSP, CISA, CEH, etc.)  
- Preferred – CISSP -ISSEP/ISSAP | Bachelors | 6          |
<table>
<thead>
<tr>
<th>SIN</th>
<th>Title</th>
<th>Description</th>
<th>Min. Edu.</th>
<th>Years Exp.</th>
</tr>
</thead>
</table>
| 541990L | **Senior Information Security Analyst** | **Required Licenses or Certifications:** IAT Level II/III certified (Security+, CISSP, CISA, CEH, etc.) Preferred – CISSP -ISSEP/ISSAP  
**Security Clearance:** No  
- Implement and document analysis, testing, and evaluations activities necessary to ensure that the systems and networks obtain and maintain full accreditation with NIST 800-53 controls and RMF standards  
- Perform patch management and execute system vulnerability scans and anti-malware software using approved processes.  
- Use approved tools to collect IAVAs, determine which are relevant to ABIS systems, categorize them in terms of severity, prioritize them on the watch-list based on category, schedule patches based on priorities but no less frequently than monthly, verify system logs that patches were installed correctly, and support system scans to verify the remediation.  
- Implement industry standard operating system and application hardening practices, including strong user access controls and authentication, robust roles and privileges management, disciplined patching and scanning, firewall and boundary protection, and IDS/IPS capabilities.  
- Conduct system assessments and the development/implementation of a continuous monitoring program, configuration changes, policy compliance as well as user and network activity auditing.  
- Develop and implement a Continuous Diagnostics and Mitigation (CDM) plan to assess the CS posture of all ABIS systems, and ensure compliance with FISMA standards, and address evolving threats.  
- Ability to periodically perform vulnerability assessments and penetration testing to secure systems and networks  
- Support Incident Response/Disaster Recovery - containment, assessment, and risk remediation techniques  
- Support holistic and integrated Cybersecurity approach ensures information confidentiality, integrity, and availability of AABIS/IABIS systems  
- Participates in enterprise architecture planning activities  
- Creates information security system requirements  
- Creates and maintains information security architecture diagrams and control catalogs  
- Participates in information security system and control testing activities  
- Partners with other IT teams in business continuity and disaster recovery planning activities  
- Collaborates with risk and compliance functions to ensure controls meet regulatory requirements and adequately reduce risk  
- Supporting Identification, Credential, and Access Management (ICAM) requirements  
- Supporting Continuous Diagnostics and Mitigation (Monitoring) (CDM) Implementation and Management  
- Developing and conducting security training - Performing compliance management functions  
- Supporting IV&V (Independent Verification and Validation) / Auditing  
- Conducting Assessment and Authorization (A&A)  
- Conducting penetration testing  
- Supporting security incident remediation services  
- Development and deployment of security architecture and engineering changes  
- Support advanced network security engineering  
- Enhancing security operations capabilities and operating a full security operations center (SOC) to include Monitoring, Incident Response, Vulnerability Management, and O&M of all security tools  
- Working knowledge of risk management concepts  
- Certifications - IAT Level II/III certified (Security+, CISSP, CISA, CEH, etc.) Preferred – CISSP -ISSEP/ISSAP | Masters  | 8          |
<table>
<thead>
<tr>
<th>SIN</th>
<th>Title</th>
<th>Description</th>
<th>Min. Edu.</th>
<th>Years Exp.</th>
</tr>
</thead>
</table>
| 541611, 541990L | **Journeyman Project Manager/Program Manager** | **Required Licenses or Certifications:** PMP, IAT Level II/III certified (Security+, CISSP, CISA, CEH, etc.)  
**Security Clearance:** Variable  
- Bachelor’s degree with over 6 years of experience  
- Experience managing all resources on the project  
- Direct point of contact with client on all project/program related matters  
- Manage small and large complex projects especially related to IT security contracts and other related fields  
- Experience typically includes engagement experience in program scope and approach, focus on program delivery and technical integration, ability to drive risk services’ strategy and planning changes at the executive levels, oversight of key risk enablers, and management of project resources.  
- Certifications – PMP, IAT Level II/III certified (Security+, CISSP, CISA, CEH, etc.) | Bachelors | 6          |
| 541611, 541990L | **Senior Project Manager/Program Manager** | **Required Licenses or Certifications:** PMP, IAT Level II/III certified (Security+, CISSP, CISA, CEH, etc.)  
**Security Clearance:** Variable  
- Bachelor’s degree with over 6 years of experience  
- Experience managing all resources on the project  
- Direct point of contact with client on all project/program related matters  
- Manage small and large complex projects especially related to IT security contracts and other related fields  
- Experience typically includes engagement experience in program scope and approach, focus on program delivery and technical integration, ability to drive risk services’ strategy and planning changes at the executive levels, oversight of key risk enablers, and management of project resources.  
- Certifications – PMP, IAT Level II/III certified (Security+, CISSP, CISA, CEH, etc.) | Masters   | 8          |
| 541611, 541990L | **Senior Executive Strategist** | **Required Licenses or Certifications:** IAT Level II/III certified (Security+, CISSP, CISA, CEH, etc.)  
**Security Clearance:** Variable  
- Master’s Degree (MS/MA) and a minimum of twelve years of experience in business, IT, and process risk assessments  
- Provide scientific mission-focused senior executive leadership in the areas of risk assessments, organizational effectiveness, business and financial strategy, policy and compliance strategy, leadership and management strategy, communications, scientific leadership, technology strategy, and data science.  
- Interface with senior leadership in a strategic, evaluatory, and facilitating manner to help the organization better achieve their goals across the board.  
- Certifications - IAT Level II/III certified (Security+, CISSP, CISA, CEH, etc.) | Masters   | 8          |
<table>
<thead>
<tr>
<th>SIN</th>
<th>Title</th>
<th>Description</th>
<th>Min. Edu.</th>
<th>Years Exp.</th>
</tr>
</thead>
</table>
| 541611, 541990L | **Senior Subject Matter Expert (SME)** | **Required Licenses or Certifications:** IAT Level II/III certified (Security+, CISSP, CISA, CEH, etc.)  
**Security Clearance:** Variable  
- Expert with Advanced degree (M.S., Ph.D.) and a minimum of twelve years of experience in a leadership-level science and technology role, minimum of five years’ experience in a professional consulting role.  
- Broadly skilled, technically adept, and scientifically versed individual that can span multiple domains of expertise including, but not limited to risk assessments, enterprise IT, financial, process, and business risks, cybersecurity, information assurance, software development, science, and strategy.  
- Skilled multi-audience executive-level communicator and can serve as an effective expert translator between multiple domain areas, as well as develop, implement, and train on cross-functional strategic solutions based on the needs of the organization.  
- Make recommendations and advise on organization-wide system improvements, optimization or maintenance efforts in the following specialties: information systems architecture; cybersecurity; information assurance; automation; risk management; software; lifecycle management; software development methodologies; and modeling and simulation.  
- Certifications - IAT Level II/III certified (Security+, CISSP, CISA, CEH, etc.) | Masters | 8 |
| 8     |                                            |                                                                                                       |           |            |
| 3     |                                            |                                                                                                       |           |            |
| 6     |                                            |                                                                                                       |           |            |
| 8     |                                            |                                                                                                       |           |            |
| 541611, 541990L | **Subject Matter Expert (SME)** | **Required Licenses or Certifications:** IAT Level II/III certified (Security+, CISSP, CISA, CEH, etc.)  
**Security Clearance:** Variable  
- Expert with Advanced degree (M.S., Ph.D.) and a minimum of twelve years of experience in a leadership-level science and technology role, minimum of five years’ experience in a professional consulting role.  
- Broadly skilled, technically adept, and scientifically versed individual that can span multiple domains of expertise including, but not limited to risk assessments, enterprise IT, financial, process, and business risks, cybersecurity, information assurance, software development, science, and strategy.  
- Skilled multi-audience executive-level communicator and can serve as an effective expert translator between multiple domain areas, as well as develop, implement, and train on cross-functional strategic solutions based on the needs of the organization.  
- Make recommendations and advise on organization-wide system improvements, optimization or maintenance efforts in the following specialties: information systems architecture; cybersecurity; information assurance; automation; risk management; software; lifecycle management; software development methodologies; and modeling and simulation.  
- Certifications - IAT Level II/III certified (Security+, CISSP, CISA, CEH, etc.) | Masters | 12 |
<table>
<thead>
<tr>
<th>SIN</th>
<th>Title</th>
<th>Description</th>
<th>Min. Edu.</th>
<th>Years Exp.</th>
</tr>
</thead>
</table>
| 541611, 541990L | Junior Knowledge Manager - SharePoint - Developer | Required Licenses or Certifications: None  
Security Clearance: Variable  
Knowledge Manger – SharePoint Developer is responsible for current and future knowledge systems, data and management of information for client focused environment.  
Brief Description of Duties:  
• Provides SharePoint expertise and support to the Project Manager.  
• Develops and manages SharePoint Knowledge Management (KM) Portals and the day to day operations of the portal.  
• Gathers user functional, interface, and user experience requirements for additions or changes to their respective SharePoint portal(s).  
• Responds to user-initiated help/service tickets and provide resolution.  
• Provides SharePoint portal development and management expertise.  
• Provides SharePoint user experience and interface (UX/UI) expertise.  
• Develops and deploys libraries, lists, pages, shells, and content for their respective SharePoint portal.  
• Develops training material and trains users for their respective SharePoint portal.  
• Monitors the professional appearance of SharePoint pages. | Bachelors | 3          |
| 541611, 541990L | Journeyman Knowledge Manager - SharePoint - Developer | Required Licenses or Certifications: None  
Security Clearance: Variable  
Knowledge Manger – SharePoint Developer is responsible for current and future knowledge systems, data and management of information for client focused environment.  
Brief Description of Duties:  
• Provides SharePoint expertise and support to the Project Manager.  
• Develops and manages SharePoint Knowledge Management (KM) Portals and the day to day operations of the portal.  
• Gathers user functional, interface, and user experience requirements for additions or changes to their respective SharePoint portal(s).  
• Responds to user-initiated help/service tickets and provide resolution.  
• Provides SharePoint portal development and management expertise.  
• Provides SharePoint user experience and interface (UX/UI) expertise.  
• Develops and deploys libraries, lists, pages, shells, and content for their respective SharePoint portal.  
• Develops training material and trains users for their respective SharePoint portal.  
• Monitors the professional appearance of SharePoint pages. | Bachelors | 6          |
| 541611, 541990L | Senior Knowledge Manager - SharePoint - Developer | Required Licenses or Certifications: None  
Security Clearance: Variable  
Knowledge Manger – SharePoint Developer is responsible for current and future knowledge systems, data and management of information for client focused environment.  
Brief Description of Duties:  
• Provides SharePoint expertise and support to the Project Manager.  
• Develops and manages SharePoint Knowledge Management (KM) Portals and the day to day operations of the portal.  
• Gathers user functional, interface, and user experience requirements for additions or changes to their respective SharePoint portal(s).  
• Responds to user-initiated help/service tickets and provide resolution.  
• Provides SharePoint portal development and management expertise.  
• Provides SharePoint user experience and interface (UX/UI) expertise.  
• Develops and deploys libraries, lists, pages, shells, and content for their respective SharePoint portal.  
• Develops training material and trains users for their respective SharePoint portal.  
• Monitors the professional appearance of SharePoint pages. | Masters | 8          |
<table>
<thead>
<tr>
<th>SIN</th>
<th>Title</th>
<th>Description</th>
<th>Min. Edu.</th>
<th>Years Exp.</th>
</tr>
</thead>
</table>
| 541611, 541990L | Junior Data Analyst    | **Required Licenses or Certifications:** None  
**Security Clearance:** Variable  
• Demonstrate experience, skill and knowledge in the area of acquisition and data analytics.  
• Provide support of analysis of the cost, schedule, and performance parameters of all active contracts within CBP/OIT.  
• Maintain and update all the data analysis, through a live action dashboard that provides near real-time statistics of all OIT active contracts.  
• Demonstrate strong knowledge of various DHS contract vehicles as well as appropriately quantifying acquisition data. | Bachelors | 3          |
| 541611, 541990L | Journeyman Data Analyst | **Required Licenses or Certifications:** None  
**Security Clearance:** Variable  
• Demonstrate experience, skill and knowledge in the area of acquisition and data analytics.  
• Provide support of analysis of the cost, schedule, and performance parameters of all active contracts within CBP/OIT.  
• Maintain and update all the data analysis, through a live action dashboard that provides near real-time statistics of all OIT active contracts.  
• Demonstrate strong knowledge of various DHS contract vehicles as well as appropriately quantifying acquisition data. | Bachelors | 6          |
| 541611, 541990L | Senior Data Analyst     | **Required Licenses or Certifications:** None  
**Security Clearance:** Variable  
• Demonstrate experience, skill and knowledge in the area of acquisition and data analytics.  
• Provide support of analysis of the cost, schedule, and performance parameters of all active contracts within CBP/OIT.  
• Maintain and update all the data analysis, through a live action dashboard that provides near real-time statistics of all OIT active contracts.  
• Demonstrate strong knowledge of various DHS contract vehicles as well as appropriately quantifying acquisition data. | Masters   | 8          |
<table>
<thead>
<tr>
<th>SIN</th>
<th>Title</th>
<th>Description</th>
<th>Min. Edu.</th>
<th>Years Exp.</th>
</tr>
</thead>
</table>
| 541611, 541990L | Junior Research Analyst | **Required Licenses or Certifications:** None  
**Security Clearance:** Variable  
Research analyst interpret, manage, and analyze research data in order to translate results into better solutions, work to facilitate greater returns through analyzing habits and data of selected subjects.  
**Research Analyst Duties and Responsibilities**  
- Analyze data and information to find ways to improve operations  
- Inform and advise various levels of management and stakeholders  
- Analyze habits and data available from subjects  
- Research market and industry trends and patterns  
- Create detailed reports of findings  
- Simplify findings into presentations  
- Organize and store data for future research projects  
- Document all data and research procedures  
- Create diagrams and documentation to pinpoint problems and find solutions  
- Implement tests of processes, policies, and protocols  
- Identify and understand problems through forecasting, gap analysis, quantitative reporting, research, and statistical analysis  
- Recommend changes and improvements based on research findings  
- Write reports, white papers, and other published documents  
- Compile and analyze data points  
- Conducts open-source intelligence (OSINT) analysis on foreign companies, corporations and personnel who desire to contract with the United States government  
- Authors Contractor Activity Reports (CARs) using OSINT results to construct a company profile to include, company’s information, identify all key management personnel and their personal identifiable information (PII) and financial information to be used in all-source analysis and assessment  
- Utilizes OSINT to identify any and all nefarious actors or actions conducted by the business, their personnel or any related business the company conducts business with.  
- Identifies if businesses or personnel have any dealings with the Great Power Competition (GPC) countries of interest | Bachelors | 3         |
<table>
<thead>
<tr>
<th>SIN</th>
<th>Title</th>
<th>Description</th>
<th>Min. Edu.</th>
<th>Years Exp.</th>
</tr>
</thead>
</table>
| 541611,   | **Journeyman Research Analyst** | Required Licenses or Certifications: None  
Security Clearance: Variable  
Research analyst interpret, manage, and analyze research data in order to translate results into better solutions, work to facilitate greater returns through analyzing habits and data of selected subjects.  
Research Analyst Duties and Responsibilities  
• Analyze data and information to find ways to improve operations  
• Inform and advise various levels of management and stakeholders  
• Analyze habits and data available from subjects  
• Research market and industry trends and patterns  
• Create detailed reports of findings  
• Simplify findings into presentations  
• Organize and store data for future research projects  
• Document all data and research procedures  
• Create diagrams and documentation to pinpoint problems and find solutions  
• Implement tests of processes, policies, and protocols  
• Identify and understand problems through forecasting, gap analysis, quantitative reporting, research, and statistical analysis  
• Recommend changes and improvements based on research findings  
• Write reports, white papers, and other published documents  
• Compile and analyze data points  
• Conducts open-source intelligence (OSINT) analysis on foreign companies, corporations and personnel who desire to contract with the United States government  
• Authors Contractor Activity Reports (CARs) using OSINT results to construct a company profile s to include, company’s information, identify all key management personnel and their personal identifiable information (PII) and financial information to be used in all-source analysis and assessment  
• Utilizes OSINT to identify any and all nefarious actors or actions conducted by the business, their personnel or any related business the company conducts business with.  
• Identifies if businesses or personnel have any dealings with the Great Power Competition (GPC) countries of interest | Bachelors | 6          |
<table>
<thead>
<tr>
<th>SIN</th>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
</table>
| 541611 | Senior Research Analyst    | **Required Licenses or Certifications:** None  
**Security Clearance:** Variable  
Research analysts interpret, manage, and analyze research data in order to translate results into better solutions, work to facilitate greater returns through analyzing habits and data of selected subjects.  
Research Analyst Duties and Responsibilities  
• Analyze data and information to find ways to improve operations  
• Inform and advise various levels of management and stakeholders  
• Analyze habits and data available from subjects  
• Research market and industry trends and patterns  
• Create detailed reports of findings  
• Simplify findings into presentations  
• Organize and store data for future research projects  
• Document all data and research procedures  
• Create diagrams and documentation to pinpoint problems and find solutions  
• Implement tests of processes, policies, and protocols  
• Identify and understand problems through forecasting, gap analysis, quantitative reporting, research, and statistical analysis  
• Recommend changes and improvements based on research findings  
• Write reports, white papers, and other published documents  
• Compile and analyze data points  
• Conducts open-source intelligence (OSINT) analysis on foreign companies, corporations and personnel who desire to contract with the United States government  
• Authors Contractor Activity Reports (CARs) using OSINT results to construct a company profile to include, company’s information, identify all key management personnel and their personal identifiable information (PII) and financial information to be used in all-source analysis and assessment  
• Utilizes OSINT to identify any and all nefarious actors or actions conducted by the business, their personnel or any related business the company conducts business with.  
• Identifies if businesses or personnel have any dealings with the Great Power Competition (GPC) countries of interest |

<table>
<thead>
<tr>
<th>Min. Edu.</th>
<th>Years Exp.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Masters</td>
<td>8</td>
</tr>
<tr>
<td>SIN</td>
<td>Title</td>
</tr>
<tr>
<td>-----</td>
<td>-------</td>
</tr>
</tbody>
</table>
| 541611 | Junior Acquisition Analyst | **Required Licenses or Certifications:** None  
**Security Clearance:** Variable  
Demonstrate experience, skill and knowledge in pre-award functions associated with awarding new contracts and task orders or other acquisitions at the program and project levels requiring government approval prior to release, including assisting in the preparation, review, and revision of draft Requests for Proposal and applicable Purchase Request packages (acquisition artifacts), integrated planning with other pre-award activities, and coordinating the activities associated with getting the authorization to award. Assist with development of acquisition plans, functional requirements or specifications, market research reports, independent government cost estimates, determination and findings, and justification and approval.  
Knowledge in the development of the following documents, including, but not limited to:  
- Acquisition Plans (AP)  
- Functional Requirements or Specifications  
- Market Research Reports  
- Independent Government Cost Estimates (IGCE)  
- Determination & Findings  
- Information Technology Acquisition Review (ITAR) requirements, if applicable  
- DHS Chief Information Officer (CIO) Checklists  
- DHS Waiver documents and process  
- Justification and Approval (J&A) (as required for other than full and open competition or limited sources)  
- Interagency Agreements (IAA) and Assisted Acquisitions  
- Justification Memos – Bona-fide needs statement for end-of-year procurement actions |

| 541611 | Journeyman Acquisition Analyst | **Required Licenses or Certifications:** None  
**Security Clearance:** No  
Demonstrate experience, skill and knowledge in pre-award functions associated with awarding new contracts and task orders or other acquisitions at the program and project levels requiring government approval prior to release, including assisting in the preparation, review, and revision of draft Requests for Proposal and applicable Purchase Request packages (acquisition artifacts), integrated planning with other pre-award activities, and coordinating the activities associated with getting the authorization to award. Assist with development of acquisition plans, functional requirements or specifications, market research reports, independent government cost estimates, determination and findings, and justification and approval.  
Knowledge in the development of the following documents, including, but not limited to:  
- Acquisition Plans (AP)  
- Functional Requirements or Specifications  
- Market Research Reports  
- Independent Government Cost Estimates (IGCE)  
- Determination & Findings  
- Information Technology Acquisition Review (ITAR) requirements, if applicable  
- DHS Chief Information Officer (CIO) Checklists  
- DHS Waiver documents and process  
- Justification and Approval (J&A) (as required for other than full and open competition or limited sources)  
- Interagency Agreements (IAA) and Assisted Acquisitions  
- Justification Memos – Bona-fide needs statement for end-of-year procurement actions | Bachelors 6 |
<table>
<thead>
<tr>
<th>SIN</th>
<th>Title</th>
<th>Description</th>
<th>Min. Edu.</th>
<th>Years Exp.</th>
</tr>
</thead>
</table>
| 541611| Senior Acquisition Analyst | Required Licenses or Certifications: None  
Security Clearance: Variable  
Demonstrate experience, skill and knowledge in pre-award functions associated with awarding new contracts and task orders or other acquisitions at the program and project levels requiring government approval prior to release, including assisting in the preparation, review, and revision of draft Requests for Proposal and applicable Purchase Request packages (acquisition artifacts), integrated planning with other pre-award activities, and coordinating the activities associated with getting the authorization to award. Assist with development of acquisition plans, functional requirements or specifications, market research reports, independent government cost estimates, determination and findings, and justification and approval.  
Knowledge in the development of the following documents, including, but not limited to:  
• Acquisition Plans (AP)  
• Functional Requirements or Specifications  
• Market Research Reports  
• Independent Government Cost Estimates (IGCE)  
• Determination & Findings  
• Information Technology Acquisition Review (ITAR) requirements, if applicable  
• DHS Chief Information Officer (CIO) Checklists  
• DHS Waiver documents and process  
• Justification and Approval (J&A) (as required for other than full and open competition or limited sources)  
• Interagency Agreements (IAA) and Assisted Acquisitions  
• Justification Memos – Bona-fide needs statement for end-of-year procurement actions | Masters   | 8          |
| 541611| Junior Procurement Analyst | Required Licenses or Certifications: None  
Security Clearance: Variable  
Writes contracting and procedural documentation for the wide range of contracting functions; serves as a resource in converting manual contracting business processes into automated business processes; analyzes new policies and laws, and interprets changes for senior management prior to issuing to contract specialists; reviews procurement packages that are complex and difficult prior to senior executive level signature approval; resolve complex procurement issues; integral member of a team that prepares reports on audits; analyzes and evaluates audit and inspection reports; performs as an expert with authority to respond to inspection and audit reports; develops operating guidance and procedures for the complex issues that arise and uses them as a basis to provide training to staff; interprets new legislation/policies and provides synopsis to senior level management; conducts training of interns or other contract specialists; explains impact of new policies, regulations, and guidance; participates as a member of procurement task forces or chairs these bodies working on high level procurement issues with agency wide impact; writes contracting procedures for use by operational contracting specialists; writes updated guidance impact to business processes and informs contracting staff via writing; responds in writing to audit reports and defends complex contracting action; prepares written contracting material for use in training; prepares briefings on complex procurement issues for use by senior procurement officials; defends and explains complex issues with auditors resulting from an audit. | Bachelors | 3          |
<table>
<thead>
<tr>
<th>SIN</th>
<th>Title</th>
<th>Description</th>
<th>Min. Edu.</th>
<th>Years Exp.</th>
</tr>
</thead>
</table>
| 541611| Journeyman Procurement Analyst | **Required Licenses or Certifications:** None  
**Security Clearance:** Variable  
Writes contracting and procedural documentation for the wide range of contracting functions; serves as a resource in converting manual contracting business processes into automated business processes; analyzes new policies and laws, and interprets changes for senior management prior to issuing to contract specialists; reviews procurement packages that are complex and difficult prior to senior executive level signature approval; resolve complex procurement issues; integral member of a team that prepares reports on audits; analyzes and evaluates audit and inspection reports; performs as an expert with authority to respond to inspection and audit reports; develops operating guidance and procedures for the complex issues that arise and uses them as a basis to provide training to staff; interprets new legislation/policies and provides synopsis to senior level management; conducts training of interns or other contract specialists; explains impact of new policies, regulations, and guidance; participates as a member of procurement task forces or chairs these bodies working on high level procurement issues with agency wide impact; writes contracting procedures for use by operational contracting specialists; writes updated guidance impact to business processes and informs contracting staff via writing; responds in writing to audit reports and defends complex contracting action; prepares written contracting material for use in training; prepares briefings on complex procurement issues for use by senior procurement officials; defends and explains complex issues with auditors resulting from an audit. | Bachelors | 6          |
| 541611| Senior Procurement Analyst       | **Required Licenses or Certifications:** None  
**Security Clearance:** Variable  
Writes contracting and procedural documentation for the wide range of contracting functions; serves as a resource in converting manual contracting business processes into automated business processes; analyzes new policies and laws, and interprets changes for senior management prior to issuing to contract specialists; reviews procurement packages that are complex and difficult prior to senior executive level signature approval; resolve complex procurement issues; integral member of a team that prepares reports on audits; analyzes and evaluates audit and inspection reports; performs as an expert with authority to respond to inspection and audit reports; develops operating guidance and procedures for the complex issues that arise and uses them as a basis to provide training to staff; interprets new legislation/policies and provides synopsis to senior level management; conducts training of interns or other contract specialists; explains impact of new policies, regulations, and guidance; participates as a member of procurement task forces or chairs these bodies working on high level procurement issues with agency wide impact; writes contracting procedures for use by operational contracting specialists; writes updated guidance impact to business processes and informs contracting staff via writing; responds in writing to audit reports and defends complex contracting action; prepares written contracting material for use in training; prepares briefings on complex procurement issues for use by senior procurement officials; defends and explains complex issues with auditors resulting from an audit. | Masters   | 8          |
<table>
<thead>
<tr>
<th>Level</th>
<th>Education</th>
<th>and</th>
<th>Experience</th>
<th>Acquired Degree</th>
<th>Minimum Experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>High School diploma or GED Certification</td>
<td>1 year</td>
<td>Less than High School/GED</td>
<td>2 years</td>
<td></td>
</tr>
<tr>
<td>II</td>
<td>Associates Degree or higher</td>
<td>2 years</td>
<td>High School/GED</td>
<td>7 years</td>
<td></td>
</tr>
<tr>
<td>III</td>
<td>Bachelor's Degree or higher</td>
<td>5 years</td>
<td>High School/GED</td>
<td>11 years</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Associate</td>
<td>7 years</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Master</td>
<td>3 years</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Doctorate</td>
<td>1 year</td>
<td></td>
</tr>
<tr>
<td>IV</td>
<td>Master's Degree or higher</td>
<td>6 years</td>
<td>High School/GED</td>
<td>15 years</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Associate</td>
<td>10 years</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Bachelor</td>
<td>8 years</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Doctorate</td>
<td>4 years</td>
<td></td>
</tr>
</tbody>
</table>

Due to the availability or limitation of education, occasionally substitution of experience as referenced below for a professional labor type with additional years of experience will be provided per the approval of the federal agency acquiring the service.
ITC standard regulations

1) 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 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

2) Services Performed

a) All 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.

b) The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity.

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

3) Travel. Any Contractor travel required in the performance of services must comply with the Pub. L. 99-234 and FAR Part 31.205-46, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel.

4) Warranty

a) Unless otherwise specified in this contract, the Contractor's standard commercial warranty as stated in the contract's commercial pricelist will apply to this contract.

b) The Contractor's commercial guarantee/warranty shall be included in the Commercial Supplier Agreement to include Enterprise User License Agreements or Terms of Service (TOS) agreements, if applicable.

c) Except as otherwise provided by an express or implied warranty, the Contractor will not be liable to the ordering activity for consequential damages resulting from any defect or deficiencies in accepted items.
<table>
<thead>
<tr>
<th>Regulation Number</th>
<th>Regulation Title/Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>52.222-46</td>
<td>EVALUATION OF COMPENSATION FOR PROFESSIONAL EMPLOYEES (FEB 1993)</td>
</tr>
<tr>
<td>52.222-48</td>
<td>EXEMPTION FROM APPLICATION OF THE SERVICE CONTRACT LABOR STANDARDS TO CONTRACTS FOR MAINTENANCE, CALIBRATION, OR REPAIR OF CERTAIN EQUIPMENT CERTIFICATION (MAY 2014)</td>
</tr>
<tr>
<td>52.223-19</td>
<td>COMPLIANCE WITH ENVIRONMENTAL MANAGEMENT SYSTEMS (MAY 2011)</td>
</tr>
<tr>
<td>52.223-2</td>
<td>AFFIRMATIVE PROCUREMENT OF BIOBASED PRODUCTS UNDER SERVICE AND CONSTRUCTION CONTRACTS (SEP 2013)</td>
</tr>
<tr>
<td>52.229-1</td>
<td>STATE AND LOCAL TAXES (APR 1984)</td>
</tr>
<tr>
<td>52.222-62</td>
<td>PAID SICK LEAVE UNDER EXECUTIVE ORDER 13706 (JAN 2017)</td>
</tr>
<tr>
<td>52.223-13</td>
<td>ACQUISITION OF EPEAT® - REGISTERED IMAGING EQUIPMENT (JUN 2014)</td>
</tr>
<tr>
<td>52.223-14</td>
<td>ACQUISITION OF EPEAT® - REGISTERED TELEVISIONS (JUN 2014)</td>
</tr>
<tr>
<td>52.223-16</td>
<td>ACQUISITION OF EPEAT® - REGISTERED PERSONAL COMPUTER PRODUCTS (OCT 2015)</td>
</tr>
<tr>
<td>552.238-115</td>
<td>SPECIAL ORDERING PROCEDURES FOR THE ACQUISITION OF ORDER-LEVEL MATERIALS (MAY 2019)</td>
</tr>
<tr>
<td>552.238-107</td>
<td>TRAFFIC RELEASE (SUPPLIES) (MAY 2019)</td>
</tr>
<tr>
<td>552.238-73</td>
<td>IDENTIFICATION OF ELECTRONIC OFFICE EQUIPMENT PROVIDING ACCESSIBILITY FOR THE HANDICAPPED (MAY 2019)</td>
</tr>
<tr>
<td>552.238-86</td>
<td>DELIVERY SCHEDULE (MAY 2019)</td>
</tr>
<tr>
<td>552.238-89</td>
<td>DELIVERIES TO THE U.S. POSTAL SERVICE (MAY 2019)</td>
</tr>
<tr>
<td>552.238-90</td>
<td>CHARACTERISTICS OF ELECTRIC CURRENT (MAY 2019)</td>
</tr>
<tr>
<td>552.238-91</td>
<td>MARKING AND DOCUMENTATION REQUIREMENTS FOR SHIPPING (MAY 2019)</td>
</tr>
<tr>
<td>552.238-92</td>
<td>VENDOR MANAGED INVENTORY (VMI) PROGRAM (MAY 2019)</td>
</tr>
<tr>
<td>552.238-93</td>
<td>ORDER ACKNOWLEDGMENT (MAY 2019)</td>
</tr>
<tr>
<td>552.238-94</td>
<td>ACCELERATED DELIVERY REQUIREMENTS (MAY 2019)</td>
</tr>
</tbody>
</table>