GENERAL SERVICES ADMINISTRATION
FEDERAL SUPPLY SERVICE
Authorized Federal Supply Schedule Price List

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

Multiple Award Schedule
FSC Group 70 Information Technology Equipment, Software, and Services
Contract Number GS-35F-0392X

Contract Period
May 18, 2011 – May 17, 2026
Current through Modification Mod A837 effective October 27, 2021

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

Contractor
Lunarline, Inc.
3300 Fairfax Drive, Suite 212
Arlington, VA 22201
P: 571-481-9300
F: 703-890-1594
E: lunarline.contracts@motorolasolutions.com
www.lunarline.com

Contract Administration Source
Lawrence Brooks
E: lawrence.brooks@motorolasolutions.com

Business Size: Large Business
# Table of Contents

- **Customer Information** ........................................................................................................................................................................ 3
- **Price List** .................................................................................................................................................................................................... 5
- **SIN 511210 IT Software License Descriptions** ........................................................................................................................................ 6
- **SIN 54151HACS Labor Category Descriptions** ......................................................................................................................................... 6
- **SIN 54151S Labor Category Descriptions** ............................................................................................................................................ 10
- **SIN 611420 Course Descriptions** .................................................................................................................................................... 27
- **Terms and Conditions Applicable to SIN 511210** ................................................................................................................................. 30
- **Terms and Conditions Applicable to SIN 54151HACS** ............................................................................................................................ 30
- **Terms and Conditions Applicable to SIN 54151S** ........................................................................................................................................... 39
- **Terms and Conditions Applicable to SIN 611420** ....................................................................................................................................... 42
CUSTOMER INFORMATION

1a Table of Awarded Special Item Numbers (SINs):

<table>
<thead>
<tr>
<th>SIN</th>
<th>SIN Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>511210</td>
<td>Software Licenses</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Highly Adaptive Cybersecurity Services (HACS)</td>
</tr>
<tr>
<td>54151S</td>
<td>Information Technology Professional Services</td>
</tr>
<tr>
<td>611420</td>
<td>Information Technology Training</td>
</tr>
</tbody>
</table>

1b Lowest Priced Model Number and Price for Each SIN:

<table>
<thead>
<tr>
<th>SIN</th>
<th>Item</th>
<th>Description</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>511210</td>
<td>1</td>
<td>LunarGravity</td>
<td>$986.42</td>
</tr>
<tr>
<td>54151HACS</td>
<td>4</td>
<td>Cyber Analyst Jr</td>
<td>103.68</td>
</tr>
<tr>
<td>54151S</td>
<td>17</td>
<td>Help Desk Analyst</td>
<td>49.11</td>
</tr>
<tr>
<td>611420</td>
<td>1</td>
<td>Cybersecurity Fundamentals Workshop 4 Day</td>
<td>2,021.05</td>
</tr>
</tbody>
</table>

1c Hourly Rates, Job Titles, Experience, Functional Responsibility, and Education List: Refer to Price List

2 Maximum Order*: $500,000/Order

*If the best value selection places your order over the Maximum Order identified in this catalog/price list, you have an opportunity to obtain a better schedule contract price. Before placing your order, contact the aforementioned contactor for a better price. The contractor may (1) offer a new price for this requirement (2) offer the lowest price available under this contract or (3) decline the order. A delivery order that exceeds the maximum order may be placed under the schedule contract in accordance with FAR 8.404.

3 Minimum Order: $100

4 Geographic Coverage:

- SINs 511210 and 611420: International
- SINs 54151HACS and 54151S: Domestic within the 48 contiguous states, Alaska, Hawaii, Puerto Rico, Washington, DC, and U.S. Territories

5 Points of Production: Professional and subscription services only

6 Discount from List Prices: Prices shown are Net

7 Quantity/Volume Discounts:

- SIN 511210:
  - 2-4 licenses receive a 5% quantity discount
  - 5+ licenses receive a 20% quantity discount
- SIN 54151HACS: 1% for orders at or exceeding $500,000
- SIN 54151S:
  - 1% for orders at or exceeding $100,000; and
  - 3% for orders at or exceeding $500,000
- SIN 611420: None

8 Prompt Payment Terms: 1% net 20 days for SINs 54151S and 611420. SINs 54151HACS and 511210 are net 30 days.

Information for Ordering Offices: Prompt payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions.
9a Government purchase cards are accepted at or below the micro-purchase threshold
9b Government purchase cards are not accepted above the micro-purchase threshold

10 Foreign Items: None

11a Time of Delivery: 30 days ARO
11b Expedited Delivery: Items available for expedited delivery are noted in this price list
11c Overnight and 2-day Delivery: Not available
11d Urgent Requirements: Agencies can contact the Contractor’s Representative to effect a faster delivery

12 F.O.B. Point(s): Destination
        Note: All travel required in the performance of this contract and orders placed hereunder must comply with the Federal Travel Regulations (FTR) or Joint Travel Regulations (JTR), as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all contractor travel. Contractors cannot use GSA city pair contracts. The contractor shall not add the Industrial Funding Fee onto travel costs. (F.O.B. Terms noted above)

13a Ordering Address: Lunarline, Inc., 3300 Fairfax Dr, Ste 212, Arlington, VA 22201
13b Ordering Procedures: For supplies and services, the ordering procedures, information on Blanket Purchase Agreements (BPAs) are found in Federal Acquisition Regulation (FAR) 8.405-3

14 Payment Address: Lunarline, Inc., c/o Delta Risk 106 S. St. Mary’s St. Ste 601 San Antonio, TX 78205
15 Warranty Provision: Not applicable
16 Export Packing Charges: Not applicable
17 Terms and Conditions of Government Purchase Card Acceptance: Accepted at or below the micro-purchase level
18 Terms and Conditions of Rental, Maintenance, and Repair: Not applicable
19 Terms and Conditions of Installation: Not applicable
20 Terms and Conditions of Repair Parts: Not applicable
20a Terms and Conditions for Any Other Services: Not applicable
21 List of Service and Distribution Points: Not applicable
22 List of Participating Dealers: Not applicable
23 Preventative maintenance: Not applicable
24a Special Attributes: Not applicable
24b Section 508 Compliance for Electronic and Information Technology (EIT) Supplies and Services:
        • SIN 511510: All offerings are 508 compliant in accordance with § 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d), FAR 39.2, and the EIT Accessibility Standards (36 CFR 1194). Section 508 compliance information on the supplies and services in this contract are available at the following address: lunarline.com. The EIT standard can be found at: Section508.gov/
        • SINs 54151HACS, 54151S, and 611420: Not applicable

25 DUNS: 14-7181569

26 Lunarline has an active registration in the System for Award Management (SAM) database
# PRICE LIST

## SIN 511520

<table>
<thead>
<tr>
<th>No.</th>
<th>Software Name</th>
<th>Annual Fee/License</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>LunarGravity</td>
<td>$986.42</td>
</tr>
</tbody>
</table>

## SIN 54151HACS

<table>
<thead>
<tr>
<th>No.</th>
<th>Labor Category</th>
<th>Rate/HR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cyber Program Manager</td>
<td>$204.03</td>
</tr>
<tr>
<td>2</td>
<td>Cyber Penetration Tester – Senior</td>
<td>149.62</td>
</tr>
<tr>
<td>3</td>
<td>Cyber Penetration Tester – Intermediate</td>
<td>124.69</td>
</tr>
<tr>
<td>4</td>
<td>Cyber Analyst – Senior</td>
<td>174.56</td>
</tr>
<tr>
<td>5</td>
<td>Cyber Analyst – Intermediate</td>
<td>134.66</td>
</tr>
<tr>
<td>6</td>
<td>Cyber Analyst – Junior</td>
<td>103.68</td>
</tr>
<tr>
<td>7</td>
<td>Cyber Engineer – Senior</td>
<td>179.55</td>
</tr>
<tr>
<td>8</td>
<td>Cyber Engineer – Intermediate</td>
<td>139.65</td>
</tr>
<tr>
<td>9</td>
<td>Cyber Engineer – Junior</td>
<td>113.55</td>
</tr>
<tr>
<td>10</td>
<td>Cyber Subject Matter Expert</td>
<td>194.84</td>
</tr>
</tbody>
</table>

## SIN 611420

<table>
<thead>
<tr>
<th>No.</th>
<th>Course Title</th>
<th># of Students</th>
<th>Rate/Course</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cybersecurity Fundamentals Workshop 4 Day</td>
<td>1</td>
<td>$2,021.05</td>
</tr>
<tr>
<td>2</td>
<td>Cyber Tools and Analysis Workshop 4 Day</td>
<td>1</td>
<td>2,021.05</td>
</tr>
<tr>
<td>3</td>
<td>Recovery Planning Practitioner COOP 5 Day</td>
<td>1</td>
<td>2,425.25</td>
</tr>
</tbody>
</table>

## SIN 54151S

<table>
<thead>
<tr>
<th>No.</th>
<th>Labor Category</th>
<th>Rate/HR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Analyst (Business/System/Data)</td>
<td>$129.24</td>
</tr>
<tr>
<td>2</td>
<td>Application Analyst</td>
<td>70.82</td>
</tr>
<tr>
<td>3</td>
<td>Application Developer - Senior</td>
<td>117.22</td>
</tr>
<tr>
<td>4</td>
<td>Application Developer - Mid</td>
<td>93.17</td>
</tr>
<tr>
<td>5</td>
<td>Application Developer - Junior</td>
<td>74.54</td>
</tr>
<tr>
<td>6</td>
<td>Application Integration Specialist</td>
<td>139.26</td>
</tr>
<tr>
<td>7</td>
<td>Certification Specialist - Senior</td>
<td>94.07</td>
</tr>
<tr>
<td>8</td>
<td>Certification Specialist - Mid</td>
<td>78.38</td>
</tr>
<tr>
<td>9</td>
<td>Certification Specialist - Junior</td>
<td>62.70</td>
</tr>
<tr>
<td>10</td>
<td>Computer System Security Specialist</td>
<td>86.49</td>
</tr>
<tr>
<td>11</td>
<td>Configuration Management Specialist</td>
<td>89.16</td>
</tr>
<tr>
<td>12</td>
<td>Database Administrator</td>
<td>133.24</td>
</tr>
<tr>
<td>13</td>
<td>Database Designer</td>
<td>129.24</td>
</tr>
<tr>
<td>14</td>
<td>Enterprise Architect - Senior</td>
<td>135.98</td>
</tr>
<tr>
<td>15</td>
<td>Enterprise Architect - Mid</td>
<td>113.32</td>
</tr>
<tr>
<td>16</td>
<td>Enterprise Architect - Junior</td>
<td>97.27</td>
</tr>
<tr>
<td>17</td>
<td>Help Desk Analyst</td>
<td>49.11</td>
</tr>
<tr>
<td>18</td>
<td>Information Assurance Engineer - Senior</td>
<td>129.24</td>
</tr>
<tr>
<td>19</td>
<td>Information Assurance Engineer - Mid</td>
<td>80.27</td>
</tr>
<tr>
<td>20</td>
<td>Information Assurance Engineer - Junior</td>
<td>73.66</td>
</tr>
<tr>
<td>21</td>
<td>Information Security Analyst - Senior</td>
<td>133.24</td>
</tr>
<tr>
<td>22</td>
<td>Information Security Analyst - Mid</td>
<td>92.59</td>
</tr>
<tr>
<td>23</td>
<td>Information Security Analyst - Junior</td>
<td>51.94</td>
</tr>
<tr>
<td>24</td>
<td>Information Security Engineer - Senior</td>
<td>149.27</td>
</tr>
<tr>
<td>25</td>
<td>Information Security Engineer - Mid</td>
<td>68.94</td>
</tr>
<tr>
<td>26</td>
<td>Information Security Engineer - Junior</td>
<td>134.25</td>
</tr>
<tr>
<td>27</td>
<td>Information System Security Specialist</td>
<td>153.52</td>
</tr>
<tr>
<td>28</td>
<td>Internet Developer - Senior</td>
<td>123.23</td>
</tr>
<tr>
<td>29</td>
<td>Internet Developer - Mid</td>
<td>97.18</td>
</tr>
<tr>
<td>30</td>
<td>IT Subject Matter Expert</td>
<td>143.26</td>
</tr>
<tr>
<td>31</td>
<td>IT Technologist</td>
<td>99.15</td>
</tr>
<tr>
<td>32</td>
<td>Network Engineer - Senior</td>
<td>133.24</td>
</tr>
<tr>
<td>33</td>
<td>Network Engineer - Mid</td>
<td>97.18</td>
</tr>
<tr>
<td>34</td>
<td>Network Security Specialist</td>
<td>139.26</td>
</tr>
<tr>
<td>35</td>
<td>Penetration Tester - Senior</td>
<td>90.66</td>
</tr>
<tr>
<td>36</td>
<td>Penetration Tester - Junior</td>
<td>75.55</td>
</tr>
<tr>
<td>37</td>
<td>Program Manager</td>
<td>139.26</td>
</tr>
<tr>
<td>38</td>
<td>Project Control Analyst</td>
<td>137.75</td>
</tr>
<tr>
<td>39</td>
<td>Project Manager</td>
<td>139.26</td>
</tr>
<tr>
<td>40</td>
<td>Quality Assurance Specialist</td>
<td>129.24</td>
</tr>
<tr>
<td>41</td>
<td>R&amp;D Specialist</td>
<td>147.76</td>
</tr>
<tr>
<td>42</td>
<td>Security Subject Matter Expert</td>
<td>147.76</td>
</tr>
<tr>
<td>43</td>
<td>Software Tester</td>
<td>93.17</td>
</tr>
<tr>
<td>44</td>
<td>System Administrator</td>
<td>133.24</td>
</tr>
<tr>
<td>45</td>
<td>System/Software Architect</td>
<td>134.25</td>
</tr>
<tr>
<td>46</td>
<td>Technical Instruction Specialist</td>
<td>89.16</td>
</tr>
<tr>
<td>47</td>
<td>Technical Writer - Mid</td>
<td>68.56</td>
</tr>
<tr>
<td>48</td>
<td>Technical Writer - Junior</td>
<td>57.13</td>
</tr>
<tr>
<td>49</td>
<td>Web Specialist</td>
<td>139.26</td>
</tr>
</tbody>
</table>
SIN 511210 IT SOFTWARE LICENSE DESCRIPTIONS

1. **Software Name:** LunarGravity  
   **Description and Equipment Compatibility:** LunarGravity allows users to convert files from a vulnerability scanner into a consolidated Excel workbook that is easily readable by humans. Users will have access to spreadsheets with information detailing each instance of every vulnerability discovered. Worksheets providing additional information, including the risk level posed by each vulnerability and a list of hosts where a given vulnerability was found, are supplied with the software. LunarGravity outputs reports in formats to support the assessment and authorization (A&A) process, the Federal Risk and Authorization Management Program (FedRAMP), risk assessment, Plan of Action & Milestones (POA&M), and Department of Defense (DoD). The software supports any vulnerability or risk assessment and authorization or penetration test. LunarGravity runs on Windows 10.X and above, and supports multiple static and dynamic code, vulnerability and penetration testing tools by the following vendors in the accompany formats:

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Scanner Name</th>
<th>Supported Exports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Security, Inc.</td>
<td>AppDetective Pro</td>
<td>*.xml</td>
</tr>
<tr>
<td>Application Security, Inc.</td>
<td>DbProtect</td>
<td>*.xml</td>
</tr>
<tr>
<td>BD Worldwide</td>
<td>BD Protect</td>
<td>*.xml</td>
</tr>
<tr>
<td>Center for Internet Security</td>
<td>Router Audit Tool</td>
<td>*.html or *.txt</td>
</tr>
<tr>
<td>DISA</td>
<td>STIG Viewer</td>
<td>(Up to Version 2.4) *.ckl</td>
</tr>
<tr>
<td>eEye</td>
<td>Retina and Retina CS</td>
<td>*.xml</td>
</tr>
<tr>
<td>Hewlett Packard</td>
<td>Fortify SCA</td>
<td>*.fpl, *.fvdl, *.xml</td>
</tr>
<tr>
<td>Insecurity.com LLC</td>
<td>WebInspect</td>
<td>*.xml</td>
</tr>
<tr>
<td>McAfee</td>
<td>Vulnerability Manager</td>
<td>*.xml</td>
</tr>
<tr>
<td>Netsparker Ltd.</td>
<td>Netsparker</td>
<td>*.htm, *.html</td>
</tr>
<tr>
<td>PortSwigger</td>
<td>Burp Suite</td>
<td>*.xml</td>
</tr>
<tr>
<td>Rapid7</td>
<td>Metasploit</td>
<td>(Limited) *.xml</td>
</tr>
<tr>
<td>Rapid7</td>
<td>Nexpose</td>
<td>(Version 2.0) *.xml</td>
</tr>
<tr>
<td>Tenable</td>
<td>Nessus</td>
<td>*.nessus</td>
</tr>
</tbody>
</table>

**Technical Support:**
- **Hot Line Technical Support Number:** 571-481-9300
- **Email Technical Support:** Lunarline.corporatesupport@motorolasolutions.com
- **Hours of Operation:** 9 AM to 5 PM Eastern Standard Time (EST)

**License Type:** Term, defined as a limited period of one (1) year. Licenses are not owned in perpetuity; users revoke the right to use the software license upon the end of the term period.

LunarGravity does not support open standard interoperability.

**Software Maintenance:** Each term license includes bug and defect fixes via updates and email technical support for one (1) year from the date of purchase.

SIN 54151HACS LABOR CATEGORY DESCRIPTIONS

1. **Commercial Job Title:** Cyber Program Manager  
   **Technical Qualifications/Experience:** Minimum five (5) years of experience in the IT industry, out of which at least three (3) years must be in the field of Project Management, Business Administration, Human Resources, and/or Client Relationship Management.

   **Functional Responsibility:** Act as the central point of contact with the Contracting Officer, Contracting Officer’s Representative and Task Managers. Responsible for coordinating the management of all work performed on this contract, including subcontractors, team members, and vendors. Keep in constant touch with the project managers regarding the status of various task order projects, the issues facing the project teams and
effectively and regularly updates the client representatives. Also facilitate the information, which the team requires from the client to effectively implement various Task Order Projects and if necessary, escalates the burning issues to the client representatives and contract officer. All the Task Order Project Managers typically report to the Program Manager for that contract.

Minimum Education: Undergraduate degree from an accredited institution or equivalent technical qualification. Seven (7) years of relevant experience is acceptable in lieu of a degree.

2 Commercial Job Title: Cyber Penetration Tester – Senior

Technical Qualifications/Experience: Minimum five (5) years of experience in security assessments, three (3) of which consist of performing penetration testing using both automated tools and manual methods to exploit identified weaknesses and vulnerabilities in information systems.

Functional Responsibility: Responsible for performing penetration testing on organizational information systems using both automated tools and manual methods to exploit identified weaknesses in applications, systems, and networks. Conducts extensive research and capitalizes on experience and skills to craft new exploitations, stress systems to achieve non-standard responses, and breach authorization boundaries. Mimics threat adversary capabilities, tactics, techniques, and procedures to attain information disclosure, root/administrative access, or other exploitation success. Conducts technical and physical social engineering activities to obtain unauthorized information disclosure while identifying human error and weakness in an organization. Responsible for adhering to the developed test plan, rules of engagement, conducting system testing as per pre-defined test cases, complete test reporting documentation, and recommending actions and strategies to mitigate known vulnerabilities and exploitation.

Minimum Education: Undergraduate degree from an accredited institution or equivalent technical qualification. Seven (7) years of relevant experience is acceptable in lieu of a degree.

3 Commercial Job Title: Cyber Penetration Tester – Intermediate

Technical Qualifications/Experience: Minimum three (3) years of experience in security assessments, two (2) of which consist of performing penetration testing using both automated tools and manual methods to exploit identified weaknesses and vulnerabilities in information systems.

Functional Responsibility: Responsible for performing penetration testing on organizational information systems using both automated tools and manual methods to exploit identified weaknesses in applications, systems, and networks. Conducts extensive research and capitalizes on experience and skills to craft new exploitations, stress systems to achieve non-standard responses, and breach authorization boundaries. Mimics threat adversary capabilities, tactics, techniques, and procedures to attain information disclosure, root/administrative access, or other exploitation success. Conducts technical and physical social engineering activities to obtain unauthorized information disclosure while identifying human error and weakness in an organization. Responsible for adhering to the developed test plan, rules of engagement, conducting system testing as per pre-defined test cases, complete test reporting documentation, and recommending actions and strategies to mitigate known vulnerabilities and exploitation.

Minimum Education: Undergraduate degree from an accredited institution or equivalent technical qualification. Five (5) years of relevant experience is acceptable in lieu of a degree.

4 Commercial Job Title: Cyber Analyst – Senior

Technical Qualifications/Experience: Minimum five (5) years of experience in defining, implementing and maintaining the information security for businesses, business units, divisions, organizations, agencies, etc. Must have strong knowledge of encryption, intrusion detection/prevention, network security, and ethical hacking/penetration testing.

Functional Responsibility: Responsible for ensuring that the organization’s networks, as well as information, is secure. Employ continuous monitoring of intrusion detection/prevention and other perimeter defense devices. Ensure appropriate data encryption (in transit and at rest) levels based on protection needs of targeted data.
Maintain awareness of system/network security posture to include vulnerability scanning to facilitate application of quick and effective corrective measures, while ensuring configuration management requirements are met. Provide technical knowledge and information assurance analysis support, to include security assessment of applications; operating systems; internet-facing interfaces, intranet and other interconnections. Strong knowledge of best practices associated with as well as appropriate authoritative guidance for physical security; network security; security risk assessments; critical infrastructure protection; continuity and contingency planning; emergency preparedness; security awareness and training. Provide analysis of existing systems vulnerabilities including possible intrusion/entry points, resource manipulation, denial of service, and/or destruction of resources. Provide technical support and analysis to document organizational information protection framework, and support policy and procedures preparation and implementation.

Minimum Education: Undergraduate degree from an accredited institution or equivalent technical qualification. Seven (7) years of relevant experience is acceptable in lieu of a degree.

5 Commercial Job Title: Cyber Analyst – Intermediate Technical Qualifications/Experience: Minimum three (3) years of experience in defining, implementing and maintaining the information security for businesses, business units, divisions, organizations, agencies, etc. Must have strong knowledge of encryption, intrusion detection/prevention, network security, and ethical hacking/penetration testing.

Functional Responsibility: Responsible for ensuring that the organization’s networks, as well as information, is secure. Employ continuous monitoring of intrusion detection/prevention and other perimeter defense devices. Ensure appropriate data encryption (in transit and at rest) levels based on protection needs of targeted data. Maintain awareness of system/network security posture to include vulnerability scanning to facilitate application of quick and effective corrective measures, while ensuring configuration management requirements are met. Provide technical knowledge and information assurance analysis support, to include security assessment of applications; operating systems; internet-facing interfaces, intranet and other interconnections. Strong knowledge of best practices associated with as well as appropriate authoritative guidance for physical security; network security; security risk assessments; critical infrastructure protection; continuity and contingency planning; emergency preparedness; security awareness and training. Provide analysis of existing systems vulnerabilities including possible intrusion/entry points, resource manipulation, denial of service, and/or destruction of resources. Provide technical support and analysis to document organizational information protection framework, and support policy and procedures preparation and implementation.

Minimum Education: Undergraduate degree from an accredited institution or equivalent technical qualification. Five (5) years of relevant experience is acceptable in lieu of a degree.

6 Commercial Job Title: Cyber Analyst – Junior Technical Qualifications/Experience: Minimum zero to one (0-1) year of experience in defining, implementing and maintaining the information security for businesses, business units, divisions, organizations, agencies, etc. Must have strong knowledge of encryption, intrusion detection/prevention, network security, and ethical hacking/penetration testing.

Functional Responsibility: Responsible for ensuring that the organization’s networks, as well as information, is secure. Employ continuous monitoring of intrusion detection/prevention and other perimeter defense devices. Ensure appropriate data encryption (in transit and at rest) levels based on protection needs of targeted data. Maintain awareness of system/network security posture to include vulnerability scanning to facilitate application of quick and effective corrective measures, while ensuring configuration management requirements are met. Provide technical knowledge and information assurance analysis support, to include security assessment of applications; operating systems; internet-facing interfaces, intranet and other interconnections. Strong knowledge of best practices associated with as well as appropriate authoritative guidance for physical security; network security; security risk assessments; critical infrastructure protection;
continuity and contingency planning; emergency preparedness; security awareness and training. Provide analysis of existing systems vulnerabilities including possible intrusion/entry points, resource manipulation, denial of service, and/or destruction of resources. Provide technical support and analysis to document organizational information protection framework, and support policy and procedures preparation and implementation.

Minimum Education: Undergraduate degree from an accredited institution or equivalent technical qualification. Three (3) years of relevant experience is acceptable in lieu of a degree.

7 Commercial Job Title: Cyber Engineer – Senior Technical Qualifications/Experience: Minimum five (5) years of experience in defining, implementing and maintaining the information security of firms. Must have a strong know-how of encryption, intrusion detection, network security and ethical hacking.

Functional Responsibility: Responsible for defining/ameliorating the IS Policy, including the Disaster Recovery Policy for client organizations. Also responsible for ensuring that the organization networks as well as information is secure at all times by constantly monitoring intrusion detection, data encryption, and taking quick and effective corrective measures in the event of a breach. Provide technical knowledge and analysis of information assurance, to include applications; operating systems; Internet and Intranet; physical security; networks; risk assessment; critical infrastructure continuity and contingency planning; emergency preparedness; security awareness and training. Provide analysis of existing system’s vulnerability to possible intrusions, resource manipulation, resource denial and destruction of resources. Provide technical support and analysis to document organizational information protection framework, and supports policy and procedures preparation and implementation. Monitors firewall logs. Analyze the client system security, conducts gap analysis, determines enterprise information security standards, and develops and implements information security standards and procedures. Ensure that all information systems are functional and secure.

Minimum Education: Undergraduate degree from an accredited institution or equivalent technical qualification. Seven (7) years of relevant experience is acceptable in lieu of a degree.

8 Commercial Job Title: Cyber Engineer – Intermediate Technical Qualifications/Experience: Minimum three (3) years of experience in defining, implementing and maintaining the information security of firms. Must have a strong know-how of encryption, intrusion detection, network security and ethical hacking.

Functional Responsibility: Responsible for defining/ameliorating the IS Policy, including the Disaster Recovery Policy for client organizations. Also responsible for ensuring that the organization networks as well as information is secure at all times by constantly monitoring intrusion detection, data encryption, and taking quick and effective corrective measures in the event of a breach. Provide technical knowledge and analysis of information assurance, to include applications; operating systems; Internet and Intranet; physical security; networks; risk assessment; critical infrastructure continuity and contingency planning; emergency preparedness; security awareness and training. Provide analysis of existing system’s vulnerability to possible intrusions, resource manipulation, resource denial and destruction of resources. Provide technical support and analysis to document organizational information protection framework, and supports policy and procedures preparation and implementation. Monitors firewall logs. Analyze the client system security, conduct gap analysis, determine enterprise information security standards, and develop and implement information security standards and procedures. Ensure that all information systems are functional and secure.

Minimum Education: Undergraduate degree from an accredited institution or equivalent technical qualification. Five (5) years of relevant experience is acceptable in lieu of a degree.

9 Commercial Job Title: Cyber Engineer – Junior Technical Qualifications/Experience: Minimum zero to one (0-1) year of experience in defining, implementing and maintaining the information security of firms. Must have a strong know-how of encryption, intrusion detection, network security and ethical hacking.
**Functional Responsibility:** Responsible for defining/ameliorating the IS Policy, including Disaster Recovery Policy for client organizations. Also responsible for ensuring that the organization networks as well as information is secure at all times by constantly monitoring intrusion detection, data encryption, and taking quick and effective corrective measures in the event of a breach. Provide technical knowledge and analysis of information assurance, to include applications; operating systems; Internet and Intranet; physical security; networks; risk assessment; critical infrastructure continuity and contingency planning; emergency preparedness; security awareness and training. Provide analysis of existing system’s vulnerability to possible intrusions, resource manipulation, resource denial and destruction of resources. Provide technical support and analysis to document organizational information protection framework, and supports policy and procedures preparation and implementation. Monitors firewall logs. Provide system administration of Network, Web, and/or communications systems, including Local Area Network (LAN), Wide Area Network (WAN). Maintain servers, creates monitoring reports and logs and ensure functionality of links.

**Minimum Education:** Undergraduate degree from an accredited institution or equivalent technical qualification. Three (3) years of relevant experience is acceptable in lieu of a degree.

**Commercial Job Title Cyber Subject Matter Expert:** Technical Qualifications/Experience: Minimum six (6) years of experience in defining, implementing and maintaining the information security of firms. Must have strong know-how of encryption, intrusion detection, network security and ethical hacking.

**Functional Responsibility:** Responsible for defining the IS Policy of an organization. Also responsible for ensuring that the organization networks as well as information is secure at all times, constantly monitoring the intrusion detection, data encryption, and for taking quick and effective corrective measures in the event of a breach. Provide technical knowledge and analysis of information assurance, to include applications; operating systems; Internet and Intranet; physical security; networks; risk assessment; critical infrastructure continuity and contingency planning; emergency preparedness; security awareness and training. Provide analysis of existing system's vulnerability to possible intrusions, resource manipulation, resource denial and destruction of resources. Provide technical support and analysis to document organizational information protection framework, and supports policy and procedures preparation and implementation. Monitor firewall logs. Provide system administration of Network, Web, and/or communications systems, including Local Area Network (LAN), Wide Area Network (WAN). Maintain servers, creates monitoring reports and logs and ensure functionality of links.

**Minimum Education:** Undergraduate degree from an accredited institution or equivalent technical qualification. Eight (8) years of relevant experience is acceptable in lieu of a degree.

---

**SIN 54151S LABOR CATEGORY DESCRIPTIONS**

1. **Commercial Job Title: Analyst (Business/System/Data) Technical Qualifications/Experience:** Overall six (6) years of experience in analyzing the business processes, data and information systems of organizations, mentoring other Business/System Analysts, coordinating and supporting the development, enhancement, and maintenance of products and services applicable to multiple lines of a customer’s business using information technology.

**Functional Responsibility:** Perform information technology analysis activities to support business decisions relative to the development, enhancement, and maintenance of products and services applicable to multiple lines of business. Responsible for technically analyzing business processes, data and/or information systems, including analysis of system architecture and associated hardware/software, e.g., functional implementation of each application, database(s), platform(s), etc. Data analysis, including reliability, integrity, etc., associated processes, business logic, etc., is also included. Anticipate and identify user problems and needs. Recommend business solutions based on analysis activities, customer requirements, industry trends, and best practices.
practices/authoritative guidance. Lead, plan, schedule, and control complex projects and activities with customers, support groups, and vendors on concurrent projects. Apply extensive business and industry knowledge to develop project specifications. Advise on methods to improve business processes and remove non-value added activities. Coordinate and participate in proposals, feasibility studies, implementations, and new business development. Lead training activities for knowledge transfer, and build relationships with multiple customer/business levels.

Minimum Education: Bachelor’s degree in Computer Sciences, Information Systems, Business, Mathematics or Engineering (Electrical, Computer, Mechanical) or related degree. Candidates having a bachelor’s degree in disciplines other than those listed above may be considered if and only if they have at least eight (8) years of experience in analyzing the business processes and information systems of organizations.

2 Commercial Job Title: Application Analyst Technical Qualifications/Experience: Overall three (3) years of experience in analyzing the software applications for their functionality, monitoring performance, identifying bottlenecks and recommending measures to improve application performance.

Functional Responsibility: Work with Software Design and Development groups to analyze software applications for functionality, performance and integration with other systems. Monitor application performance, identify bottlenecks and recommend measures to improve application performance.

Minimum Education: Bachelor’s degree in Computer Sciences, Information Systems, Business, Mathematics or Engineering (Electrical, Computer, Mechanical) or related degree. Candidates having a bachelor’s degree in disciplines other than those listed above may also be considered if and only if they have at least four (4) years of experience in analyzing the software applications of organizations.

3 Commercial Job Title: Application Developer – Senior Technical Qualifications/Experience: Minimum six (6) years of experience in supervising and mentoring other Application Developers in the performance of detailed analysis, building software development tools and producing highly technical programs such as cross-compilers and communications software operating systems. Must be proficient in programming in the relevant programming language/s, e.g., Java, XML, .Net, Web Methods, C, C++, Perl, COBOL, Oracle PL/SQL, Unix Shell scripting.

Functional Responsibility: Lead business logic and data modeling activities associated with application development. Direct the activities of programmers and analysts in the performance of detailed analysis, building software development tools and in producing highly technical programs such as cross-compilers and communications software operating systems. Responsible for measuring software performance through project design, implementation and evaluation of results. Supervise and participate in the development of manuals and user guides for programmers and operating staff. Establish and supervise software design efforts necessary to integrate new hardware and code programs in applicable languages using standard requirements documentation, e.g., detailed flow diagrams, input/output descriptions, performance specifications, etc. Supervise software analysis, the development of program specifications and the development of program code. Perform implementation tasks and direct the conduct of application testing to insure results. Direct and participate in the development of manuals and user guides for programmers and operating staff.

Minimum Education: Bachelor’s degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor’s degree in disciplines other than those listed above may also be considered if and only if they have at least eight (8) years of experience in supervising and mentoring Application Developers in the performance of detailed analysis, building software development tools, and producing highly technical programs such as cross-compilers and communications software operating systems.

4 Commercial Job Title: Application Developer – Mid Technical Qualifications/Experience: Minimum four (4) years of experience in independently developing and testing various mission critical applications and
implementation of information processing systems and applications that use current operating systems, programming languages and applications development tools, computer systems, multi-programming technology, database management techniques, and data communications protocol. Must be skilled in programming in the relevant programming language(s) (Java, XML, .Net, Web Methods, C, C++, Perl, COBOL, Oracle PL/SQL, Unix Shell scripting).

Functional Responsibility: Assist in the logic behind and the data modeling associated with application development. Perform the development and/or programming, and implementation of information processing systems and applications that use current operating systems, programming languages and applications development tools, computer systems, multi-programming technology, database management techniques, and data communications protocol. Work independently in support of joint applications development efforts. Responsible for writing application software, data manipulation, databases programming, testing and implementation, technical and user documentation, software conversions; environments include, but are not limited to, mainframe, mid-range, personal computers, laptops, mobile devices, and other emerging technology platforms.

Minimum Education: Bachelor’s degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor’s degree in disciplines other than those listed above may also be considered if and only if they have at least six (6) years of experience in independently developing industry applications.

5 Commercial Job Title: Application Developer – Junior Technical Qualifications/Experience: Minimum two (2) years of experience in independently developing and testing various mission critical applications and implementation of information processing systems and applications that use current operating systems, programming languages and applications development tools, computer systems, multi-programming technology, database management techniques, and data communications protocol. Must be skilled in programming in the relevant programming language(s) (Java, XML, .Net, Web Methods, C, C++, Perl, COBOL, Oracle PL/SQL, Unix Shell scripting).

Functional Responsibility: Assist in the logic behind and the data modeling associated with application development. Perform the development and/or programming, and implementation of information processing systems and applications that use current operating systems, programming languages and applications development tools, computer systems, multi-programming technology, database management techniques, and data communications protocol. Work independently in support of joint applications development efforts. Responsible for writing application software, data manipulation, databases programming, testing and implementation, technical and user documentation, software conversions; environments include, but are not limited to, mainframe, mid-range, personal computers, laptops, mobile devices, and other emerging technology platforms.

Minimum Education: Bachelor’s degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor’s degree in disciplines other than those listed above may also be considered if and only if they have at least six (6) years of experience in independently developing industry applications.

6 Commercial Job Title: Application Integration Specialist Technical Qualifications/Experience: Minimum six (6) years of technical experience with the integration of multi-vendor software and hardware components in Client/Server, LAN and WAN environments. Requires competence in software and hardware implementation, analysis techniques, concepts and methods. Has the proven ability to work well independently with minimal supervision.

Functional Responsibility: Provide computer systems expertise relative to automated information system(s) integration with existing infrastructure, architecture, and/or other systems. Perform systems analysis, alternative solutions, and design of technical and business solutions. Under minimal guidance and supervision,
conduct project feasibility and implementation studies, including the development project plans, testing methodologies/plans, and overarching project management documentation. Develop and implement data conversion routines. Perform/direct system testing to insure satisfactory results within requirements. Duties require knowledge of data sources, data flow, system interactions, computer equipment, including hardware and software applications. Provide technical support to the project team. Establish and maintain development, testing environments and configuration management processes and structures. Serve as primary point-of-contact for third party software and hardware vendors.

Minimum Education: Bachelor’s degree in Computer Science, Information Systems, Engineering, Business, Economics, or Mathematics. Candidates having a bachelor’s degree in disciplines other than those listed above may also be considered if they have at least eight (8) years of experience with the integration of multi-vendor software and hardware components in Client/Server, LAN and WAN environments, software and hardware implementation, analysis techniques, concepts and methods.

7 Commercial Job Title: Certification Specialist – Senior Technical Qualifications/Experience: Overall six (6) years of experience in assessing, analyzing, evaluating, validating, certifying and accrediting, etc., various businesses, systems, software development processes, etc., relative to one or more compliance standard, security controls/requirements, etc.

Functional Responsibility: Responsible for evaluating various businesses, systems, software development processes, etc., validating against standard requirements and/or compliance controls, e.g., ISO, CMMI, HIPAA/HITECH, NIST, DIACAP, DODIIS/DCID, CNSS, ICD 503, etc. Responsible for assisting in the scoping effort relative to the target compliance activity. Assist in the development of the compliance methodology based on experience as well as best practices associated with target compliance activity. Document tasks to justify compliance, bring target into compliance (both technically and non), and present compliance package for approval by clients and/or approval chains as is appropriate. Analyze and evaluate the security requirements/controls in an organization, validating them with standard security guidelines and policies, and certifying that all information systems are compliant with standard security guidelines.

Minimum Education: Bachelor’s degree in Computer Sciences, Information Systems, Mathematics, Engineering or related field. Candidates having a bachelor’s degree in disciplines other than those listed above may be considered if and only if they have at least four (4) years of relevant experience.

8 Commercial Job Title: Certification Specialist – Mid Technical Qualifications/Experience: Overall three (3) years of experience in assessing, analyzing, evaluating, validating, certifying and accrediting, etc., various businesses, systems, software development processes, etc., relative to one or more compliance standard, security controls/requirements, etc.

Functional Responsibility: Responsible for evaluating various businesses, systems, software development processes, etc., validating against standard requirements and/or compliance controls, e.g., ISO, CMMI, HIPAA/HITECH, NIST, DIACAP, DODIIS/DCID, CNSS, ICD 503, etc. Responsible for assisting in the scoping effort relative to the target compliance activity. Assist in the development of the compliance methodology based on experience as well as best practices associated with target compliance activity. Document tasks to justify compliance, bring target into compliance (both technically and non), and present compliance package for approval by clients and/or approval chains as is appropriate. Analyze and evaluate the security requirements/controls in an organization, validating them with standard security guidelines and policies, and certifying that all information systems are compliant with standard security guidelines.

Minimum Education: Bachelor’s degree in Computer Sciences, Information Systems, Mathematics, Engineering or related field. Candidates having a bachelor’s degree in disciplines other than those listed above may be considered if and only if they have at least four (4) years of relevant experience.
9  **Commercial Job Title:** Certification Specialist – Junior  
Technical Qualifications/Experience: Overall one (1) year of experience in assessing, analyzing, evaluating, validating, certifying and accrediting, etc., various businesses, systems, software development processes, etc., relative to one or more compliance standard, security controls/requirements, etc.

Functional Responsibility: Responsible for evaluating various businesses, systems, software development processes, etc., validating against standard requirements and/or compliance controls, e.g., ISO, CMMI, HIPAA/HITECH, NIST, DIACAP, DODIIS/DCID, CNSS, ICD 503, etc. Responsible for assisting in the scoping effort relative to the target compliance activity. Assist in the development of the compliance methodology based on experience as well as best practices associated with target compliance activity. Document tasks to justify compliance, bring target into compliance (both technically and non), and present compliance package for approval by clients and/or approval chains as is appropriate. Analyze and evaluate the security requirements/controls in an organization, validating them with standard security guidelines and policies, and certifying that all information systems are compliant with standard security guidelines.

Minimum Education: Bachelor’s degree in Computer Sciences, Information Systems, Mathematics, Engineering or related degree. Candidates having a bachelor’s degree in disciplines other than those listed above may be considered if and only if they have at least four (4) years of relevant experience.

10  **Commercial Job Title:** Computer System Security Specialist  
Technical Qualifications/Experience: Minimum three (3) years of experience in defining, implementing and maintaining the information security for businesses, business units, divisions, organizations, agencies, etc. Must have strong knowledge of encryption, intrusion detection/prevention, network security, and ethical hacking/penetration testing.

Functional Responsibility: Responsible for ensuring that the organization’s networks, as well as information, is secure. Employ continuous monitoring of intrusion detection/prevention and other perimeter defense devices. Ensure appropriate data encryption (in transit and at rest) levels based on protection needs of targeted data. Maintain awareness of system/network security posture to include vulnerability scanning to facilitate application of quick and effective corrective measures, while ensuring configuration management requirements are met. Provide technical knowledge and information assurance analysis support, to include security assessment of applications; operating systems; internet-facing interfaces, intranet and other interconnections. Strong knowledge of best practices associated with as well as appropriate authoritative guidance for physical security; network security; security risk assessments; critical infrastructure protection; continuity and contingency planning; emergency preparedness; security awareness and training. Provide analysis of existing systems vulnerabilities including possible intrusion/entry points, resource manipulation, denial of service, and/or destruction of resources. Provide technical support and analysis to document organizational information protection framework, and support policy and procedures preparation and implementation.

Minimum Education: Bachelor’s degree in Computer Sciences, Information Systems, Mathematics, Engineering, or related field. Candidates having a bachelor’s degree in disciplines other than those listed above may also be considered if and only if they have at least five (5) years of experience in analyzing, designing, implementing, integrating and maintaining computer/information systems security postures.

11  **Commercial Job Title:** Configuration Management Specialist  
Technical Qualifications/Experience: Minimum four (4) years of general IT experience, with three (3) years of specialized experience in Configuration Management, Version Control, Process Improvement, Activity/Process Modeling. Must be familiar with one or more of the Configuration Tools like Clearcase, PVCS, Endevor, CMVC, Visual SourceSafe, or other CM tool.

Functional Responsibility: Support the development and maintenance of configuration management plans, processes, procedures, etc., and scheduling, and documenting configuration management reviews. Shall be capable of monitoring the configuration control process and ensuring that procedures comply with client
and/or applicable specifications. Requires minimal supervision; however overarching strategic direction must be provided. Knowledgeable of software development techniques, change control processes, configuration audits and client/government regulations, manuals, technical orders, standards and industry publications related to configuration/data management required to perform the task.

Minimum Education: Bachelor’s degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor’s degree in disciplines other than those listed above may also be considered if and only if they have at least five (5) years of experience in performing configuration management and version control tasks.

12 Commercial Job Title: Database Administrator Technical Qualifications/Experience: Five (5) years of general experience including two (2) years specialized experience. Serves in a supervisory manner, has responsibility for junior staff tasking/development, also serves as a management interface. Two of the five years of experience must include providing direction to personnel performing database administration tasks and technical expertise in using at least one of the following DBMS products relevant to the specific task: IMS, DB2, ADABAS, ORACLE, SYBASE, SQL Server, INGRES or similar.

Functional Responsibility: Responsible for building/installing databases on servers/clients. Maintain and create users, nodes, instances, databases, tablespaces, containers, bufferpools and logs. Migrate data between databases. Extract data from one system into flat files and then load into the database without constraints. Write stored procedures, and triggers to populate data from non-constraints tables to normalized tables with constraints. Tune the database manager configuration, database configuration parameters like bufferpools, shared memory variables, I/O variables, application heap, database heap size, logs and sort area to increase performance of the system. Analyze the execution path of the query to determine the cost, indexing and cardinality. Write scripts to create instances, databases, scheduling online, offline backups and restoring databases. Implement Active Standby Clustering, database partitioning using utilities. Provide highly technical expertise and guidance in the design, implementation, operation and maintenance of database management systems (DBMS). Evaluate and recommend available DBMS products after matching requirements with system capabilities. Determine file organization, indexing methods, and security procedures for specific applications. Control the design and use of databases. Control the global view of databases, control the access to the databases, assure the safekeeping of the databases (from accidental or intentional damage or loss), and monitor the use of databases. Must be capable of defining all required database administration policies, procedures, standards, and guidelines. Is an authority on the design of databases and the use of database management systems. Evaluate and recommend available DBMS products after matching requirements with system capabilities. Prepare and deliver presentations on DBMS concepts.

Minimum Education: Bachelor’s degree in Computer Sciences, Information Systems, Mathematics, Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor’s degree in disciplines other than those listed above may also be considered if they have at least seven (7) years of experience in database administration.

13 Commercial Job Title: Database Designer Technical Qualifications/Experience: Minimum five (5) years of experience in analyzing and designing databases (Oracle, MS SQL, DB2, DMS, Sybase).

Functional Responsibility: Responsible for designing the database. This includes the design of the tables, fields, screens, triggers and stored procedures so as to optimize the database performance (efficiency, reliability, scalability). Analyze the database systems and programs, which include access methods, access time, file structures, device allocation, validation checks, statistical methods, and security. Will also work with the user community to understand data access and integration needs, ensure integration of systems through the database structure, perform data modeling, monitor database standards and procedures, system usage and performance, troubleshoot and resolve database and data problems, and develop and administer disaster recovery plans.
Minimum Education: Bachelor’s degree in Computer Sciences, Information Systems, Mathematics, Engineering (Electrical, Computer, Mechanical) or related degree. Candidates having a bachelor’s degree in disciplines other than those listed above may also be considered if they have at least seven (7) years of experience analyzing and designing databases.

14 Commercial Job Title: Enterprise Architect – Senior Technical Qualifications/Experience: Minimum six (6) years of experience in enterprise system architecture.

Functional Responsibility: Contribute to the establishment and maintenance of an overall IT architecture relevant to and consistent with business and technology direction and objectives. Develop information technology technical and application architectures and participate in setting technology direction and standards. Provide technical architectural design review for major business applications and technology initiatives. Facilitate linkage with key business areas by understanding enterprise requirements and by communicating architecture frameworks best practices and standards. Develop recommendations and requirements for legacy applications to evolve towards conformance with target architecture. Continually review applications, workflow, systems, and network management and network infrastructure, for opportunities to improve effectiveness and efficiency.

Minimum Education: Bachelor’s degree in Computer Sciences, Information Systems, Mathematics, Engineering or related field. A degree in disciplines other than those listed above may also be considered if and only if they have at least six (6) years of relevant experience.

15 Commercial Job Title: Enterprise Architect – Mid Technical Qualifications/Experience: Minimum four (4) years of experience in enterprise system architecture.

Functional Responsibility: Contribute to the establishment and maintenance of an overall IT architecture relevant to and consistent with business and technology direction and objectives. Develop IT technical and application architectures and participate in setting technology direction and standards. Provide technical architectural design review for major business applications and technology initiatives. Facilitate linkage with key business areas by understanding enterprise requirements and by communicating architecture frameworks best practices and standards. Develop recommendations and requirements for legacy applications to evolve towards conformance with target architecture. Continually review applications, workflow, systems, and network management and network infrastructure, for opportunities to improve effectiveness and efficiency.

Minimum Education: Bachelor’s degree in Computer Sciences, Information Systems, Mathematics, Engineering or related field. A degree in disciplines other than those listed above may also be considered if and only if they have at least six (6) years of relevant experience.

16 Commercial Job Title: Enterprise Architect – Junior Technical Qualifications/Experience: Minimum two (2) years of experience in enterprise system architecture.

Functional Responsibility: Support the Enterprise Architect in designing and maintaining overall enterprise system architecture relevant to and consistent with business and technology direction and objectives. Under the guidance of the Enterprise Architect, facilitate linkage with key business areas by understanding enterprise requirements and by communicating architecture frameworks best practices and standards. Must have a basic understanding of networking architectures.

Minimum Education: Bachelor’s degree in Computer Sciences, Information Systems, Mathematics, Engineering or related field. A degree in disciplines other than those listed above may also be considered if and only if they have at least four (4) years of relevant experience.

17 Commercial Job Title: Help Desk Analyst Technical Qualifications/Experience: Minimum two (2) years of experience in providing help desk support on various problems and issues related to application software,
information systems and processes support functions such as assisting users and system developers with issues and problems in system operation.

**Functional Responsibility:** Responsible for providing first and second level help desk support to solve problems related to the operations and performance of software applications, operating systems, databases, networks and functional understanding. Provide software support functions like code maintenance, backups, functionality modifications, reports generation, modify/upgrade software documentation, user training, software migrations, version control, technical support and user training.

**Minimum Education:** Bachelor’s degree in Computer Sciences, Information Systems, Mathematics or Engineering or a related field. A degree in disciplines other than those listed above may also be considered if and only if they have at least six (6) years of relevant experience.

### 18 Commercial Job Title: Information Assurance Engineer – Senior

**Technical Qualifications/Experience:** Minimum six (6) years of experience in defining IS Security policies, analyzing, designing, implementing, integrating and maintaining the information security of firms.

**Functional Responsibility:** Analyze and define security requirement for computer systems which may include mainframes, workstations, and personal computers. Design, develop, engineer, and implement solutions that meet security requirements. Provide integration and implementation of the computer system security solution. Establish and satisfy complex system-wide information security requirements based upon the analysis of user, policy, regulatory, and resource demands. Support customers at the highest levels in the development and implementation of doctrine and policies. Apply know-how to government and commercial common user systems, as well as to dedicated special purpose systems requiring specialized security features and procedures.

**Minimum Education:** Bachelor’s degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor’s degree in disciplines other than those listed above will also be considered if and only if they have at least six (6) years of experience in analyzing, designing, implementing, integrating and maintaining the Information Security of firms.

### 19 Commercial Job Title: Information Assurance Engineer – Mid

**Technical Qualifications/Experience:** Minimum three (3) years of experience in documenting and analyzing IS security policies, implementing, integrating and maintaining the information security of firms.

**Functional Responsibility:** Analyze and define security requirement for computer systems which may include mainframes, workstations, and personal computers. Design, develop, engineer, and implement solutions that meet security requirements. Provide integration and implementation of the computer system security solution. Establish and satisfy complex system-wide information security requirements based upon the analysis of user, policy, regulatory, and resource demands. Support customers at the highest levels in the development and implementation of doctrine and policies. Apply know-how to government and commercial common user systems, as well as to dedicated special purpose systems requiring specialized security features and procedures.

**Minimum Education:** Bachelor’s degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor’s degree in disciplines other than those listed above may also be considered if and only if they have at least five (5) years of experience in analyzing, designing, implementing, integrating and maintaining the information security of firms.

### 20 Commercial Job Title: Information Assurance Engineer – Junior

**Technical Qualifications/Experience:** Minimum two (2) years of experience in documenting and analyzing IS security policies, implementing, integrating and maintaining the information security of firms.
Functional Responsibility: Support the Information Assurance Engineer in implementing, and maintaining the 
information systems security policies and procedures previously defined by the Information Assurance 
Engineer along with the Technical Management of large organizations. Implement solutions that meet security 
requirements. Provide integration and implementation of the computer system security solution. Apply know‐
how to government and commercial common user systems, as well as to dedicated special purpose systems 
requiring specialized security features and procedures.

Minimum Education: Bachelor’s degree in Computer Sciences, Information Systems, Mathematics or 
Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor’s degree in 
disciplines other than those listed above may also be considered if and only if they have at least four (4) years 
of experience in analyzing, designing, implementing, integrating and maintaining the Information Security of 
firms.

21  Commercial Job Title: Information Security Analyst – Senior Technical Qualifications/Experience: 
Minimum eight (8) years of experience in analyzing computer security at large firms, conducting gap analysis, 
identifying and alleviating potential loopholes.

Functional Responsibility: Analyze the client system security, conduct gap analysis, determine enterprise 
information security standards, and develop and implement information security standards and procedures. 
Ensure that all information systems are functional and secure.

Minimum Education: Bachelor’s degree in Computer Sciences, Information Systems, Mathematics or 
Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor’s degree in 
disciplines other than those listed above may also be considered if and only if they have at least seven (7) years 
of experience in analyzing computer security at large firms.

22  Commercial Job Title: Information Security Analyst – Mid Technical Qualifications/Experience: Minimum 
five (5) years of experience in analyzing computer security at large firms, conducting gap analysis, identifying 
and alleviating potential loopholes.

Functional Responsibility: Analyze the client system security, conduct gap analysis, determines enterprise 
information security standards, and develop and implement information security standards and procedures. 
Ensure that all information systems are functional and secure.

Minimum Education: Bachelor’s degree in Computer Sciences, Information Systems, Mathematics or 
Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor’s degree in 
disciplines other than those listed above will also be considered if and only if they have at least seven (7) years 
of experience in analyzing computer security at large firms.

23  Commercial Job Title: Information Security Analyst – Junior Technical Qualifications/Experience: Minimum 
one (1) year of experience in analyzing computer security at large firms, conducting gap analysis, identifying 
and alleviating potential loopholes.

Functional Responsibility: Support the Information Security Analysts. Analyze the client system security, 
conduct gap analysis, determine enterprise information security standards, and develop and implement 
information security standards and procedures.

Minimum Education: Bachelor’s degree in Computer Sciences, Information Systems, Mathematics or 
Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor’s degree in 
disciplines other than those listed above may also be considered if and only if they have at least four (4) years 
of experience in analyzing computer security at large firms.

24  Commercial Job Title: Information Security Engineer – Senior Technical Qualifications/Experience: 
Minimum eight (8) years of experience in defining, implementing and maintaining the information security of 
firms. Must have a strong know-how of encryption, intrusion detection, network security and ethical hacking.
**Functional Responsibility:** Responsible for defining/ameliorating the IS Policy, including the Disaster Recovery Policy for client organizations. Also responsible for ensuring that the organization networks as well as information is secure at all times by constantly monitoring intrusion detection, data encryption, and taking quick and effective corrective measures in the event of a breach. Provide technical knowledge and analysis of information assurance, to include applications; operating systems; Internet and Intranet; physical security; networks; risk assessment; critical infrastructure continuity and contingency planning; emergency preparedness; security awareness and training. Provide analysis of existing system’s vulnerability to possible intrusions, resource manipulation, resource denial and destruction of resources. Provide technical support and analysis to document organizational information protection framework, and supports policy and procedures preparation and implementation. Monitors firewall logs. Analyze the client system security, conducts gap analysis, determines enterprise information security standards, and develops and implements information security standards and procedures. Ensure that all information systems are functional and secure.

**Minimum Education:** Bachelor’s degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor’s degree in disciplines other than those listed above may also be considered if and only if they have at least eight (8) years of experience in defining, implementing and maintaining the information security of firms.

25 **Commercial Job Title:** Information Security Engineer – Mid **Technical Qualifications/Experience:** Minimum five (5) years of experience in defining, implementing and maintaining the information security of firms. Must have a strong know-how of encryption, intrusion detection, network security and ethical hacking.

**Functional Responsibility:** Responsible for defining/ameliorating the IS Policy, including the Disaster Recovery Policy for client organizations. Also responsible for ensuring that the organization networks as well as information is secure at all times by constantly monitoring intrusion detection, data encryption, and taking quick and effective corrective measures in the event of a breach. Provide technical knowledge and analysis of information assurance, to include applications; operating systems; Internet and Intranet; physical security; networks; risk assessment; critical infrastructure continuity and contingency planning; emergency preparedness; security awareness and training. Provide analysis of existing system’s vulnerability to possible intrusions, resource manipulation, resource denial and destruction of resources. Provide technical support and analysis to document organizational information protection framework, and supports policy and procedures preparation and implementation. Monitors firewall logs. Analyze the client system security, conduct gap analysis, determine enterprise information security standards, and develop and implement information security standards and procedures. Ensure that all information systems are functional and secure.

**Minimum Education:** Bachelor’s degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor’s degree in disciplines other than those listed above may also be considered if and only if they have at least eight (8) years of experience in defining, implementing and maintaining the information security of firms.

26 **Commercial Job Title:** Information Security Engineer – Junior **Technical Qualifications/Experience:** Minimum two (2) years of experience in defining, implementing and maintaining the information security of firms. Must have a strong know-how of encryption, intrusion detection, network security and ethical hacking.

**Functional Responsibility:** Responsible for defining/ameliorating the IS Policy, including Disaster Recovery Policy for client organizations. Also responsible for ensuring that the organization networks as well as information is secure at all times by constantly monitoring intrusion detection, data encryption, and taking quick and effective corrective measures in the event of a breach. Provide technical knowledge and analysis of information assurance, to include applications; operating systems; Internet and Intranet; physical security; networks; risk assessment; critical infrastructure continuity and contingency planning; emergency preparedness; security awareness and training. Provide analysis of existing system’s vulnerability to possible intrusions, resource manipulation, resource denial and destruction of resources. Provide technical support and
analysis to document organizational information protection framework, and supports policy and procedures preparation and implementation. Monitors firewall logs. Provide system administration of Network, Web, and/or communications systems, including Local Area Network (LAN), Wide Area Network (WAN). Maintain servers, creates monitoring reports and logs and ensure functionality of links.

**Minimum Education:** Bachelor’s degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor’s degree in disciplines other than those listed above may also be considered if and only if they have at least ten (10) years of experience in defining, implementing and maintaining the information security of firms.

**Commercial Job Title:** Information System Security Specialist

**Technical Qualifications/Experience:**
Minimum ten (10) years of experience in defining, implementing and maintaining the information security of firms. Must have strong know-how of encryption, intrusion detection, network security and ethical hacking.

**Functional Responsibility:** Responsible for defining the IS Policy of an organization. Also responsible for ensuring that the organization networks as well as information is secure at all times, constantly monitoring the intrusion detection, data encryption, and for taking quick and effective corrective measures in the event of a breach. Provide technical knowledge and analysis of information assurance, to include applications; operating systems; Internet and Intranet; physical security; networks; risk assessment; critical infrastructure continuity and contingency planning; emergency preparedness; security awareness and training. Provide analysis of existing system's vulnerability to possible intrusions, resource manipulation, resource denial and destruction of resources. Provide technical support and analysis to document organizational information protection framework, and supports policy and procedures preparation and implementation. Monitor firewall logs. Provide system administration of Network, Web, and/or communications systems, including Local Area Network (LAN), Wide Area Network (WAN). Maintain servers, creates monitoring reports and logs and ensure functionality of links. Establish backups and monitor site security.

**Minimum Education:** Bachelor’s degree in Computer Sciences, Information Systems, Mathematics or Engineering or related field. A degree in disciplines other than those listed above may also be considered if and only if they have at least fourteen (14) years of relevant experience.

**Commercial Job Title:** Internet Developer – Senior

**Technical Qualifications/Experience:** Minimum eight (8) years of experience in leading the analyzing systems and developing and Internet/Intranet applications in .Net, XML, Java, EJB and Java Script and deploying the applications on the Application Servers like WebLogic, WebSphere and iPlanet. Must be proficient with Web Architecture and Development Methodologies.

**Functional Responsibility:** Lead a team of Internet Developers. Analyze, design, develop and test internet applications using languages like Microsoft .Net, Java, XML, JSP, EJB and JavaScript and deploy the applications on the Application Servers like WebLogic, WebSphere and iPlanet. Responsible for unit testing, code review, preparing technical and user documentation.

**Minimum Education:** Bachelor’s degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical).

**Commercial Job Title:** Internet Developer – Mid

**Technical Qualifications/Experience:** Minimum four (4) years of experience in independently analyzing web systems and developing Internet/Intranet applications in .Net, XML, Java, EJB and Java Script and deploying the applications on the Application Servers like WebLogic, WebSphere and iPlanet. Must be proficient in one or more of .Net, Java, HTML, DHTML, JavaScript, CGI, Cold Fusion, COM/DCOM, and CORBA.

**Functional Responsibility:** Analyze, understand the architecture and develop Internet applications using languages like Microsoft .Net, Java, XML, JSP, EJB and JavaScript and deploying the applications on the Application Servers like WebLogic, WebSphere and iPlanet. Also responsible for writing interfaces, developing
stored Procedures, Triggers and Views, Unit testing and code review. Can work independently in support of a joint applications development effort.

**Minimum Education:** Bachelor’s degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor’s degree in disciplines other than those listed above may also be considered if and only if they have at least six (6) years of experience in independently developing industry internet/web applications.

**30 Commercial Job Title:** IT Subject Matter Expert

**Technical Qualifications/Experience:** Minimum five (5) years of experience in studying, analyzing, evaluating, designing and improving specific programs and business processes (example: expertise in Naval Air Defense Systems, Child Support Programs, Teachers Licensing Programs, CFR validation, Treasury Systems, Driver Licensing Systems, Housing Loan Programs or any other program critical to designing/improving the Information Systems), help define the Software Requirement Specifications and Business Process Documents and assist the System Architect in developing the system architecture.

**Functional Responsibility:** Responsible for serving as facilitator for Integrated Product Team, defining/ameliorating the policies and procedures of an organization, process or program. Utilize their specialization and subject matter knowhow to assist the business analysts and Project Managers in defining the Software Requirement Specifications and Business Process Documents and assist the System Architect in developing the system architecture. Also assist the testing team in integrated system testing to ensure that the system is working under various conditions/scenarios critical for the program or the application.

**Minimum Education:** Bachelor’s degree in Computer Sciences, Information Systems, Mathematics, Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor’s degree in disciplines other than those listed above may also be considered if and only if they have at least nine (9) years of experience working with the functional and technical aspects of various programs like Naval Air Defense Systems, Child Support Programs, Teachers Licensing Programs, CFR validation, Treasury Systems, Driver Licensing Systems, Housing Loan Programs or any other program critical to designing/improving the information systems.

**31 Commercial Job Title:** IT Technologist

**Technical Qualifications/Experience:** Minimum four (4) years of technical experience in IT systems, and Application Integration.

**Functional Responsibility:** Responsible for ensuring a stable and usable system through the integration of various software and hardware platforms and components. Provide technical support to the project team. Establish and maintain development and testing environments and the configuration management process and structures. Serve as point-of-contact for third-party software and hardware vendors. Responsible for providing software support functions like code maintenance, backups, functionality modifications, reports generation, modify/upgrade software documentation, user training, software migrations, version control, technical support and user training.

**Minimum Education:** Bachelor’s degree in Computer Sciences, Information Systems, Mathematics, Engineering or related field. A degree in disciplines other than those listed above may also be considered if and only if they have at least six (6) years of relevant experience.

**32 Commercial Job Title:** Network Engineer – Senior

**Technical Qualifications/Experience:** Minimum six (6) years of experience in planning, management, support, and operation of the LAN/WAN environment. Must be knowledgeable in computer technology, including architecture, operating systems, and hardware components, such as workstations, disks, and graphics input and output devices; must be knowledgeable in distributed computing system concepts, including client/server computing issues, mass storage technology, and computer network technology. Must have experience in configuring UNIX workstations, including SunOS and SPARC products, and associated third party peripherals. Must thoroughly understand complex network principles related to IEE802, ISDN, X.25, TI, TCP/IP, and NFS. This should include protocol specifications, performance
limitations, network interconnectivity issues, and network security. Network experience must include configuring one or more networks based on serial communications, MODEMS, Ethernet, TCP/IP, and NFS. It is desirable to have UNIX software development experience; must have ability to effectively communicate technical information to non-technical personnel, both orally and in writing.

**Functional Responsibility:** Responsible for planning, management, support, and operation of the LAN/WAN environment. Provide system administration of Network, Web, and/or communications systems, including Local Area Network (LAN), Wide Area Network (WAN). Maintain servers, create monitoring reports and logs and ensure functionality of links. Establish backups and monitor site security. Responsible for developing, refining, and troubleshooting a large distributed environment, involving UNIX and MS-DOS platforms. Design, develop, test and implement new system software modules and enhancements to current systems; design, develop, test, and implement diagnostic utilities to analyze and report system status and performance. Evaluate overall system performance of operating system facilities, software products, computer services, and communications and networking facilities; specifies, system components as required to enable system to meet desired performance objectives.

**Minimum Education:** Bachelor’s degree in Computer Sciences, Information Systems, Mathematics, Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor’s degree in disciplines other than those listed above may also be considered if they have at least eight (8) years of experience in planning, management, support, and operation of the LAN/WAN environment.

**Commercial Job Title:** Network Engineer – Mid

**Technical Qualifications/Experience:** Minimum four (4) years of experience in networking administration. Must be knowledgeable in computer technology, including architecture, operating systems, and hardware components, such as workstations, disks, and graphics input and output devices; must be knowledgeable in distributed computing system concepts, including client/server computing issues, mass storage technology, and computer network technology. Must have experience in configuring UNIX workstations, including SunOS and SPARC products, and associated third party peripherals. Mass storage experience should include optical technology; must thoroughly understand complex network principles related to IEE802, ISDN, X.25, TI, TCP/IP, and NFS. This should include protocol specifications, performance limitations, network inter-connectivity issues, and network security. Network experience must include configuring one or more networks based on serial communications, MODEMS, Ethernet, TCP/IP, and NFS. It is desirable to have UNIX software development experience; must have the ability to effectively communicate technical information to non-technical personnel, both orally and in writing.

**Functional Responsibility:** Responsible for developing, refining, and troubleshooting a large distributed environment, involving UNIX and MS-DOS platforms. Design, develop, test and implement new system software modules and enhancements to current systems; design, develop, test, and implement diagnostic utilities to analyze and report system status and performance. Monitor and evaluate overall system performance of operating system facilities, software products, computer services, and communications and networking facilities. Specify, install and tests system components as required to enable system to meet desired performance objectives.

**Minimum Education:** Bachelor’s degree in Computer Sciences, Information Systems, Mathematics, Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor’s degree in disciplines other than those listed above may also be considered if they have at least seven (7) years of experience in developing, refining, and troubleshooting a large distributed environment, involving UNIX and MS-DOS platforms.

**Commercial Job Title:** Network Security Specialist

**Technical Qualifications/Experience:** Minimum five (5) years of experience in installing, configuring, and maintaining organization's operating systems, and network components to ensure security of networks.
Functional Responsibility: Install, configure and maintain organization's operating systems. Analyze and resolve problems associated with server hardware, NT, applications software. Detect, diagnose, and report NT related problems on both NT server and NT desktop systems. Perform a wide variety of tasks in software/hardware maintenance and operational support of NT Server systems. Analyze general information assurance-related technical problems and provides basic engineering and technical support in solving these problems. Design, develop, engineer, and implement solutions that meet network security requirements. Perform vulnerability/risk analyses of computer systems and applications during all phases of the system development life cycle.

Minimum Education: Bachelor’s degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor’s degree in disciplines other than those listed above may also be considered if and only if they have at least seven (7) years of relevant experience in installing, configuring, and maintaining organization’s operating systems, and network components.

35  Commercial Job Title: Penetration Tester – Senior  
Technical Qualifications/Experience: Minimum five (5) years of experience in independently performing penetration testing using automated tools to determine potential security breaches, and detect any intrusion into the organization’s Information Systems by hackers or viruses.

Functional Responsibility: Responsible for performing penetration testing on organizational systems, data and networks using automated tools like TripWire to determine potential internet or information security breaches, and detect any intrusion into the organization’s information systems by hackers or viruses. Responsible for following the penetration test plan, conducting the unit as well as system testing as per pre-defined test cases, complete test reporting documentation, identify breaches, or potential breaches and the root causes of such breaches.

Minimum Education: Bachelor’s degree in Computer Science, Information Systems, Engineering, Business, Mathematics or related field. Candidates having a bachelor’s degree in disciplines other than those listed above may also be considered if they have at least seven (7) years of experience in performing penetration testing, and intrusion detection using automated tools like Tripwire.

36  Commercial Job Title: Penetration Tester – Junior  
Technical Qualifications/Experience: Minimum two (2) years of experience in independently performing penetration testing using automated tools to determine potential security breaches, and detect any intrusion into the organization’s Information Systems by hackers or viruses.

Functional Responsibility: Responsible for performing penetration testing on organizational systems, data and networks using automated tools like TripWire to determine potential internet or information security breaches, and detect any intrusion into the organization’s information systems by hackers or viruses. Responsible for following the penetration test plan, conducting the unit as well as system testing as per pre-defined test cases, complete test reporting documentation, identify breaches, or potential breaches and the root causes of such breaches.

Minimum Education: Bachelor’s degree in Computer Science, Information Systems, Engineering, Business, Mathematics or related field. Candidates having a bachelor’s degree in disciplines other than those listed above may also be considered if they have at least seven (7) years of experience in performing penetration testing, and intrusion detection using automated tools like Tripwire.

37  Commercial Job Title: Program Manager  
Technical Qualifications/Experience: Minimum eight (8) years of experience in the IT industry, out of which at least 5 years must be in the field of Project Management, Business Administration, Human Resources, and/or Client Relationship Management.
Functional Responsibility: Act as the central point of contact with the Contracting Officer, Contracting Officer’s Representative and Task Managers. Responsible for coordinating the management of all work performed on this contract, including subcontractors, team members, and vendors. Keep in constant touch with the project managers regarding the status of various task order projects, the issues facing the project teams and effectively and regularly updates the client representatives. Also facilitate the information, which the team requires from the client to effectively implement various Task Order Projects and if necessary, escalates the burning issues to the client representatives and contract officer. All the Task Order Project Managers typically report to the Program Manager for that contract.

Minimum Education: Bachelor’s degree or equivalent technical qualification or 2 to 3 years of additional experience. Master’s Degree in Computer Science; Master’s Degree in Business Administration is desirable.

38 Commercial Job Title: Project Control Analyst Technical Qualifications/Experience: Minimum four (4) years of experience in analyzing the project schedules and costs. Must have a thorough knowhow of Software Development Lifecycle, and proficiency in Project Management tools like MS Project, tools like Visio, MS Word, Excel and Power Point.

Functional Responsibility: Assist the Project Manager in analyzing the project schedules, and costs. Monitor and analyze each project task and sub task using automated tools like MS Project, identifies potential sources of project delays and cost over‐runs and reports the results to the Project Manager. Also analyze the utilization and productivity of each project resources, and identify potential bottlenecks.

Minimum Education: Bachelor’s degree in Accounting, Business Administration or related field. Candidates having a bachelor’s degree in disciplines other than those listed above may also be considered if and only if they have at least six (6) years of relevant experience in analyzing the project schedules and costs.

39 Commercial Job Title: Project Manager Technical Qualifications/Experience: Minimum five (5) years of experience in managing IT projects. Must have a thorough knowhow of Software Development Lifecycle, project planning, risk management, project reporting, proficiency in Project Management tools like MS Project, tools like Visio, MS Word, Excel and Power Point.

Functional Responsibility: Responsible for the timely execution of the various Task Order projects awarded under the master contract. Responsible for project planning, team composition, task allocation, task monitoring, task facilitation, risk management, disaster recovery, over viewing analysis/designing, programming, testing and user documentation. Maintain project status documentation, give regular updates to the account manager, give technical presentations to the client representatives and periodically attends status meetings with the client representatives. Report to the Program Manager for the contract.

Minimum Education: Bachelor’s degree in Computer Sciences, Information Systems, Mathematics, Engineering (Electrical, Computer, Mechanical) or related field. A Master’s degree in Computer Science is desirable. Candidates having a bachelor’s degree in disciplines other than those listed above may also be considered if and only if they have at least seven (7) years of experience in managing IT projects.

40 Commercial Job Title: Quality Assurance Specialist Technical Qualifications/Experience: Minimum eight (8) years of experience in defining test cases, developing test plans and leading the software testing and validation teams in performing the unit, and integrated system (functional, load, regression) testing of complex software/systems. Must have a thorough understanding of Software Testing and Quality Assurance Methodologies like IEEE, SEI CMM/I, ISO 9000, and TQA.

Functional Responsibility: Provide development of project Software Quality Assurance Plan and the implementation of procedures that conforms to the requirements of the contract as detailed in Quality Assurance Surveillance Plan. Provide an independent assessment of how the project’s software development process is being implemented relative to the defined process and recommends methods to optimize the
organization’s process. Perform regular internal audits to ensure proper quality control. Responsible for system and/or application testing (client server and web applications) to ensure that the system/application software is compliant with the access control exposure. Detailed tasks include developing a system/application test plan/design, test procedures and complete test reporting documentation, test execution and tracking, and release management. Includes testing both the functionality of the application via the front end and validate the test results via the back-end. Testing is done using several testing tools like Load runner and WinRunner. Responsible for developing the test cases system/application test plan/design, test procedures and leading a team of testers in performing the unit, and integrated system (functional, load, regression) testing of complex software/systems. Responsible for reviewing the test reporting documentation, test execution and tracking, and release management. Responsible for ensuring that the system/application software is compliant with the access control exposure.

**Minimum Education:** Bachelor’s degree in Computer Science, Information Systems, Engineering, Business, Economics, Mathematics, Public Administration or related field.

---

41  **Commercial Job Title:** R&D Specialist  
**Technical Qualifications/Experience:** Minimum five (5) years of experience in researching data, technology, and available tools and develop IT solutions, tools and applications to better manage and run the IT projects and organization.

**Functional Responsibility:** Research data, software tools, technologies, methodologies, and IT solutions to potential problems faced by project and organizational teams. Develop, test and implement automated applications, tools, and systems in order to improve the efficiency of the organizational processes and/or better management and operations of IT projects.

**Minimum Education:** Bachelor’s degree in Computer Sciences, Information Systems, Mathematics, Engineering or related field. A degree in disciplines other than those listed above will also be considered if and only if they have at least seven (7) years of relevant experience.

---

42  **Commercial Job Title:** Security Subject Matter Expert  
**Technical Qualifications/Experience:** Minimum five (5) years of experience in providing advice and guidance on various matters related to organizational security systems, IS Policy, potential vulnerabilities and solutions to fix these vulnerabilities.

**Functional Responsibility:** Utilize the knowhow, expertise and experience in the field of Information, Internet, System, and Network Security to assist the IS Specialist in defining proven Information Security Policy, and standards for various organizations. Also assist Information Security Analysts, Information Security Engineers, and Information Assurance Engineers in implementing the Information Security controls, detecting intrusion, conducting vulnerability assessments and finding solutions to fix potential weak spots for breaches.

**Minimum Education:** Bachelor’s degree in Computer Sciences, Information Systems, Mathematics, Engineering or related field. A degree in disciplines other than those listed above may also be considered if and only if they have at least six (6) years of relevant experience.

---

43  **Commercial Job Title:** Software Tester  
**Technical Qualifications/Experience:** Minimum five (5) years of experience in independently performing unit and system integration testing (load, functional and regression testing) manually as well as using automated tools like Load Runner, WinRunner and Test Director. Must have expertise in both black box as well as white box testing. Must know how to conduct application, regression and load testing.

**Functional Responsibility:** Responsible for performing the system and/or application testing (client server and web applications) to ensure that the system/application software is compliant with the access control exposure. Responsible for following the test plan, conducting the unit as well as system testing as per pre-defined test cases, complete test reporting documentation, identify bugs and the root cause.
Minimum Education: Bachelor’s degree in Computer Science, Information Systems, Engineering, Business, Economics, Mathematics Public Administration, or related field. Candidates having a bachelor’s degree in disciplines other than those listed above will also be considered if they have at least seven (7) years of experience in performing unit and integration testing manually as well as using automated tools like Load Runner, WinRunner and Test Director.

**Commercial Job Title: System Administrator**

Technical Qualifications/Experience: Minimum five (5) years of experience in installing, managing, maintaining and troubleshooting hardware and software on systems (Windows, HP Unix, Sun Solaris, MVS, VMM Unisys 2200) on different platforms like mainframe, midrange and PCs.

Functional Responsibility: Responsible for the installing, managing, maintaining and troubleshooting hardware and software on systems, to maintain the on-going operational performance of programs (software) and the hardware on which the programs run within the Mainframe, Mid-Range, or PC environments. Implement and support local area network (LAN) and campus area network (CAN) hardware and software. Analyze customer workflow and procedures to recommend operational support tools and technologies to satisfy customer needs. Act as a liaison between the customer, suppliers, and other technical groups to resolve network and hardware problems. Analyze performance problems and recommends solutions to enhance functionality, reliability and/or usability. Implement operational support standards and procedures relating to change management, performance management, and security. Recommend changes and improvements to existing standards. Develop site administration manual (SAM) documentation. Provide user orientation on hardware, software and network operations.

Minimum Education: Bachelor’s degree in Computer Sciences, Information Systems, Mathematics, Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor’s degree in disciplines other than those listed above may also be considered if they have at least seven (7) years of experience in installing, managing, maintaining and troubleshooting hardware and software on systems (Windows, HP Unix, Sun Solaris, MVS, VMM Unisys 2200) on different platforms like mainframe, midrange and PCs.

**Commercial Job Title: System/Software Architect**

Technical Qualifications/Experience: Minimum eight (8) years of experience in the field of IT out of which at least five (5) years must be devoted to designing various components of information systems for organizations based on the various business processes and applications. Must be very familiar with design tools like ERWin, Visio and Rational Rose and must have architected at least 3 systems in the past.

Functional Responsibility: Contribute to the establishment and maintenance of an overall IT architecture relevant to and consistent with the company’s business and technology direction and objectives. Design and develop new software products or major enhancements to existing software. Address problems of systems integration, compatibility, and multiple platforms. Develop information technology technical and application architectures and participates in setting technology direction and standards. Provide technical architectural design review for major business applications and technology initiatives. Facilitate linkage with key business areas by understanding enterprise requirements and by communicating architecture frameworks best practices and standards. Develop recommendations and requirements for legacy applications to evolve towards conformance with target architecture. Continually reviews the company’s applications, workflow, systems, and network management and network infrastructure, for opportunities to improve effectiveness and efficiency.

Minimum Education: Bachelor’s degree in Computer Sciences, Information Systems, Mathematics, Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor’s degree in disciplines other than those listed above may also be considered if and only if they have at least ten (10) years of experience in architecturing IT systems.
46  **Commercial Job Title:** Technical Instruction Specialist  
**Technical Qualifications/Experience:** Minimum three (3) to seven (7) years of managing technology and security training programs including training documentation. Experience with multimedia aided instruction is preferred.

**Functional Responsibility:** Provide computer training and classroom instructions to users and staff personnel as appropriate. Gather and assemble relevant material to be presented. Utilize appropriate teaching methods, individual, group, workshops, etc. Ensure students understand the theoretical and practical aspects of subject material/software application/database applications being taught. Evaluate effectiveness of instruction by ensuring students have a thorough knowledge of subject matter and hands-on skill at performing required task.

**Minimum Education:** Bachelor’s degree or equivalent technical qualification or two (2) to three (3) years of additional experience. Minimum one (1) year of training development and delivery experience.

47  **Commercial Job Title:** Technical Writer – Mid  
**Technical Qualifications/Experience:** Overall four (4) years of experience in preparing technical documents and manuals.

**Functional Responsibility:** Prepare technical documentation, including but not limited to, Technical System Manuals, Operation Manuals, Training documents, functional specifications, test and validation reports, and software application documents.

**Minimum Education:** Associate degree in any technical discipline.

48  **Commercial Job Title:** Technical Writer – Junior  
**Technical Qualifications/Experience:** Minimum two (2) years of experience in preparing technical documents and manuals.

**Functional Responsibility:** Prepare technical documentation, including but not limited to, Technical System Manuals, Operation Manuals, Training documents, functional specifications, test and validation reports, and software application documents.

**Minimum Education:** Associate degree in any technical discipline.

49  **Commercial Job Title:** Web Specialist  
**Technical Qualifications/Experience:** Minimum five (5) years of experience in conceptualizing, analyzing, designing and implementing the web modules, web based applications and web sites for State and/or Federal Government.

**Functional Responsibility:** Responsible for need analysis, conceptualization, analysis, design and implementation of web applications, web modules, e-forms, web sites and portals for the State and Federal Government agencies. Responsible for improvements to the existing Government Web applications.

**Minimum Education:** Bachelor’s degree in Computer Sciences, Information Systems, Business, Arts, Economics, Mathematics, Engineering (Electrical, Computer, Mechanical) or related field.

**SIN 611420 COURSE DESCRIPTIONS**

1  **Course Title:** Cybersecurity Fundamentals Workshop 4 Day  
**Overview:** This course provides participants with a high-level overview of various aspects of Cybersecurity in the context of a modern and Internet-connected environment. Through lecture, hands-on exercises, and group discussion, you will gain a foundational perspective on the challenges of designing a cybersecurity program, implementing secure systems, and other factors needed for a comprehensive cybersecurity solution. Upon completion of this course, each participant will be able to define cybersecurity terminology, compliance requirements, review sample attacks, and gain an understanding of the impact of current threat trends on cybersecurity implementation.
2  **Course Title: Cyber Tools and Analysis Hands-On 4 Day**  
**Overview:** Our hands-on course is designed to give students hands-on experience with cyber tool deployments across multiple operating system platforms. Students will learn network defense and analysis techniques as well as methods to prevent network attacks.

**Topics Covered:**

- Technical Security Controls
- Cyber Security Tools Introduction
- Operating System Introduction
- Operating System Configuration
- Network-Based Applications
- Network Architectures
- Network Defense Techniques
- Attack Prevention Methods

**Takeaway Items:** A printed training book and a CD that includes reference materials pertaining to the course.

3  **Course Title: Recovery Planning Practitioner COOP 5 Day**  
**Overview:** This course is designed to provide an operational basis for all facets of recovery planning through information delivery and practical exercises. As a result of this course, students will be able to conduct risk analyses, business impact analyses, recovery strategy analyses and develop viable emergency response plans and recovery plans through the information obtained as a result of these assessments. The Recovery Planning Practitioner Course imparts an ability to conduct Business Impact Analyses so that executive management will have a prioritized list of all functions performed, a determination of when the loss of a given function becomes unacceptable to the organization, and the resources necessary to enable the recovery of each function.

The Recovery Planning Practitioner course provides students with insights into conducting recovery strategy analysis, understanding the different strategies that are currently available and their applicability based on their strengths and weaknesses. This course will expose the students to emergency response techniques from the development of checklists to crafting concise communications releases. Upon completion of the study of recovery planning fundamentals, this course will give students a thorough knowledge of how to develop viable, easy to use recovery plans that address all hazards and all contingencies. Finally, this course is designed to provide the elements of an ongoing viable recovery capability through training and exercising programs that meet the needs of all audiences for all organizations.

**Modules:**

- Module 1: Introduction
- Module 2: Risk Analysis
- Module 3: Business Impact Analysis
- Module 4: Recovery Strategy Analysis
- Module 5: Emergency Response Planning
- Module 6: Plan Development
- Module 7: Training Programs
Module 8: Plan Exercise

Takeaway Items: A printed training manual, a CD with a comprehensive set of NIST-DoD approved templates, as well as copies of the guidelines, instructions, standards, and presentations discussed during the training.

In addition, students will have the option to sit in on the Certified Continuity Manager (CCM) certification exam. Lunarline has partnered with the National Institute for Business Continuity Management (NIBCM), allowing students who have completed the Recovery Planning course to take this exam. When registering for the course and exam, students can choose either the public sector (COOP) or the private sector (Business Continuity Planning) specialty.
TERMS AND CONDITIONS APPLICABLE TO SIN 511210

1 Terms Regarding Manufacturers’ End-User License Agreements: This contract, or the warranties guaranteed hereunder, is in no way affected, altered, or modified by any Manufacturer End-User License Agreement, unless the Contracting Officer has expressly incorporated a “Government” User End Licensing Agreement into the Contract. The terms of any “Commercial, Special or Other” user licensing agreement that has not been officially incorporated herein are applicable only to the Contractor-Manufacturer relationship, and do not alter the Government's rights or the Contractor's obligations under this contract.

Refer to the attached EULA for complete details.

TERMS AND CONDITIONS APPLICABLE TO SIN 54151HACS

1 Scope: The prices, terms and conditions stated under SIN 54151HACS Cloud Computing Services apply exclusively to Cloud Computing Services within the scope of this Information Technology Schedule.

This SIN provides ordering activities with access to technical services that run in cloud environments and meet the NIST Definition of Cloud Computing Essential Characteristics. Services relating to or impinging on cloud that do not meet all NIST essential characteristics should be listed in other SINs.

The scope of this SIN is limited to cloud capabilities provided entirely as a service. Hardware, software and other artifacts supporting the physical construction of a private or other cloud are out of scope for this SIN. Currently, an Ordering Activity can procure the hardware and software needed to build on premise cloud functionality, through combining different services on other IT Schedule 70 SINs.

Sub-categories in scope for this SIN are the three (3) NIST Service Models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Offerors may optionally select a single sub-category that best fits a proposed cloud service offering. Only one sub-category may be selected per each proposed cloud service offering. Offerors may elect to submit multiple cloud service offerings, each with its own single sub-category. The selection of one of three sub-categories does not prevent Offerors from competing for orders under the other two sub-categories. See service model guidance for advice on sub-category selection.

Sub-category selection within this SIN is optional for any individual cloud service offering, and new cloud computing technologies that do not align with the aforementioned three sub-categories may be included without a sub-category selection so long as they comply with the essential characteristics of cloud computing as outlined by NIST. See Table 1 for a representation of the scope and sub-categories.

<table>
<thead>
<tr>
<th>SIN Description</th>
<th>Sub-Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Commercially available cloud computing services</td>
<td>1. <strong>Software as a Service (SaaS)</strong>: Consumer uses provider’s applications on cloud infrastructure. Does not manage/control platform or infrastructure. Limited application level configuration may be available.</td>
</tr>
<tr>
<td>• Meets the National Institute for Standards and Technology (NIST) definition of Cloud Computing essential characteristics</td>
<td>2. <strong>Platform as a Service (PaaS)</strong>: Consumer deploys applications onto cloud platform service using provider-supplied tools. Has control over deployed applications and some limited platform configuration but does not manage the platform or infrastructure.</td>
</tr>
<tr>
<td>• Open to all deployment models (private, public, community or hybrid), vendors specify deployment models</td>
<td>3. <strong>Infrastructure as a Service (IaaS)</strong>: Consumer provisions computing resources. Has control over OS, storage, platform, deployed applications and some limited infrastructure configuration, but does not manage the infrastructure.</td>
</tr>
</tbody>
</table>

2 Responsibilities of the Contractor: The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) cover work of this character.
Acceptance Testing: Any required Acceptance Test Plans and Procedures shall be negotiated by the Ordering Activity at task order level. The Contractor shall perform acceptance testing of the systems for Ordering Activity approval in accordance with the approved test procedures.

Training: If training is provided commercially the Contractor shall provide normal commercial installation, operation, maintenance, and engineering interface training on the system. Contractor is responsible for indicating if there are separate training charges.

Information Assurance/Security Requirements: The Contractor shall meet information assurance/security requirements in accordance with the Ordering Activity requirements at the Task Order level.

Related Professional Services: The Contractor is responsible for working with the Ordering Activity to identify related professional services and any other services available on other SINs that may be associated with deploying a complete cloud solution. Any additional substantial and ongoing professional services related to the offering such as integration, migration, and other cloud professional services are out of scope for this SIN.

Performance of Cloud Computing Services: The Contractor shall respond to Ordering Activity requirements at the Task Order level with proposed capabilities to Ordering Activity performance specifications or indicate that only standard specifications are offered. In all cases the Contractor shall clearly indicate standard service levels, performance and scale opportunities.

The Contractor shall provide appropriate cloud computing services on the date and to the extent and scope agreed to by the Contractor and the Ordering Activity.

Reporting: The Contractor shall respond to Ordering Activity requirements and specify general reporting capabilities available for the Ordering Activity to verify performance, cost and availability.

In accordance with commercial practices, the Contractor may furnish the Ordering Activity/user with a monthly summary Ordering Activity report.

3 Responsibilities of the Ordering Activity: The Ordering Activity is responsible for indicating the cloud computing services requirements unique to the Ordering Activity. Additional requirements should not contradict existing SIN or IT Schedule 70 Terms and Conditions. Ordering Activities should include (as applicable) Terms & Conditions to address Pricing, Security, Data Ownership, Geographic Restrictions, Privacy, SLAs, etc.

Cloud services typically operate under a shared responsibility model, with some responsibilities assigned to the Cloud Service Provider (CSP), some assigned to the Ordering Activity, and others shared between the two. The distribution of responsibilities will vary between providers and across service models.

Ordering activities should engage with CSPs to fully understand and evaluate the shared responsibility model proposed. Federal Risk and Authorization Management Program (FedRAMP) documentation will be helpful regarding the security aspects of shared responsibilities, but operational aspects may require additional discussion with the provider.

Ordering Activity Information Assurance/Security Requirements Guidance:

- The Ordering Activity is responsible for ensuring to the maximum extent practicable that each requirement issued is in compliance with the Federal Information Security Management Act (FISMA) as applicable.

- The Ordering Activity shall assign a required impact level for confidentiality, integrity and availability (CIA) prior to issuing the initial statement of work.¹ The Contractor must be capable of meeting at least


FSS Price List, MAS

Page 31 of 43

GS-35F-0392X
the minimum security requirements assigned against a low-impact information system in each CIA assessment area (per FIPS 200) and must detail the FISMA capabilities of the system in each of CIA assessment area.

- Agency level FISMA certification, accreditation, and evaluation activities are the responsibility of the Ordering Activity. The Ordering Activity reserves the right to independently evaluate, audit, and verify the FISMA compliance for any proposed or awarded Cloud Computing Services.

- The Ordering Activity has final responsibility for assessing the FedRAMP status of the service, complying with and making a risk-based decision to grant an Authorization to Operate (ATO) for the cloud computing service, and continuous monitoring. A memorandum issued by the Office of Management and Budget (OMB) on Dec 8, 2011 outlines the responsibilities of Executive departments and agencies in the context of FedRAMP compliance.²

- Ordering activities are responsible for determining any additional information assurance and security related requirements based on the nature of the application and relevant mandates.

**Deployment Model:** If a particular deployment model (Private, Public, Community, or Hybrid) is desired, Ordering Activities are responsible for identifying the desired model(s). Alternately, Ordering Activities could identify requirements and assess Contractor responses to determine the most appropriate deployment model(s).

**Delivery Schedule:** The Ordering Activity shall specify the delivery schedule as part of the initial requirement. The Delivery Schedule options are found in Information for Ordering Activities Applicable to All Special Item Numbers.

**Interoperability:** Ordering Activities are responsible for identifying interoperability requirements. Ordering Activities should clearly delineate requirements for API implementation and standards conformance.

**Performance of Cloud Computing Services:** The Ordering Activity should clearly indicate any custom minimum service levels, performance and scale requirements as part of the initial requirement.

**Reporting:** The Ordering Activity should clearly indicate any cost, performance or availability reporting as part of the initial requirement.

**Privacy:** The Ordering Activity should specify the privacy characteristics of their service and engage with the Contractor to determine if the cloud service is capable of meeting Ordering Activity requirements. For example, a requirement could be requiring assurance that the service is capable of safeguarding Personally Identifiable Information (PII), in accordance with NIST SP 800-122³ and OMB memos M-06-16⁴ and M-07-16⁵. An Ordering Activity will determine what data elements constitute PII according to OMB Policy, NIST Guidance and Ordering Activity policy.

**Accessibility:** The Ordering Activity should specify the accessibility characteristics of their service and engage with the Contractor to determine if the cloud service is capable of meeting Ordering Activity requirements. For example, a requirement could require assurance that the service is capable of providing accessibility based on Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d).

**Geographic Requirements:** Ordering activities are responsible for specifying any geographic requirements and engaging with the Contractor to determine that the cloud services offered have the capabilities to meet

---

³ NIST SP 800-122, “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)”
geographic requirements for all anticipated task orders. Common geographic concerns could include whether service data, processes and related artifacts can be confined on request to the United States and its territories, or the continental United States (CONUS).

Data Ownership and Retrieval and Intellectual Property: Intellectual property rights are not typically transferred in a cloud model. In general, CSPs retain ownership of the Intellectual Property (IP) underlying their services and the customer retains ownership of its intellectual property. The CSP gives the customer a license to use the cloud services for the duration of the contract without transferring rights. The government retains ownership of the IP and data they bring to the customized use of the service as spelled out in the FAR and related materials.

General considerations of data ownership and retrieval are covered under the terms of Schedule 70 and the FAR and other laws, ordinances, and regulations (Federal, State, City, or otherwise). Because of considerations arising from cloud shared responsibility models, ordering activities should engage with the Contractor to develop more cloud-specific understandings of the boundaries between data owned by the government and that owned by the cloud service provider, and the specific terms of data retrieval.

In all cases, the Ordering Activity should enter into an agreement with a clear and enforceable understanding of the boundaries between government and cloud service provider data, and the form, format and mode of delivery for each kind of data belonging to the government.

The Ordering Activity should expect that the Contractor shall transfer data to the government at the government’s request at any time, and in all cases when the service or order is terminated for any reason, by means, in formats and within a scope clearly understood at the initiation of the service. Example cases that might require clarification include status and mode of delivery for:

- Configuration information created by the government and affecting the government’s use of the cloud provider’s service.
- Virtual machine configurations created by the government but operating on the cloud provider’s service.
- Profile, configuration and other metadata used to configure SaaS application services or PaaS platform services.

The key is to determine in advance the ownership of classes of data and the means by which Government owned data can be returned to the Government.

Service Location Distribution: The Ordering Activity should determine requirements for continuity of operations and performance and engage with the Contractor to ensure that cloud services have adequate service location distribution to meet anticipated requirements. Typical concerns include ensuring that:

- Physical locations underlying the cloud are numerous enough to provide continuity of operations and geographically separate enough to avoid an anticipated single point of failure within the scope of anticipated emergency events.
- Service endpoints for the cloud are able to meet anticipated performance requirements in terms of geographic proximity to service requestors.

Note that cloud providers may address concerns in the form of minimum distance between service locations, general regions where service locations are available, etc.

Related Professional Services: Ordering activities should engage with Contractors to discuss the availability of limited assistance with initial setup, training and access to the services that may be available through this SIN.
Any additional substantial and ongoing professional services related to the offering such as integration, migration, and other cloud professional services are out of scope for this SIN. Ordering activities should consult the appropriate GSA professional services schedule.

4 Guidance for Contractors: This section offers guidance for interpreting the Contractor Description Requirements in Table 2, including the NIST essential cloud characteristics, service models and deployment models. This section is not a list of requirements.

Contractor-specific definitions of cloud computing characteristics and models or significant variances from the NIST essential characteristics or models are discouraged and will not be considered in the scope of this SIN or accepted in response to Factors for Evaluation. The only applicable cloud characteristics, service model/subcategories and deployment models for this SIN will be drawn from the NIST 800-145 special publication. Services qualifying for listing as cloud computing services under this SIN must substantially satisfy the essential characteristics of cloud computing as documented in the NIST Definition of Cloud Computing SP 800-145.

Contractors must select deployment models corresponding to each way the service can be deployed. Multiple deployment model designations for a single cloud service are permitted but at least one deployment model must be selected.

In addition, Contractors submitting services for listing under this SIN are encouraged to select a sub-category for each service proposed under this SIN with respect to a single principal NIST cloud service model that most aptly characterizes the service. Service model categorization is optional.

Both service and deployment model designations must accord with NIST definitions. Guidance is offered in this document on making the most appropriate selection.

NIST Essential Characteristics:

- **General Guidance:** NIST’s essential cloud characteristics provide a consistent metric for whether a service is eligible for inclusion in this SIN. It is understood that due to legislative, funding and other constraints that government entities cannot always leverage a cloud service to the extent that all NIST essential characteristics are commercially available. For the purposes of the Cloud SIN, meeting the NIST essential characteristics is determined by whether each essential capability of the commercial service is available for the service, whether or not the Ordering Activity actually requests or implements the capability. The guidance in Table 2 offers examples of how services might or might not be included based on the essential characteristics, and how the Contractor should interpret the characteristics in light of current government contracting processes.

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Capability</th>
<th>Guidance</th>
</tr>
</thead>
</table>
| On-demand self-service | • Ordering activities can directly provision services without requiring Contractor intervention.  
• This characteristic is typically implemented via a service console or programming interface for provisioning | Government procurement guidance varies on how to implement on-demand provisioning at this time.  
Ordering activities may approach on-demand in a variety of ways, including “not-to-exceed” limits, or imposing monthly or annual payments on what are essentially on demand services.  
Services under this SIN must be capable of true on-demand self-service, and ordering activities and Contractors must negotiate how they implement on demand capabilities in practice at the Task Order level:  
• Ordering activities must specify their procurement approach and requirements for on-demand service  
• Contractors must propose how they intend to meet the approach |

---

| **Broad Network Access** | • Ordering activities are able to access services over standard agency networks | • Broad network access must be available without significant qualification and in relation to the deployment model and security domain of the service. Contractors must specify any ancillary activities, services or equipment required to access cloud services or integrate cloud with other cloud or non-cloud networks and services. For example, a private cloud might require an Ordering Activity to purchase or provide a dedicated router, etc. which is acceptable but should be indicated by the Contractor. |
| **Resource Pooling** | • Pooling distinguishes cloud services from offsite hosting. Ordering activities draw resources from a common pool maintained by the Contractor. Resources may have general characteristics such as regional location. | • The cloud service must draw from a pool of resources and provide an automated means for the Ordering Activity to dynamically allocate them.
  • Manual allocation, e.g. manual operations at a physical server farm where Contractor staff configure servers in response to Ordering Activity requests, does not meet this requirement.
  • Similar concerns apply to software and platform models; automated provisioning from a pool is required.
  • Ordering activities may request dedicated physical hardware, software or platform resources to access a private cloud deployment service. However the provisioned cloud resources must be drawn from a common pool and automatically allocated on request. |
| **Rapid Elasticity** | Rapid provisioning and de-provisioning commensurate with demand | • Rapid elasticity is a specific demand-driven case of self-service.
  • Procurement guidance for on-demand self-service applies to rapid elasticity as well, i.e. rapid elasticity must be technically available but ordering activities and Contractors may mutually negotiate other contractual arrangements for procurement and payment.
  • ‘Rapid’ should be understood as measured in minutes and hours, not days or weeks.
  • Elastic capabilities by manual request, e.g. via a console operation or programming interface call, are required.
  • Automated elasticity which is driven dynamically by system load, etc. is optional. Contractors must specify whether automated demand-driven elasticity is available and the general mechanisms that drive the capability. |
| **Measured Service** | Measured service should be understood as a reporting requirement that enables an Ordering Activity to control their use in cooperation with self service. | • Procurement guidance for on-demand self-service applies to measured service as well, i.e. rapid elasticity must be technically available but ordering activities and Contractors may mutually designate other contractual arrangements.
  • Regardless of specific contractual arrangements, reporting must indicate actual usage, be continuously available to the Ordering Activity, and provide meaningful metrics appropriate to the service measured.
  • Contractors must specify that measured service is available and the general sort of metrics and mechanisms available. |

- **Inheriting Essential Characteristics**: Cloud services may depend on other cloud services, and cloud service models such as PaaS and SaaS are able to inherit essential characteristics from other cloud services that support them. For example a PaaS platform service can inherit the broad network access made available by the IaaS service it runs on, and in such a situation would be fully compliant with the broad network access essential characteristic. Services inheriting essential characteristics must make the inherited characteristic fully available at their level of delivery to claim the relevant characteristic by inheritance.
Inheriting characteristics does not require the inheriting provider to directly bundle or integrate the inherited service, but it does require a reasonable measure of support and identification. For example, the Ordering Activity may acquire an IaaS service from “Provider A” and a PaaS service from “Provider B”. The PaaS service may inherit broad network access from “Provider A” but must identify and support the inherited service as an acceptable IaaS provider.

- **Assessing Broad Network Access:** Typically broad network access for public deployment models implies high bandwidth access from the public internet for authorized users. In a private cloud deployment internet access might be considered broad access, as might be access through a dedicated shared high bandwidth network connection from the Ordering Activity, in accord with the private nature of the deployment model.

- **Resource Pooling and Private Cloud:** All cloud resource pools are finite, and only give the appearance of infinite resources when sufficiently large, as is sometimes the case with a public cloud. The resource pool supporting a private cloud is typically smaller with more visible limits. A finite pool of resources purchased as a private cloud service qualifies as resource pooling so long as the resources within the pool can be dynamically allocated to the ultimate users of the resource, even though the pool itself appears finite to the Ordering Activity that procures access to the pool as a source of dynamic service allocation.

- **NIST Service Model:** The Contractor may optionally document the service model of cloud computing (e.g. IaaS, PaaS, SaaS, or a combination thereof, that most closely describes their offering, using the definitions in The NIST Definition of Cloud Computing SP 800-145. The following guidance is offered for the proper selection of service models.

NIST’s service models provide this SIN with a set of consistent sub-categories to assist ordering activities in locating and comparing services of interest. Service model is primarily concerned with the nature of the service offered and the staff and activities most likely to interact with the service. Contractors should select a single service model most closely corresponding to their proposed service based on the guidance below. It is understood that cloud services can technically incorporate multiple service models and the intent is to provide the single best categorization of the service.

Contractors should take care to select the NIST service model most closely corresponding to each service offered. Contractors should not invent, proliferate or select multiple cloud service model sub-categories to distinguish their offerings, because ad-hoc categorization prevents consumers from comparing similar offerings. Instead vendors should make full use of the existing NIST categories to the fullest extent possible.

For example, in this SIN an offering commercially marketed by a Contractor as “Storage as a Service” would be properly characterized as Infrastructure as a Service (IaaS), storage being a subset of infrastructure. Services commercially marketed as “LAMP as a Service” or “Database as a Service” would be properly characterized under this SIN as Platform as a Service (PaaS), as they deliver two kinds of platform services. Services commercially marketed as “Travel Facilitation as a Service” or “Email as a Service” would be properly characterized as species of Software as a Service (SaaS) for this SIN.

However, Contractors can and should include appropriate descriptions (include commercial marketing terms) of the service in the full descriptions of the service’s capabilities.

When choosing between equally plausible service model sub-categories, Contractors should consider several factors:

1) **Visibility to the Ordering Activity:** Service model sub-categories in this SIN exist to help Ordering Activities match their requirements with service characteristics. Contractors should select the most intuitive and appropriate service model from the point of view of an Ordering Activity.

2) **Primary Focus of the Service:** Services may offer a mix of capabilities that span service models in the strict technical sense. For example, a service may offer both IaaS capabilities for processing and storage,
along with some PaaS capabilities for application deployment, or SaaS capabilities for specific applications. In a service mix situation the Contractor should select the service model that is their primary focus. Alternatively contractors may choose to submit multiple service offerings for the SIN, each optionally and separately subcategorized.

3) **Ordering Activity Role:** Contractors should consider the operational role of the Ordering Activity’s primary actual consumer or operator of the service. For example, services most often consumed by system managers are likely to fit best as IaaS; services most often consumed by application deployers or developers as PaaS, and services most often consumed by business users as SaaS.

4) **Lowest Level of Configurability.** Contractors should consider IaaS, PaaS and SaaS as an ascending hierarchy of complexity, and select the model with the lowest level of available Ordering Activity interaction. As an example, virtual machines are an IaaS service often bundled with a range of operating systems, which are PaaS services. The Ordering Activity usually has access to configure the lower level IaaS service, and the overall service should be considered IaaS. In cases where the Ordering Activity cannot configure the speed, memory, network configuration, or any other aspect of the IaaS component, consider categorizing as a PaaS service.

Cloud management and cloud broker services should be categorized based on their own characteristics and not those of the other cloud services that are their targets. Management and broker services typically fit the SaaS service model, regardless of whether the services they manage are SaaS, PaaS or IaaS. Use Table 3 to determine which service model is appropriate for the cloud management or cloud broker services, or, alternately choose not to select a service model for the service.

The guidance in the table below offers examples of how services might be properly mapped to NIST service models and how a Contractor should interpret the service model sub-categories.

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Guidance on Mapping to NIST Service Models</th>
</tr>
</thead>
</table>
| Infrastructure as a Service (IaaS) | Select an IaaS model for service based equivalents of hardware appliances such as virtual machines, storage devices, routers and other physical devices.  
- IaaS services are typically consumed by system or device managers who would configure physical hardware in a non-cloud setting  
- The principal customer interaction with an IaaS service is provisioning then configuration, equivalent to procuring and then configuring a physical device.  
Examples of IaaS services include virtual machines, object storage, disk block storage, network routers and firewalls, software defined networks.  
Gray areas include services that emulate or act as dedicated appliances and are directly used by applications, such as search appliances, security appliances, etc. To the extent that these services or their emulated devices provide direct capability to an application they might be better classified as Platform services (PaaS). To the extent that they resemble raw hardware and are consumed by other platform services they are better classified as IaaS. |
| Platform as a Service (PaaS) | Select a PaaS model for service based equivalents of complete or partial software platforms. For the purposes of this classification, consider a platform as a set of software services capable of deploying all or part of an application.  
- A complete platform can deploy an entire application. Complete platforms can be proprietary or open source  
- Partial platforms can deploy a component of an application which combined with other components make up the entire deployment  
PaaS services are typically consumed by application deployment staff whose responsibility is to take a completed agency application and cause it to run on the designated complete or partial platform service. |
• The principal customer interaction with a PaaS service is deployment, equivalent to deploying an application or portion of an application on a software platform service.

• A limited range of configuration options for the platform service may be available.

Examples of complete PaaS services include:
• A Linux/Apache/MySQL/PHP (LAMP) platform ready to deploy a customer PHP application,
• A Windows .Net platform ready to deploy a .Net application,
• A custom complete platform ready to develop and deploy an customer application in a proprietary language
• A multiple capability platform ready to deploy an arbitrary customer application on a range of underlying software services.

The essential characteristic of a complete PaaS is defined by the customer’s ability to deploy a complete custom application directly on the platform.

PaaS includes partial services as well as complete platform services. Illustrative examples of individual platform enablers or components include:
• A database service ready to deploy a customer’s tables, views and procedures,
• A queuing service ready to deploy a customer’s message definitions
• A security service ready to deploy a customer’s constraints and target applications for continuous monitoring

The essential characteristic of an individual PaaS component is the customer’s ability to deploy their unique structures and/or data onto the component for a partial platform function.

Note that both the partial and complete PaaS examples all have two things in common:
• They are software services, which offer significant core functionality out of the box
• They must be configured with customer data and structures to deliver results

As noted in IaaS, operating systems represent a grey area in that OS is definitely a platform service, but is typically bundled with IaaS infrastructure. If your service provides an OS but allows for interaction with infrastructure, please sub-categorize it as IaaS. If your service “hides” underlying infrastructure, consider it as PaaS.

Software as a Service (SaaS)

Select a SaaS model for service based equivalents of software applications.
• SaaS services are typically consumed by business or subject-matter staff who would interact directly with the application in a non-cloud setting
• The principal customer interaction with a SaaS service is actual operation and consumption of the application services the SaaS service provides.

Some minor configuration may be available, but the scope of the configuration is limited to the scope and then the permissions of the configuring user. For example an agency manager might be able to configure some aspects of the application for their agency but not all agencies. An agency user might be able to configure some aspects for themselves but not everyone in their agency. Typically only the Contractor would be permitted to configure aspects of the software for all users.

Examples of SaaS services include email systems, business systems of all sorts such as travel systems, inventory systems, etc., wiki’s, websites or content management systems, management applications that allow a customer to manage other cloud or non-cloud services, and in general any system where customers interact directly for a business purpose.

Gray areas include services that customers use to configure other cloud services, such as cloud management software, cloud brokers, etc. In general these sorts of systems should be considered SaaS, per guidance in this document.

• Deployment Model: Deployment models (e.g. private, public, community, or hybrid) are not restricted at the SIN level and any specifications for a deployment model are the responsibility of the Ordering Activity.

Multiple deployment model selection is permitted, but at least one model must be selected. The guidance in Table 4 offers examples of how services might be properly mapped to NIST deployment models and how the Contractor should interpret the deployment model characteristics. Contractors should take care to select the range of NIST deployment models most closely corresponding to each service offered.
Note that the scope of this SIN does not include hardware or software components used to construct a cloud, only cloud capabilities delivered as a service, as noted in the Scope section.

<table>
<thead>
<tr>
<th>Deployment Model</th>
<th>Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private Cloud</td>
<td>The service is provided exclusively for the benefit of a definable organization and its components; access from outside the organization is prohibited. The actual services may be provided by third parties, and may be physically located as required, but access is strictly defined by membership in the owning organization.</td>
</tr>
<tr>
<td>Public Cloud</td>
<td>The service is provided by general public use and can be accessed by any entity or organization willing to contract for it.</td>
</tr>
<tr>
<td>Community Cloud</td>
<td>The service is provided for the exclusive use of a community with a definable shared boundary such as a mission or interest. As with private cloud, the service may be in any suitable location and administered by a community member or a third party.</td>
</tr>
<tr>
<td>Hybrid Cloud</td>
<td>The service is composed of one or more of the other models. Typically hybrid models include some aspect of transition between the models that make them up, for example a private and public cloud might be designed as a hybrid cloud where events like increased load permit certain specified services in the private cloud to run in a public cloud for extra capacity, e.g. bursting.</td>
</tr>
</tbody>
</table>

**TERMS AND CONDITIONS APPLICABLE TO SIN 54151S**

1 **Scope**: The prices, terms and conditions stated under SIN 54151S Information Technology Professional Services apply exclusively to IT Professional Services within the scope of this Information Technology Schedule.

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

2 **Performance Incentives I-FSS-60 Performance Incentives (Apr 2000)**: Performance incentives may be agreed upon between the Contractor and the ordering activity on individual fixed price orders or BPAs under this contract.

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

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

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

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

4 **Performance of Services**: The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity.

The Contractor agrees to render services only during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.
The ordering activity should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner.

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

5 **Stop-Work Order (FAR 52.242-15) (Aug 1989):** The Contracting Officer may, at any time, by written order to the Contractor, require the Contractor to stop all, or any part, of the work called for by this contract for a period of 90 days after the order is delivered to the Contractor, and for any further period to which the parties may agree. The order shall be specifically identified as a stop-work order issued under this clause. Upon receipt of the order, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the order during the period of work stoppage. Within a period of 90 days after a stop-work is delivered to the Contractor, or within any extension of that period to which the parties shall have agreed, the Contracting Officer shall either:

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

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

- The stop-work order results in an increase in the time required for, or in the Contractor’s cost properly allocable to, the performance of any part of this contract; and
- The Contractor asserts its right to the adjustment within 30 days after the end of the period of work stoppage; provided that, if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon the claim submitted at any time before final payment under this contract.

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

If a stop-work order is not canceled and the work covered by the order is terminated for default, the Contracting Officer shall allow, by equitable adjustment or otherwise, reasonable costs resulting from the stop-work order.


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

8 **Responsibilities of the Ordering Activity:** Subject to security regulations, the ordering activity shall permit Contractor access to all facilities necessary to perform the requisite IT Professional Services.

9 **Independent Contractor:** All IT Professional Services performed by the Contractor under the terms of this contract shall be as an independent Contractor, and not as an agent or employee of the ordering activity.
10 Organizational Conflicts of Interest

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.

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.

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

12 Payments: For firm-fixed price orders the ordering activity shall pay the Contractor, upon submission of proper invoices or vouchers, the prices stipulated in this contract for service rendered and accepted. Progress payments shall be made only when authorized by the order. For time-and-materials orders, the Payments under Time-and-Materials and Labor-Hour Contracts at FAR 52.212-4 (MAR 2009) (Alternate I – OCT 2008) (Deviation I – FEB 2007) applies to time-and-materials orders placed under this contract. For labor-hour orders, the Payment under Time-and-Materials and Labor-Hour Contracts at FAR 52.212-4 (MAR 2009) (Alternate I – OCT 2008) (Deviation I – FEB 2007) applies to labor-hour orders placed under this contract.

As prescribed in 16.601(e)(3), insert the following provision:

- The Government contemplates award of a Time-and-Materials or Labor-Hour type of contract resulting from this solicitation.
- The offeror must specify fixed hourly rates in its offer that include wages, overhead, general and administrative expenses, and profit. The offeror must specify whether the fixed hourly rate for each labor category applies to labor performed by:
  - The offeror;
  - Subcontractors; and/or
  - Divisions, subsidiaries, or affiliates of the offeror under a common control.

Incidental support costs are available outside the scope of this contract. The costs will be negotiated separately with the ordering activity in accordance with the guidelines set forth in the FAR.
13 **Approval of Subcontracts:** The ordering activity may require that the Contractor receive, from the ordering activity’s Contracting Officer, written consent before placing any subcontract for furnishing any of the work called for in a task order.

14 **Description of IT Professional Services and Pricing:** The Contractor shall provide a description of each type of IT Service offered under SIN 54151S IT Professional Services should be presented in the same manner as the Contractor sells to its commercial and other ordering activity customers. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles (labor categories) for those individuals who will perform the service should be provided.

Pricing for all IT Professional Services shall be in accordance with the Contractor’s customary commercial practices; e.g., hourly rates, monthly rates, term rates, and/or fixed prices, minimum general experience and minimum education.

**TERMS AND CONDITIONS APPLICABLE TO SIN 611420**

1 **Scope:** The Contractor shall provide training courses normally available to commercial customers, which will permit ordering activity users to make full, efficient use of general purpose commercial IT products. Training is restricted to training courses for those products within the scope of this solicitation.

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

2 **Order:** Written orders, EDI orders (GSA Advantage! And FACNET), credit card orders, and orders placed under BPAs shall be the basis for the purchase of training courses in accordance with the terms of this contract. Orders shall include the student’s name, course title, course date and time, and contracted dollar amount of the course.

3 **Time of Delivery:** The Contractor shall conduct training on the date (time, day, month, and year) agreed to by the Contractor and the ordering activity.

4 **Cancellation and Rescheduling:** The ordering activity will notify the Contractor at least seventy-two (72) hours before the scheduled training date if a student will be unable to attend. The Contractor will then permit the ordering activity to either cancel the order or reschedule the training at no additional charge. In the event the training class is rescheduled, the ordering activity will modify its original training order to specify the time and date of the rescheduled training class.

In the event the ordering activity fails to cancel or reschedule a training course within the time frame specified in paragraph a, above, the ordering activity will be liable for the contracted dollar amount of the training course. The Contractor agrees to permit the ordering activity to reschedule a student who fails to attend a training class within ninety (90) days from the original course date, at no additional charge.

The ordering activity reserves the right to substitute one student for another up to the first day of class. In the event the Contractor is unable to conduct training on the date agreed to by the Contractor and the ordering activity, the Contractor must notify the ordering activity at least seventy-two (72) hours before the scheduled training date.

5 **Follow-Up Support:** The Contractor agrees to provide each student with unlimited telephone support or online support for a period of one (1) year from the completion of the training course. During this period, the student may contact the Contractor’s instructors for refresher assistance and answers to related course curriculum questions.

6 **Price for Training:** The price that the ordering activity will be charged will be the ordering activity training price in effect at the time of order placement, or the ordering activity price in effect at the time the training course is conducted, whichever is less.
7  **Invoices and Payment:** Invoices for training shall be submitted by the Contractor after ordering activity completion of the training course. Charges for training must be paid in arrears (31 U.S.C. 3324). Prompt payment discount, if applicable, shall be shown on the invoice.

8  **Format and Content of Training:** The Contractor shall provide written materials (i.e., manuals, handbooks, texts, etc.) normally provided with course offerings. Such documentation will become the property of the student upon completion of the training class.

For hands-on training courses, there must be a one-to-one assignment of IT equipment to students.

The Contractor shall provide each student with a Certificate of Training at the completion of each training course.

The Contractor shall provide the following information for each training course offered:

- The course title and a brief description of the course content, to include the course format (e.g., lecture, discussion, hands-on training);
- The length of the course;
- Mandatory and desirable prerequisites for student enrollment;
- The minimum and maximum number of students per class;
- The locations where the course is offered;
- Class schedules; and
- Price (per student, per class (if applicable)).

For those courses conducted at the ordering activity’s location, instructor travel charges (if applicable), including mileage and daily living expenses (e.g., per diem charges) are governed by Pub. L. 99-234 and FAR Part 31.205-46, and are reimbursable by the ordering activity on order placed under the MAS, as applicable, in effect on the date(s) the travel is performed. Contractors cannot use GSA city pair contracts. The Industrial Funding Fee does NOT apply to travel and per diem charges.

For online training courses, a copy of all training material must be available for electronic download by the students.

9  **“No Charge” Training:** The Contractor shall describe any training provided with equipment and/or software provided under this contract, free of charge, in the space provided below.