Contract Period:
SEP 13, 2012 through SEP 12, 2022

Xator Corporation
1835 Alexander Bell Drive, Suite 210
Reston, VA 20190-4324
Phone: (703) 638-7107
Fax: (703) 638-6003
Internet Address: www.XatorCorp.com
Business Size: Small
Pricelist current through Modification PS-A824

Products and ordering information in this Authorized Multiple Award Schedule (MAS) Pricelist are also available on the GSA Advantage! System (http://www.gsaadvantage.gov).

<table>
<thead>
<tr>
<th>New SIN(s)</th>
<th>SIN Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>511210</td>
<td>Software Licenses</td>
</tr>
<tr>
<td>54151</td>
<td>Software Maintenance Services</td>
</tr>
<tr>
<td>54151HACS</td>
<td>HACS Highly Adaptive Cybersecurity Services (HACS)</td>
</tr>
<tr>
<td>54151HEAL</td>
<td>HEAL Health Information Technology Services</td>
</tr>
<tr>
<td>54151S</td>
<td>Information Technology Professional Services</td>
</tr>
<tr>
<td>811212</td>
<td>Computer and Office Machine Repair and Maintenance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Large Category</th>
<th>Subcategory</th>
<th>New MAS SIN</th>
<th>SIN Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Technology</td>
<td>IT Software</td>
<td>511210</td>
<td>Software Licenses</td>
</tr>
<tr>
<td>Information Technology</td>
<td>IT Software</td>
<td>54151</td>
<td>Software Maintenance Services</td>
</tr>
<tr>
<td>Information Technology</td>
<td>IT Services</td>
<td>54151HACS</td>
<td>HACS Highly Adaptive Cybersecurity Services (HACS)</td>
</tr>
<tr>
<td>Information Technology</td>
<td>IT Services</td>
<td>54151HEAL</td>
<td>HEAL Health Information Technology Services</td>
</tr>
<tr>
<td>Information Technology</td>
<td>IT Services</td>
<td>54151S</td>
<td>Information Technology Professional Services</td>
</tr>
<tr>
<td>Information Technology</td>
<td>IT Hardware</td>
<td>811212</td>
<td>Computer and Office Machine Repair and Maintenance</td>
</tr>
</tbody>
</table>
# Table of Contents

1.0 Information for Ordering Activities Applicable to All Special Item Numbers (SIN) .... 1

2.0 Terms and Conditions Applicable to Computer and Office Machine Repair and Maintenance (SIN 811212) ................................................................. 3

   2.1 Hardware Repair Service Order Terms ................................................................. 3
       2.1.1 Service Areas ............................................................................................... 3
       2.1.2 Ordering Repair Services ............................................................................. 4
       2.1.3 Loss or Damage ........................................................................................... 4
       2.1.4 Scope ......................................................................................................... 4
       2.1.5 Responsibilities of the Ordering Activity ...................................................... 4
       2.1.6 Responsibilities of the Contractor ................................................................. 5
       2.1.7 Repair Service Rate Provisions ..................................................................... 5
       2.1.8 Repair Parts/Spare Parts Rate Provisions ..................................................... 7
       2.1.9 Guarantee/Warranty—Repair Service and Repair Parts/Spare Parts .......... 7
       2.1.10 Invoices and Payments ............................................................................. 7

   2.2 Maintenance Service Order Terms ...................................................................... 7
       2.2.1 Service Areas .............................................................................................. 7
       2.2.2 Ordering Maintenance .................................................................................. 7
       2.2.3 Loss or Damage .......................................................................................... 8
       2.2.4 Scope ....................................................................................................... 8
       2.2.5 Responsibilities of the Ordering Activity ...................................................... 9
       2.2.6 Responsibilities of the Contractor ................................................................. 9
       2.2.7 Maintenance Rate Provisions ...................................................................... 9
       2.2.8 Invoices and Payments ............................................................................. 10

3.0 Terms and Conditions Applicable To Software Licenses (SIN 511210) and Software Maintenance Services (SIN 54151) ......................................................... 11

   3.1 Inspection/Acceptance ....................................................................................... 11
   3.2 Enterprise User License Agreements Requirements (EULA) ............................. 11
   3.3 GUARANTEE/Warranty .................................................................................... 12
   3.4 Technical Services ............................................................................................ 12
   3.5 Software Maintenance ..................................................................................... 12
   3.6 Funding of Term Licenses ................................................................................ 13
   3.7 Conversion from Term License to Perpetual License ........................................ 13
   3.8 Term License Cessation .................................................................................... 13
   3.9 Utilization Limitations for SINs Under the IT Software Subcategories ............ 14
   3.10 Software Conversions .................................................................................... 17
   3.11 Descriptions and Equipment Compatibility ................................................... 17
   3.12 Right-To-Copy Pricing .................................................................................. 17

4.0 Terms and Conditions Applicable to Highly Adaptive Cybersecurity Services (HACS) (SIN 54151HACS) ........................................................... 18

   4.1 SCOPE ........................................................................................................... 19
   4.2 Order ............................................................................................................ 21
   4.3 Performance of Services ................................................................................ 21
   4.4 Inspection of Services ..................................................................................... 21
   4.5 Responsibilities of the Contractor ................................................................... 21
4.6 Responsibilities of the Ordering Activity .................................................................22
4.7 Independent Contractor .........................................................................................22
4.8 Organizational Conflicts of Interest .....................................................................22
4.9 Invoices ..................................................................................................................22
4.10 Resumes ...............................................................................................................22
4.11 Approval of Subcontracts .....................................................................................23
4.12 Description of Highly Adaptive Cybersecurity Services and Pricing ..............23

5.0 Terms and Conditions Applicable To Information Technology Professional Services (SIN 54151S) ........................................................................................................24
5.1 Scope .....................................................................................................................24
5.2 Performance Incentives I-FSS-60 Performance Incentives (April 2000) ..............24
5.3 Order ......................................................................................................................24
5.4 Performance of Services .......................................................................................24
5.5 Stop-Work Order (FAR 52.242-15) (Aug 1989) .....................................................25
5.6 Inspection of Services ...........................................................................................25
5.7 Responsibilities of the Contractor ........................................................................26
5.8 Responsibilities of the Ordering Activity ...............................................................26
5.9 Independent Contractor .......................................................................................26
5.10 Organizational Conflicts of Interest .................................................................26
5.11 Invoices ...............................................................................................................26
5.12 Payments ..............................................................................................................27
5.13 Resumes ...............................................................................................................27
5.14 Incidental Support Costs .....................................................................................27
5.15 Approval of Subcontracts ...................................................................................27
5.16 Description of IT Services and Pricing ............................................................27

6.0 Terms and Conditions Applicable To Identity, Credentialing and Access Management (ICAM) (SIN 541519ICAM) ..........................................................................................28
6.1 Scope .....................................................................................................................28
6.3 Order ......................................................................................................................28
6.4 Performance of Services .......................................................................................28
6.5 Stop-Work Order (FAR 52.242-15) (Aug 1989) .....................................................29
6.6 Inspection of Services ...........................................................................................29
6.7 Responsibilities of the Contractor ........................................................................30
6.8 Responsibilities of the Ordering Activity ...............................................................30
6.9 Independent Contractor .......................................................................................30
6.10 Organizational Conflicts of Interest .................................................................30
6.11 Invoices ...............................................................................................................30
6.12 Payments ..............................................................................................................30
6.13 Resumes ...............................................................................................................31
6.14 Incidental Support Costs .....................................................................................31
6.15 Approval of Subcontracts ...................................................................................31
6.16 Description of IT Services and Pricing ............................................................31

7.0 Terms and Conditions Applicable To Health Information Technology Services (SIN 54151HEAL) ..........................................................................................32
7.1 SCOPE ..................................................................................................................32
7.2 Order ..................................................................................................................32
7.3 Performance of Services ..................................................................................32
7.4 Inspection of Services .....................................................................................33
7.5 Responsibilities of the Contractor ..................................................................33
7.6 Responsibilities of the Ordering Activity .......................................................33
7.7 Independent Contractor ..................................................................................33
7.8 Organizational Conflicts of Interest ..................................................................33
7.9 Invoices ..............................................................................................................34
7.10 Resumes ...........................................................................................................34
7.11 Incidental Support Costs ................................................................................34
7.12 Approval of Subcontracts ...............................................................................34
7.13 Description of Health IT Services and Pricing ..............................................34

8.0 Labor Category Descriptions ..............................................................................35

8.1 SIN 54151HACS - Highly Adaptive Cyber Security Services (HACS) .........35
  8.1.1 Program Manager .........................................................................................35
  8.1.2 Project Manager I .......................................................................................35
  8.1.3 Project Manager II ......................................................................................35
  8.1.4 Program & Policy Analyst 1 .........................................................................36
  8.1.5 Program & Policy Analyst 2 .........................................................................36
  8.1.6 Program & Policy Analyst 3 .........................................................................36
  8.1.7 Cyber Security Consultant ...........................................................................36
  8.1.8 Cyber Security Architect .............................................................................37
  8.1.9 Cyber Security Engineer 1 ...........................................................................37
  8.1.10 Cyber Security Engineer 2 ...........................................................................37
  8.1.11 Cyber Security Engineer 3 ...........................................................................37
  8.1.12 Cyber Security Analyst 1 ............................................................................38
  8.1.13 Cyber Security Analyst 2 ............................................................................38
  8.1.14 Cyber Security Analyst 3 ............................................................................38
  8.1.15 Cyber Security Specialist 1 .........................................................................38
  8.1.16 Cyber Security Specialist 2 .........................................................................39
  8.1.17 Cyber Security Specialist 3 .........................................................................39
  8.1.18 Cyber Hunting and Threat Intelligence Manager/Lead .........................39
  8.1.19 Cyber Hunting and Threat Intelligence Analyst 1 ..................................40
  8.1.20 Cyber Hunting and Threat Intelligence Analyst 2 ..................................40
  8.1.21 Cyber Hunting and Threat Intelligence Analyst 3 ..................................40
  8.1.22 Cyber Hunting and Threat Intelligence Analyst 4 ..................................41
  8.1.23 Penetration Testing Manager / Lead .........................................................41
  8.1.24 Penetration Tester 1 ..................................................................................41
  8.1.25 Penetration Tester 2 ..................................................................................42
  8.1.26 Penetration Tester 3 ..................................................................................42
  8.1.27 Penetration Tester 4 ..................................................................................42
  8.1.28 Incident Detection/Response Analyst 1 ....................................................43
  8.1.29 Incident Detection/Response Analyst 2 ....................................................43
  8.1.30 Incident Detection/Response Analyst 3 ....................................................43
  8.1.31 Risk and Vulnerability Assessment Analyst 1 ..........................................44
  8.1.32 Risk and Vulnerability Assessment Analyst 2 ..........................................44
SIN 54151S - Information Technology Professional Services

8.2.1 Program Administration Specialist I ................................................................. 45
8.2.2 Project Controls II ............................................................................................. 46
8.2.3 Project Manager I .............................................................................................. 46
8.2.4 Project Manager II ............................................................................................. 46
8.2.5 Quality Assurance Manager ............................................................................. 47
8.2.6 Systems Architect ............................................................................................. 47
8.2.7 Systems Programmer II .................................................................................... 47
8.2.8 Test Engineer I .................................................................................................. 47
8.2.9 Business System Analyst .................................................................................. 47
8.2.10 Database Specialist (Senior) ......................................................................... 48
8.2.11 Systems Engineer ............................................................................................ 48
8.2.12 Applications Developer (Journeyman) ........................................................... 48
8.2.13 Applications Developer (Senior) ..................................................................... 48
8.2.14 Quality Assurance Specialist (Journeyman) .................................................... 49
8.2.15 Technical Writer 2 .......................................................................................... 49
8.2.16 Data Security Analyst 1 .................................................................................. 49
8.2.17 Data Security Analyst 2 .................................................................................. 49
8.2.18 Data Security Analyst 3 .................................................................................. 50
8.2.19 Data Security Analyst 4 .................................................................................. 50
8.2.20 Data Security Analyst 5 .................................................................................. 50
8.2.21 Threat Analyst 1 .............................................................................................. 50
8.2.22 Threat Analyst 2 .............................................................................................. 51
8.2.23 Threat Analyst 3 .............................................................................................. 51
8.2.24 Threat Analyst 4 .............................................................................................. 51
8.2.25 Threat Analyst 5 .............................................................................................. 51
8.2.26 Forensics Analyst 1 ........................................................................................ 52
8.2.27 Forensics Analyst 2 ........................................................................................ 52
8.2.28 Forensics Analyst 3 ........................................................................................ 52
8.2.29 Forensics Analyst 4 ........................................................................................ 53
8.2.30 Forensics Analyst 5 ........................................................................................ 53
8.2.31 Security Assurance Analyst 1 ......................................................................... 54
8.2.32 Security Assurance Analyst 2 ......................................................................... 54
8.2.33 Security Assurance Analyst 3 ......................................................................... 54
8.2.34 Security Assurance Analyst 4 ......................................................................... 55
8.2.35 Security Assurance Analyst 5 ......................................................................... 55
8.2.36 Business Analyst 1 .......................................................................................... 55
8.2.37 Business Analyst 2 .......................................................................................... 56
8.2.38 Consultant 1 .................................................................................................... 56
8.2.39 Database Administrator 1 ................................................................................ 56
8.2.40 Database Administrator 2 ................................................................................ 56
8.2.41 Information Assurance 1 .................................................................................. 57
8.2.42 Information Assurance 3 ...............................................................................................57
8.2.43 Network Administrator 1.............................................................................................58
8.2.44 Network Administrator 2.............................................................................................58
8.2.45 Network Administrator 3.............................................................................................58
8.2.46 Network Architect.........................................................................................................58
8.2.47 Network Engineer 1.......................................................................................................58
8.2.48 Program Manager...........................................................................................................59
8.2.49 Programmer 1................................................................................................................60
8.2.50 Programmer 3................................................................................................................60
8.2.51 Programmer 5................................................................................................................60
8.2.52 Subject Matter Expert 1...............................................................................................60
8.2.53 Systems Administrator 1.............................................................................................60
8.2.54 Systems Administrator 3.............................................................................................60
8.2.55 Systems Analyst 1..........................................................................................................60
8.2.56 Systems Analyst 3..........................................................................................................61
8.2.57 Systems Analyst 4..........................................................................................................61
8.2.58 Systems Engineer 1.......................................................................................................61
8.2.59 Systems Engineer 3.......................................................................................................61
8.2.60 Systems Engineer 4.......................................................................................................62
8.2.61 Technical Writer 3..........................................................................................................62
8.2.62 Test Engineer 2...............................................................................................................62
8.2.63 Testing Specialist ..........................................................................................................62
8.2.64 Training Specialist 2.......................................................................................................62
8.2.65 Business Process Analyst 1........................................................................................63
8.2.66 Business Process Analyst 2........................................................................................63
8.2.67 Business Process Engineer 1........................................................................................63
8.2.68 Business Process Engineer 2........................................................................................63
8.2.69 Cyber Analyst 1............................................................................................................64
8.2.70 Cyber Analyst 2............................................................................................................64
8.2.71 Cyber Analyst 3............................................................................................................64
8.2.72 Cyber Engineer 1..........................................................................................................64
8.2.73 Cyber Engineer 2..........................................................................................................64
8.2.74 Cyber Engineer 3..........................................................................................................64
8.2.75 Security Engineer 1.......................................................................................................65
8.2.76 Security Engineer 2.......................................................................................................65
8.2.77 Security Engineer 3.......................................................................................................65
8.2.78 Data Warehouse Analyst 1........................................................................................65
8.2.79 Data Warehouse Engineer 1........................................................................................66
8.2.80 Disaster Recovery/COOP/Contingency Administrator 2 ...........................................66
8.2.81 Program & Policy Analyst 1.........................................................................................66
8.2.82 Program & Policy Analyst 3.........................................................................................66
8.2.83 Certification and Accreditation Analyst 1......................................................................67
8.2.84 Certification and Accreditation Analyst 3......................................................................67
8.2.85 Administrative Assistant 2...........................................................................................67
8.2.86 Contracts Administrator 2............................................................................................67
8.2.87 Financial Analyst 1.........................................................................................................68
SIN 54151HEAL - Health Information Technology Services .........................................68

8.3.1 IT Health Services Project Controls II ...............................................................68
8.3.2 IT Health Services Project Manager I .................................................................69
8.3.3 IT Health Services Project Manager II ...............................................................69
8.3.4 IT Health Services Quality Assurance Manager .................................................69
8.3.5 IT Health Systems Architect ...........................................................................70
8.3.6 IT Health Systems Programmer II .................................................................70
8.3.7 IT Health Services Test Engineer I .................................................................70
8.3.8 IT Health Database Specialist (Senior) ...........................................................71
8.3.9 IT Health Systems Engineer ..............................................................................71
8.3.10 IT Health Applications Developer (Journeyman) ..............................................71
8.3.11 IT Health Applications Developer (Senior) ......................................................71
8.3.12 IT Health Services Quality Assurance Specialist (Journeyman) ......................72
8.3.13 IT Health Data Security Analyst 1 .................................................................72
8.3.14 IT Health Data Security Analyst 2 .................................................................72
8.3.15 IT Health Data Security Analyst 3 .................................................................73
8.3.16 IT Health Data Security Analyst 4 .................................................................73
8.3.17 IT Health Data Security Analyst 5 .................................................................73
8.3.18 IT Health Services Threat Analyst 1 ..............................................................74
8.3.19 IT Health Services Threat Analyst 2 ..............................................................74
8.3.20 IT Health Services Threat Analyst 3 ..............................................................74
8.3.21 IT Health Services Threat Analyst 4 ..............................................................75
8.3.22 IT Health Services Threat Analyst 5 ..............................................................75
8.3.23 IT Health System Forensics Analyst 1 ............................................................76
8.3.24 IT Health System Forensics Analyst 2 ............................................................76
8.3.25 IT Health System Forensics Analyst 3 ............................................................76
8.3.26 IT Health System Forensics Analyst 4 ............................................................77
8.3.27 IT Health System Forensics Analyst 5 ............................................................77
8.3.28 IT Health System Security Assurance Analyst 1 .............................................78
8.3.29 IT Health System Security Assurance Analyst 2 .............................................78
8.3.30 IT Health System Security Assurance Analyst 3 .............................................79
8.3.31 IT Health System Security Assurance Analyst 4 .............................................79
8.3.32 IT Health System Security Assurance Analyst 5 .............................................80
8.3.33 IT Health System/Services Consultant 1 .......................................................80
8.3.34 IT Health System Database Administrator 1 ...................................................80
8.3.35 IT Health System Database Administrator 2 ...................................................81
8.3.36 IT Health System Information Assurance 1 ....................................................81
8.3.37 IT Health System Information Assurance 3 ....................................................81
8.3.38 IT Health System Network Administrator 1 .....................................................82
8.3.39 IT Health System Network Administrator 2 .....................................................82
8.3.40 IT Health System Network Administrator 3 .....................................................83
8.3.41 IT Health System Network Architect ...........................................................83
8.3.42 IT Health System Network Engineer 1 ...........................................................83
8.3.43 IT Health Services Program Manager ...........................................................84
8.3.44 IT Health Systems Programmer 1 ................................................................. 84
8.3.45 IT Health Systems Programmer 3 ................................................................. 84
8.3.46 IT Health Systems Programmer 5 ................................................................. 85
8.3.47 IT Health Services Subject Matter Expert 1 ................................................... 85
8.3.48 IT Health Systems Administrator 1 .............................................................. 85
8.3.49 IT Health Systems Administrator 3 .............................................................. 86
8.3.50 IT Health Services Systems Analyst 1 .......................................................... 86
8.3.51 IT Health Services Systems Analyst 3 .......................................................... 86
8.3.52 IT Health Services Systems Analyst 4 .......................................................... 87
8.3.53 IT Health Services Systems Engineer 1 ....................................................... 87
8.3.54 IT Health Services Systems Engineer 3 ....................................................... 87
8.3.55 IT Health Services Systems Engineer 4 ....................................................... 88
8.3.56 IT Health Services Test Engineer 2 .............................................................. 88
8.3.57 IT Health Services Testing Specialist .......................................................... 88
8.3.58 IT Health Systems Training Specialist ......................................................... 88
8.3.59 IT Health Systems Cyber Analyst 1 ............................................................. 89
8.3.60 IT Health Systems Cyber Analyst 2 ............................................................. 89
8.3.61 IT Health Systems Cyber Analyst 3 ............................................................. 89
8.3.62 IT Health Systems Cyber Engineer 1 ........................................................... 90
8.3.63 IT Health Systems Cyber Engineer 2 ........................................................... 90
8.3.64 IT Health Systems Cyber Engineer 3 ........................................................... 90
8.3.65 IT Health Systems Security Engineer 1 ....................................................... 90
8.3.66 IT Health Systems Security Engineer 2 ....................................................... 91
8.3.67 IT Health Systems Security Engineer 3 ....................................................... 91
8.3.68 IT Health Systems Data Warehouse Analyst 1 .............................................. 92
8.3.69 IT Health Systems Data Warehouse Engineer 1 ............................................ 92
8.3.70 IT Health Systems Program & Policy Analyst 1 .......................................... 92
8.3.71 IT Health Systems Program & Policy Analyst 3 .......................................... 92
8.3.72 IT Health Systems Certification and Accreditation Analyst 1 ...................... 93
8.3.73 IT Health Systems Certification and Accreditation Analyst 3 ...................... 93
8.3.74 IT Health Systems Facility Engineer 1 .......................................................... 94

9.0 Labor Category Pricing .......................................................................................... 95
9.1 Highly Adaptive Cybersecurity Services (HACS) (SIN 54151HACS) .................. 95
9.2 Information Technology Professional Services (SIN 54151S) ............................ 96
9.3 Health Information Technology Services (SIN 54151HEAL) .............................. 98
1.0 Information for Ordering Activities Applicable to All Special Item Numbers (SIN)

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

NEW SIN(s)
Special Item No.: 511210 Software Licenses
Special Item No.: 54151 Software Maintenance Services
Special Item No.: 54151HACS Highly Adaptive Cybersecurity Services (HACS)
Special Item No.: 54151HEAL Health Information Technology Services
Special Item No.: 54151S Information Technology Professional Services
Special Item No.: 811212 Computer and Office Machine Repair and Maintenance

1.b. Identification of the lowest priced model number and lowest unit price for that model for each special item number awarded in the contract. This price is the Government price based on a unit of one, exclusive of any quantity/dollar volume, prompt payment, or any other concession affecting price. Those contracts that have unit prices based on the geographic location of the customer, should show the range of the lowest price, and cite the areas to which the prices apply.

See Price Sheet

1.c. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles, experience, functional responsibility and education for those types of employees or subcontractors who will perform services shall be provided. If hourly rates are not applicable, indicate “Not applicable” for this item.

Labor Category Descriptions for all SINs begin on page 35

2. Maximum order. $500,000
3. Minimum order. $100
4. Geographic coverage (delivery area). Domestic delivery is delivery within the 48 contiguous states, Alaska, Hawaii, Puerto Rico, Washington, DC, and U.S. Territories. Domestic delivery also includes a port or consolidation point, within the aforementioned areas, for orders received from overseas activities.
5. Point(s) of production (city, county, and State or foreign country). United States of America
6. Discount from list prices or statement of net price. Government prices are net.
7. Quantity discounts. None
8. Prompt payment terms. 0% - 30 days from receipt of invoice or date of acceptance, whichever is later.
9.a. Notification that Government purchase cards are accepted at or below the micro-purchase threshold. The Government Purchase Card will be accepted for payment on orders at or below the micro-purchase threshold.
9.b. Notification whether Government purchase cards are accepted or not accepted above the micro-purchase threshold. The Government Purchase Card will be accepted for payment on orders above the micro-purchase threshold.
10. Foreign items (list items by country of origin). None
11.a. Time of delivery. (Contractor inserts number of days.)
11.b. Expedited Delivery. The Contractor will insert the sentence “Items available for expedited delivery are noted in this price list.” under this heading. The Contractor may use a symbol of its choosing to highlight items in its price lists that have expedited delivery.

Contact Contractor for availability

11.c. Overnight and 2-day Delivery. The Contractor will indicate whether overnight and 2-day delivery are available. Also, the Contractor will indicate that the schedule customer may contact the Contractor for rates for overnight and 2-day delivery.

Contact Contractor for availability

11.d. Urgent Requirements. The Contractor will note in its price list the “Urgent Requirements” clause of its contract and advise agencies that they can also contact the Contractor’s representative to effect a faster delivery.

When the Federal Supply Schedule contract delivery period does not meet the bona fide urgent delivery requirements of an ordering activity, ordering activities are encouraged, if time permits, to contact the Contractor for the purpose of obtaining accelerated delivery. The Contractor shall reply to the inquiry within 3 workdays after receipt. (Telephonic replies shall be confirmed by the Contractor in writing.) If the Contractor offers an accelerated delivery time acceptable to the ordering activity, any order(s) placed pursuant to the agreed upon accelerated delivery time frame shall be delivered within this shorter delivery time and in accordance with all other terms and conditions of the contract.

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

13.a. Ordering address. Xator Corporation
1835 Alexander Bell Drive, Suite 210
Reston, VA  20191-4324

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

14. Payment address(es).

Remit Payment by EFT to: Xator Corporation c/o JP Morgan Chase
ABA# 021000021
Acct # 816175702
TIN: 90-0243400
Cage Code: 393S5

---

SPECIAL ITEM NUMBER DELIVERY TIME (Days ARO)
511210 30 Days
54151 Upon mutual agreement with Ordering Agency
54151HACS Upon mutual agreement with Ordering Agency
54151S Upon mutual agreement with Ordering Agency
541515HEAL Upon mutual agreement with Ordering Agency
811212 30 Days
15. Warranty provision.

Unless specified otherwise in this contract, the Contractor’s standard commercial guarantee/warranty as stated in the contract’s commercial pricelist will apply to this contract.

The Contractor warrants and implies that the items delivered hereunder are merchantable and fit for use for the particular purpose described in this contract.

Limitation of Liability. Except as otherwise provided by an express or implied warranty, the Contractor will not be liable to the ordering activity for consequential damages resulting from any defect or deficiencies in accepted items.

16. Export packing charges, if applicable. **Not Applicable**

17. Terms and conditions of Government purchase card acceptance (any thresholds above the micro-purchase level). **None**

18. Terms and conditions of rental, maintenance, and repair (if applicable). **Contact Contractor**

19. Terms and conditions of installation (if applicable). **Products are normally self-installable if assistance is necessary with installation; professional services are available through this GSA Schedule under SIN 54151S.**

20. Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices (if applicable). **Not Applicable**

20.a. Terms and conditions for any other services (if applicable). **Not Applicable**

21. List of service and distribution points (if applicable). **Not Applicable**

22. List of participating dealers (if applicable). **Not Applicable**

23. Preventive maintenance (if applicable). **Not Applicable**

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

24.b. If applicable, indicate that Section 508 compliance information is available on Electronic and Information Technology (EIT) supplies and services and show where full details can be found (e.g. contractor’s website or other location.) The EIT standards can be found at: www.Section508.gov/. **Not Applicable**

25. Data Universal Number System (DUNS) number. **360698687**

26. Notification regarding registration in SAM.gov (formerly the Central Contractor Registration) database. **CAGE Code: 393S5**

**2.0 Terms and Conditions Applicable to Computer and Office Machine Repair and Maintenance (SIN 811212)**

**2.1 Hardware Repair Service Order Terms**

**2.1.1 Service Areas**

a. The repair service rates listed herein are applicable to any ordering activity location.
within a 50-mile radius of the Contractor/Original Equipment Manufacturer (OEM) service points. If any additional charge is to apply because of the greater distance from the Contractor/OEM service locations, the mileage rate or other distance factor shall be negotiated at the Task Order level.

b. When repair services cannot be performed at the ordering activity installation site, the repair services will be performed at the Contractor's plant(s).

2.1.2 Ordering Repair Services

a. Agencies may use written orders, EDI orders, credit card orders, or blanket purchase agreements (BPAs) or small order procedures for ordering repair service and/or repair parts/spare parts under this contract. Orders for repair service shall not extend beyond the end of the contract period.

b. When repair service is ordered, only one chargeable repairman shall be dispatched to perform repair service unless the ordering activity agrees, in advance, that additional repair personnel are required to effect repairs.

2.1.3 Loss or Damage

When the Contractor removes equipment to its/OEM location for repairs, the Contractor shall be responsible for any damage or loss, from the time the equipment is removed from the ordering activity installation, until the equipment is returned to such installation.

2.1.4 Scope

a. The Contractor shall provide repair service and repair parts/spare parts for all equipment listed herein, as requested by the ordering activity during the contract term. Repair service and repair parts/spare parts shall apply exclusively to the equipment types/models within the scope of the Information Technology Category.

b. Equipment placed under maintenance and/or service shall be in good operating condition.

i. In order to determine that the equipment is in good operating condition, the equipment shall be subject to inspection by the Contractor, without charge to the ordering activity.

ii. Costs of any repairs performed for the purpose of placing the equipment in good operating condition shall be borne by the Contractor, if the equipment was under the Contractor/OEM guarantee/warranty or maintenance responsibility prior to the effective date of the maintenance order.

iii. If the equipment was not under the Contractor/OEM responsibility, the costs necessary to place the equipment in proper operating condition are to be borne by the ordering activity, in accordance with the provisions of the contract.

2.1.5 Responsibilities of the Ordering Activity

a. Agencies may use written orders, EDI orders, credit card orders, blanket purchase agreements (BPAs), or small order procedures for ordering repair service and/or repair parts/spare parts under this contract. Orders for repair service shall not extend beyond the end of the contract period.

b. When repair service is ordered, only one chargeable repairman shall be dispatched to perform repair service, unless the ordering activity agrees, in advance, that additional
repair personnel are required to effect repairs.

c. All parts, furnished as spares or as repair parts in connection with the repair of equipment, unless otherwise indicated in the price list shall be new, standard parts manufactured by the OEM.

d. Ordering activity personnel shall not perform or attempt repairs to equipment while such equipment is under the purview of a repair order, unless agreed to by the Contractor.

e. Subject to security regulations, the ordering activity shall permit access to the equipment which is to be repaired.

f. If the Ordering Activity desires a factory authorized/certified service personnel, then this should be clearly stated in the task or delivery order.

2.1.6 Responsibilities of the Contractor

a. For equipment not covered by a maintenance contract or warranty, the Contractor's repair service personnel shall complete repairs as soon as possible after notification by the ordering activity that service is required. Within the service areas, this repair service should normally be done within 4 hours after notification.

b. If the Ordering Activity task or delivery order specifies a factory authorized/certified service personnel then the Contractor is obligated to provide such a factory authorized/certified service personnel for the equipment to be repaired or serviced, unless otherwise agreed to in advance between the Ordering Activity and the Contractor.

2.1.7 Repair Service Rate Provisions

a. Charges. Charges for repair service will include the labor charge, computed at the rates set forth in the price list, for the time during which repairmen are actually engaged in work, and, when applicable, the charge for travel or transportation.

b. All parts shall be furnished at the prices indicated in the price list in the Contractor's commercial pricelist.

c. Multiple Machines. When repairs are ordered by an ordering activity on two or more machines located in one or more buildings within walking distance of each other, the charges will be computed from the time the repairman commences work on the first machine, until the work is completed on the last machine. The time required to go from one machine to another, or from one building to another, will be considered actual work performance, and chargeable to the ordering activity, provided the time consumed in going between machines (or buildings) is reasonable.

d. At the Contractor/OEM’s Facility

i. When equipment is returned to the Contractor/OEM’s Facility for adjustments or repairs which are not covered by the guarantee/warranty provision, the cost of transportation, packing, etc., from the ordering activity location to the Contractor's plant, and return to the ordering activity location, shall be borne by the ordering activity.
ii. The ordering activity should not return defective equipment to the Contractor/OEM for adjustments and repairs or replacement without prior consultation and instruction.

e. **At the Ordering Activity Location (Within Established Service Areas)**

i. When equipment is repaired at the ordering activity location, and repair service rates are established for service areas or zones, the listed rates are applicable to any ordering activity location within such service areas or zones. No extra charge, time, or expense will be allowed for travel or transportation of repairmen or machines to or from the ordering activity office, such overhead is included in the repair service rates.

f. **At the Ordering Activity Location (Outside Established Service Areas)**

i. If repairs are to be made at the ordering activity location, and the location is outside the service area terms defined in the GSA Price list. Rates negotiated at the task order will apply.

ii. When the overall travel charge computed at the above mileage rate is unreasonable (considering the time required for travel, actual and necessary transportation costs, and the allowable ordering activity per diem rate for each night the repairman is required to remain overnight at the ordering activity location), the ordering activity shall have the option of reimbursing the Contractor for actual costs, provided that the actual costs are reasonable and allowable. The Contractor shall furnish the ordering activity with a report of travel performed and related expenses incurred. The report shall include departure and arrival dates, times, and the applicable mode of travel.

g. **Labor Rates**

i. **Regular Hours** - The Regular Hours repair service rates listed herein shall entitle the ordering activity to repair service during the period 8:00 a.m. to 5:00 p.m., Monday through Friday, exclusive of holidays observed at the ordering activity location. There shall be no additional charge for repair service which was requested during Regular Hours, but performed outside the Regular Hours defined above, at the convenience of the Contractor.

ii. **After Hours** - When the ordering activity requires that repair service be performed outside the Regular Hours defined above, charges for such service, if any, will be specified in the GSA Price List (I-FSS-600 CONTRACT PRICE LISTS (OCT 2016). Periods of less than one hour will be prorated to the nearest quarter hour. The Regular Hours rates defined above shall apply when repair service is requested during Regular Hours (8:00am to 5:00pm), but performed After Hours at the convenience of the Contractor.

iii. **Sundays and Holidays** - When the ordering activity requires that repair service be performed on Sundays and Holidays observed at the ordering activity location, the Sundays and Holidays repair service rates shall apply, and will be specified in the GSA Price List (I-FSS-600 CONTRACT PRICE LISTS (OCT 2016). Periods of less than one hour will be prorated to the nearest quarter hour.
2.1.8 Repair Parts/Spare Parts Rate Provisions

All parts, furnished as spares or as repair parts in connection with the repair of equipment, unless otherwise indicated in this pricelist, shall be new, standard parts manufactured by the equipment manufacturer.

2.1.9 Guarantee/Warranty—Repair Service and Repair Parts/Spare Parts

a. Repair Service - All repair work will be guaranteed/warranted as stated in the contract's pricelist

b. Repair Parts/Spare Parts - All parts, furnished either as spares or repairs parts will be guaranteed/warranted for a period outlined in the price list.

2.1.10 Invoices and Payments

a. Repair Service and Repair Parts/Spare Parts
   i. Invoices for repair service and parts shall be submitted by the Contractor/OEM as soon as possible after completion of work. Payment under blanket purchase agreements will be made quarterly or monthly, except where cash payment procedures are used.
   ii. Invoices shall be submitted separately to each ordering activity office ordering services under the contract. The cost of repair parts shall be shown as a separate item on the invoice, and shall be priced in accordance with paragraph #7(a), above. PROMPT PAYMENT DISCOUNT, IF APPLICABLE, SHALL BE SHOWN ON THE INVOICE.

2.2 Maintenance Service Order Terms

2.2.1 Service Areas

a. The maintenance and/or repair service rates listed herein are applicable to any ordering activity location within a 50-mile radius of the Contractor/Original Equipment Manufacturer (OEM) service points. If any additional charge is to apply because of the greater distance from the Contractor/OEM service locations, the mileage rate or other distance factor shall be negotiated at the Task Order level.

b. When maintenance and/or repair services cannot be performed at the ordering activity installation site, the repair services will be performed at the Contractor's plant(s).

2.2.2 Ordering Maintenance

a. Agencies may use written orders, EDI orders, credit card orders, or BPAs, for ordering maintenance under this contract. The Contractor shall confirm orders within fifteen (15) calendar days from the date of receipt, except that confirmation of orders shall be considered automatic for renewals for maintenance (Special Item Number 811212). Automatic acceptance of order renewals for maintenance service shall apply for machines which may have been discontinued from use for temporary periods of time not longer than 120 calendar days. If the order is not confirmed by the Contractor as prescribed by this paragraph, the order shall be considered to be confirmed by the Contractor.

b. Maintenance service shall commence on a mutually agreed upon date, which will be
written into the maintenance order. Maintenance orders shall not be made effective before the expiration of any applicable maintenance and parts guarantee/warranty period associated with the purchase of equipment. **Orders for maintenance service shall not extend beyond the end of the contract period.**

c. Maintenance may be discontinued by the ordering activity on thirty (30) calendar days written notice, or shorter notice when agreed to by the Contractor; such notice to become effective thirty (30) calendar days from the date on the notification. However, the ordering activity may extend the original discontinuance date upon written notice to the Contractor, provided that such notice is furnished at least ten (10) calendar days prior to the original discontinuance date.

d. Annual Funding. When annually appropriated funds are cited on a maintenance order, the period of maintenance shall automatically expire on September 30th of the contract period, or at the end of the contract period, whichever occurs first. Renewal of a maintenance order citing the new appropriation shall be required, if maintenance is to continue during any remainder of the contract period.

e. Cross-year Funding Within Contract Period. Where an ordering activity’s specific appropriation authority provides for funds in excess of a 12 month, fiscal year period, the ordering activity may place an order under this schedule contract for a period up to the expiration of the contract period, notwithstanding the intervening fiscal years.

f. Ordering activities should notify the Contractor in writing thirty (30) calendar days prior to the expiration of maintenance service, if maintenance is to be terminated at that time. **Orders for continued maintenance will be required if maintenance is to be continued during the subsequent period.**

2.2.3 Loss or Damage

When the Contractor removes equipment to its/OEM location for repairs, the Contractor shall be responsible for any damage or loss, from the time the equipment is removed from the ordering activity installation, until the equipment is returned to such installation.

2.2.4 Scope

a. The Contractor shall provide maintenance for all equipment listed herein, as requested by the ordering activity during the contract term. Repair service and repair parts/spare parts shall apply exclusively to the equipment types/models within the scope of this Information Technology Category.

b. Equipment placed under maintenance service shall be in good operating condition.
   i. In order to determine that the equipment is in good operating condition, the equipment shall be subject to inspection by the Contractor, without charge to the ordering activity.
   ii. Costs of any repairs performed for the purpose of placing the equipment in good operating condition shall be borne by the Contractor, if the equipment was under the Contractor/OEM guarantee/warranty or maintenance responsibility prior to the effective date of the maintenance order
   iii. If the equipment was not under the Contractor/OEM responsibility, the costs necessary to place the equipment in proper operating condition are to be borne by the ordering activity, in accordance with the provisions of the contract.
2.2.5 Responsibilities of the Ordering Activity

a. Ordering activity personnel shall not perform maintenance or attempt repairs to equipment while such equipment is under the purview of a maintenance order, unless agreed to by the Contractor.

b. Subject to security regulations, the ordering activity shall permit access to the equipment which is to be maintained or repaired.

c. If the Ordering Activity desires a factory authorized/certified service personnel, then this should be clearly stated in the task or delivery order.

2.2.6 Responsibilities of the Contractor

a. For equipment not covered by a maintenance contract or warranty, the Contractor's repair service personnel shall complete repairs as soon as possible after notification by the ordering activity that service is required. Within the service areas, this repair service should normally be done within 4 hours after notification.

b. If the Ordering Activity task or delivery order specifies a factory authorized/certified service personnel then the Contractor is obligated to provide such a factory authorized/certified service personnel for the equipment to be repaired or serviced, unless otherwise agreed to in advance between the Ordering Activity and the Contractor.

2.2.7 Maintenance Rate Provisions

a. The Contractor shall bear all costs of maintenance, including labor, parts, and such other expenses as are necessary to keep the equipment in good operating condition, provided that the required repairs are not occasioned by fault or negligence of the ordering activity.

i. REGULAR HOURS - The basic monthly rate for each make and model of equipment shall entitle the ordering activity to maintenance service during a mutually agreed upon nine (9) hour principal period of maintenance, Monday through Friday, exclusive of holidays observed at the ordering activity location.

ii. AFTER HOURS - Should the ordering activity require that maintenance be performed outside of Regular Hours, charges for such maintenance, if any, will be specified in the GSA Price List (I-FSS-600 CONTRACT PRICE LISTS (OCT 2016). Periods of less than one hour will be prorated to the nearest quarter hour.

iii. TRAVEL AND TRANSPORTATION - If any charge is to apply, over and above the regular maintenance rates, due to the distance between the ordering activity location and the Contractor/OEM service area, the charge will be negotiated at the Task Order level. Travel will be charged in accordance with the then current Joint Travel Regulations.

iv. QUANTITY DISCOUNTS - Quantity discounts from listed maintenance service rates for multiple equipment owned and/or leased by an ordering activity are indicated below:

<table>
<thead>
<tr>
<th>Quantity Range</th>
<th>Discounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>
2.2.8 Invoices and Payments

a. Maintenance Service

i. Invoices for maintenance service shall be submitted by the Contractor on a quarterly or monthly basis, after the completion of such period. Maintenance charges must be paid in arrears (31 U.S.C. 3324). PROMPT PAYMENT DISCOUNT, IF APPLICABLE, SHALL BE SHOWN ON THE INVOICE.

ii. Payment for maintenance service of less than one month’s duration shall be prorated at 1/30th of the monthly rate for each calendar day.
3.0 Terms and Conditions Applicable To Software Licenses (SIN 511210) and Software Maintenance Services (SIN 54151)

511210 Includes both term and perpetual software licenses and maintenance. Includes operating system software, application software, EDI translation and mapping software, enabled email message based applications, Internet software, database management applications, and other software.

54151 Software maintenance services creates, designs, implements, and/or integrates customized changes to software that solve one or more problems and is not included with the price of the software. Software maintenance services includes person-to-person communications regardless of the medium used to communicate: telephone support, online technical support, customized support, and/or technical expertise which are charged commercially.

Additional Sin Description:

TERM LICENSES: The word "Term" is defined in this Solicitation as "a limited period of time". Term Software Licenses have a limited duration and are not owned in perpetuity. Unless Offerors provide an option for converting Term licenses into perpetual licenses, users lose the right to use these licenses upon the end of the term period. This SIN is NOT Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS) as defined in SIN 518210C - Cloud and Cloud-Related IT Professional Services. Term Software Licenses are distinct from Electronic Commerce and Subscription Services (SIN 54151ECOM).

PERPETUAL LICENSES: The word "perpetual" is defined in this Solicitation as "continuing forever, everlasting, valid for all time".

3.1 Inspection/Acceptance

The Contractor shall only tender for acceptance those items that conform to the requirements of this contract. The ordering activity reserves the right to inspect or test any software that has been tendered for acceptance. The ordering activity may require repair or replacement of nonconforming software at no increase in contract price. The ordering activity must exercise its post acceptance rights

   (1) within a reasonable time after the defect was discovered or should have been discovered; and
   (2) before any substantial change occurs in the condition of the software, unless the change is due to the defect in the software.


3.2 Enterprise User License Agreements Requirements (EULA)

Commercial Supplier Agreements to include Enterprise User License Agreements or Terms of Service (TOS) agreements. The Contractor shall provide all Commercial Supplier Agreements to include Enterprise User License Agreements or Terms of Service (TOS) agreements in an editable Microsoft Office (Word) format for review prior to award.
3.3 GUARANTEE/Warranty

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

b. The Contractor warrants and implies that the items delivered hereunder are merchantable and fit for use for the particular purpose described in this contract. If no implied warranties are given, an express warranty of at least 60 days must be given in accordance with FAR 12.404(b)(2)

c. Limitation of Liability. Except as otherwise provided by an express or implied warranty, the Contractor will not be liable to the ordering activity for consequential damages resulting from any defect or deficiencies in accepted items.

3.4 Technical Services

The Contractor, without additional charge to the ordering activity, shall provide a hot line technical support number for the purpose of providing user assistance and guidance in the implementation of the software. To be determined at the Task Order level.

3.5 Software Maintenance

a. Software maintenance as it is defined: (select software maintenance type):

1. Software Maintenance as a Product (SIN 511210)

Software maintenance as a product includes the publishing of bug/defect fixes via patches and updates/upgrades in function and technology to maintain the operability and usability of the software product. It may also include other no charge support that are included in the purchase price of the product in the commercial marketplace. No charge support includes items such as user blogs, discussion forums, on-line help libraries and FAQs (Frequently Asked Questions), hosted chat rooms, and limited telephone, email and/or web-based general technical support for user’s self-diagnostics.

Software maintenance as a product DOES NOT include the creation, design, implementation, integration, etc. of a software package. These examples are considered software maintenance services under SIN 54151 Software Maintenance Services.

Software Maintenance as a product is billed at the time of purchase.

2. Software Maintenance as a Service (SIN 54151)

Software maintenance services creates, designs, implements, and/or integrates customized changes to software that solve one or more problems and is not included with the price of the software. Software maintenance services includes person-to-person communications regardless of the medium used to communicate: telephone support, on-line technical support, customized support, and/or technical expertise which are charged commercially. Software maintenance services are billed in arrears in accordance with 31 U.S.C. § 3324.

b. Invoices for maintenance service shall be submitted by the Contractor on a quarterly or monthly basis, after the completion of such period. Maintenance charges must be paid in arrears (31 U.S.C. 3324). PROMPT PAYMENT DISCOUNT, IF APPLICABLE, SHALL BE SHOWN ON THE INVOICE.
3.6 Funding of Term Licenses

a. Annual Funding. When using annually appropriated funds are cited on an order for term licenses, the period of the term licenses shall automatically expire on September 30 of the contract period.

b. Cross-Year Funding Within Contract Period. Where an ordering activity’s specific appropriation authority provides for funds in excess of a 12 month (fiscal year) period, the ordering activity may place an order under this schedule contract for a period up to the expiration of the contract period, notwithstanding the intervening fiscal years.

c. Ordering activities should notify the Contractor in writing thirty (30) calendar days prior to the expiration of an order, if the term licenses is to be terminated at that time. Orders for the continuation of term licenses will be required if the term licenses and/or maintenance is to be continued during the subsequent period.

3.7 Conversion from Term License to Perpetual License

a. When a contractor commercially offers conversions of term licenses to perpetual licenses, and an ordering activity requests such a conversion, the contractor shall provide the total amount of conversion credits available for the subject software within ten (10) calendar days after placing the order.

b. When conversion credits are provided, they shall continue to accrue from one contract period to the next, provided the software has been continually licensed without interruption.

c. The term license for each software product shall be discontinued on the day immediately preceding the effective date of conversion from a term license to a perpetual license.

d. When conversion from term licenses to perpetual licenses is offered, the price the ordering activity shall pay will be the perpetual license price that prevailed at the time such software was initially ordered under a term license, or the perpetual license price prevailing at the time of conversion from a term license to a perpetual license, whichever is the less, minus an amount equal to a percentage of all term license payments during the period that the software was under a term license within the ordering activity.

3.8 Term License Cessation

a. After a software product has been on a continuous term license for a period of XX months (TBD at order level), a fully paid-up, non-exclusive, perpetual license for the software product shall automatically accrue to the ordering activity. The period of continuous term license for automatic accrual of a fully paid-up perpetual license does not have to be achieved during a particular fiscal year; it is a written Contractor commitment which continues to be available for software that is initially ordered under this contract, until a fully paid-up perpetual license accrues to the ordering activity. However, should the term license of the software be discontinued before the specified period of the continuous term license has been satisfied, the perpetual license accrual shall be forfeited. Contractors who do not commercially offer conversions of term licenses to perpetual licenses shall indicate that their term licenses are not eligible for conversion at any time.

b. Each separately priced software product shall be individually enumerated, if different
accrual periods apply for the purpose of perpetual license attainment.

c. The Contractor agrees to provide updates and software maintenance services for the software after a perpetual license has accrued, at the prices and terms of Special Item Number 54151 – Software Maintenance Services, if the licensee elects to order such services. Title to the software shall remain with the Contractor.

3.9 Utilization Limitations for SINs Under the IT Software Subcategories

a. Software acquisition is limited to commercial computer software defined in FAR Part 2.101.

b. When acquired by the ordering activity, commercial computer software and related documentation so legend shall be subject to the following:

1. Title to and ownership of the software and documentation shall remain with the Contractor, unless otherwise specified.

2. Software licenses are by site and by ordering activity. An ordering activity is defined as a cabinet level or independent ordering activity. The software may be used by any subdivision of the ordering activity (service, bureau, division, command, etc.) that has access to the site the software is placed at, even if the subdivision did not participate in the acquisition of the software. Further, the software may be used on a sharing basis where multiple agencies have joint projects that can be satisfied by the use of the software placed at one ordering activity's site. This would allow other agencies access to one ordering activity's database. For ordering activity public domain databases, user agencies and third parties may use the computer program to enter, retrieve, analyze and present data. The user ordering activity will take appropriate action by instruction, agreement, or otherwise, to protect the Contractor's proprietary property with any third parties that are permitted access to the computer programs and documentation in connection with the user ordering activity's permitted use of the computer programs and documentation. For purposes of this section, all such permitted third parties shall be deemed agents of the user ordering activity.

3. Except as is provided in paragraph 9.b(2) above, the ordering activity shall not provide or otherwise make available the software or documentation, or any portion thereof, in any form, to any third party without the prior written approval of the Contractor. Third parties do not include prime Contractors, subcontractors and agents of the ordering activity who have the ordering activity's permission to use the licensed software and documentation at the facility, and who have agreed to use the licensed software and documentation only in accordance with these restrictions. This provision does not limit the right of the ordering activity to use software, documentation, or information therein, which the ordering activity may already have or obtains without restrictions.

4. The ordering activity shall have the right to use the software and documentation with the run-time computing environment (e.g. operating system, virtual machine, mobile operating system, processor etc.) to be specifically identified for which it is acquired at any other facility/user device to which that time computing environment may be transferred, or in cases of Disaster Recovery, the ordering activity has the right to transfer the software to another site/user device if the ordering activity site for which it is acquired is deemed to be unsafe for ordering activity personnel; to use the software and documentation with a backup time computing environment when the
primary is inoperative; to copy computer programs for safekeeping (archives) or backup purposes; to transfer a copy of the software to another site/user for purposes of benchmarking new hardware and/or software; and to modify the software and documentation or combine it with other software, provided that the unmodified portions shall remain subject to these restrictions.

5. "Commercial Computer Software" may be marked with the Contractor's standard commercial restricted rights legend, but the schedule contract and schedule pricelist, including this clause, "Utilization Limitations" are the only governing terms and conditions, and shall take precedence and supersede any different or additional terms and conditions included in the standard commercial legend.

6. Licensee Data belongs exclusively to Licensee, regardless of where the Data may reside at any moment in time including, but not limited to Licensor hardware, networks or other infrastructure and facilities where Data may reside, transit through or be stored from time to time. Licensor makes no claim to a right of ownership in Licensee Data. Licensor agrees to keep the Licensee Data Confidential as that term is defined in the relevant FAR and DFARS provisions pertaining to Confidential Information and Confidentiality. Licensor is not permitted to use Licensee's data for a purpose that is not explicitly granted in writing by Licensee. Upon Licensee request, for any reason whatsoever, Licensor must promptly return all Licensee Data in Licensor's possession in a format as may be designated at the time of request by Licensee.

7. Licensee may create or hire others (including Licensor) to create modifications, customizations or other enhancements to the Software which might be classified as “Derivative Works” of the software. Unless otherwise negotiated and mutually agreed upon at the order level, the intellectual property (IP) rights to the Derivative Works shall be owned by the owner of the underlying intellectual property. The Derivative Work[s] shall be made available to the Licensee through a royalty free, perpetual worldwide, no charge license to the Licensee.

c. Utilization Limitations for Perpetual Licenses

1. Software Asset Identification Tags (SWID) (Option 1 Perpetual License) Option 1 is applicable when the Offeror agrees to include the International Organization for Standardization/International Electrotechnical Commission 19770-2 (ISO/IEC 19770-2:2015) standard identification tag (SWID Tag) as an embedded element in the software. An ISO/IEC 19970-2 tag is a discoverable identification element in software that provides licensees enhanced asset visibility. Enhance visibility supports both the goals of better software asset management and license compliance. Offerors may use the National Institute of Standards and Technology (NIST) document “NISTIR 8060: Guidelines for Creation of Interoperable Software Identification (SWID) Tags,” December 2015 to determine if they are in compliance with the ISO/IEC 19770-2 standard.

2. Section 837 of The Federal Information Technology Acquisition Reform Act (FITARA) of 2014, requires GSA to seek agreements with software vendors that enhance government-wide acquisition, shared use, and dissemination of software, as well as compliance with end user license agreements. The Megabyte Act of 2016 requires agencies to inventory software assets and to make informed decisions prior to new software acquisitions. In June of 2016, the Office of Management and Budget issued
guidance on software asset management requiring each CFO Act (Public Law 101-576 – 11/15/1990) agency to begin software inventory management (M-16-12). To support these requirements, Offerors may elect to include the terms of Option 1 and/or Option 2, which support software asset management and government-wide reallocation or transferability of perpetually licensed software.

d. Reallocation of Perpetual Software (Option 2 Perpetual License)

1. The purpose of SIN 511210 OPTION 2 is to allow ordering activities to transfer software assets for a pre-negotiated charge to other ordering activities.

2. When an ordering activity becomes aware that a reusable software asset may be available for transfer, it shall contact the Contractor, identify the software license or licenses in question, and request that these licenses be reallocated or otherwise made available to the new ordering activity.

3. Contractors shall release the original ordering activity from all future obligations under the original license agreement and shall present the new ordering activity with an equivalent license agreement. When the new ordering activity agrees to the license terms, henceforth any subsequent infringement or breach of licensing obligations by the new ordering activity shall be a matter exclusively between the new ordering activity and the Contractor.

4. The original ordering activity shall de-install, and/or make unusable all of the software assets that are to be transferred. It shall have no continuing right to use the software and any usage shall be considered a breach of the Contractor’s intellectual property and a matter of dispute between the original ordering activity/original license grantee and the licensor.

5. As a matter of convenience, once the original licenses are deactivated, di-installed, or made otherwise unusable by the original ordering activity or license grantee, the Contractor may elect to issue new licenses to the new ordering activity to replace the old licenses. When new licenses are not issued, the Contractor shall provide technical advice on how best to achieve the functional transfer of the software assets.

6. Software assets that are eligible for transfer that have lapsed Software Maintenance Services (SIN 54151) may require a maintenance reinstatement fee, chargeable to the new ordering activity or license grantee. When such a fee is paid, the new ordering activity shall receive all the rights and benefits of Software Maintenance Services.

7. When software assets are eligible for transfer, and are fully covered under pre-paid Software Maintenance Services (SIN 54151), the new ordering activity shall not be required to pay maintenance for those license assets prior to the natural termination of the paid for maintenance period. The rights associated with paid for current Software Maintenance Services shall automatically transfer with the software licenses without fee. When the maintenance period expires, the new ordering activity or license grantee shall have the option to renew maintenance.

8. The administrative fee to support the transfer of licenses, exclusive of any new incremental licensing or maintenance costs shall be XX percentage (%) of the original license fee (TBD at order level). The fee shall be paid only at the time of
transfer. In applying the transfer fee, the Software Contractor shall provide transactional data that supports the original costs of the licenses.

3.10 Software Conversions

Full monetary credit will be allowed to the ordering activity when conversion from one version of the software to another is made as the result of a change in operating system, or from one computer system to another. Under a perpetual license, the purchase price of the new software shall be reduced by the amount that was paid to purchase the earlier version. Under a term license, if conversion credits had accrued while the earlier version was under a term license, those credits shall carry forward and remain available as conversion credits which may be applied towards the perpetual license price of the new version.

3.11 Descriptions and Equipment Compatibility

The Contractor shall include, in the schedule pricelist, a complete description of each software product including the operating systems on which the software can be used. Also included shall be a brief, introductory explanation of the modules and documentation which are offered.

3.12 Right-To-Copy Pricing

Right-to-copy pricing is not offered.
4.0 Terms and Conditions Applicable to Highly Adaptive Cybersecurity Services (HACS) (SIN 54151HACS)

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

Vendor suitability for offering services through the Highly Adaptive Cybersecurity Services (HACS) SIN must be in accordance with the following laws and standards when applicable to the specific task orders, including but not limited to:

- Federal Acquisition Regulation (FAR) Part 52.204-21
- OMB Memorandum M-17-12 - Preparing for and Responding to a Breach of Personally Identifiable Information (PII)
- OMB Memorandum M-19-03 - Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program
- 2017 Report to the President on Federal IT Modernization
- The Cybersecurity National Action Plan (CNAP)
- NIST SP 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems
- NIST SP 800-27A - Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
- NIST SP 800-30 - Guide for Conducting Risk Assessments
- NIST SP 800-35 - Guide to Information Technology Security Services
- NIST SP 800-44 - Guidelines on Securing Public Web Servers
- NIST SP 800-48 - Guide to Securing Legacy IEEE 802.11 Wireless Networks
- NIST SP 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-61 - Computer Security Incident Handling Guide
- NIST SP 800-64 - Security Considerations in the System Development Life Cycle
- NIST SP 800-82 - Guide to Industrial Control Systems (ICS) Security
- NIST SP 800-86 - Guide to Integrating Forensic Techniques into Incident Response
- NIST SP 800-115 - Technical Guide to Information Security Testing and Assessment
• NIST SP 800-128 - Guide for Security-Focused Configuration Management of Information Systems
• NIST SP 800-137 - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
• NIST SP 800-153 - Guidelines for Securing Wireless Local Area Networks (WLANs)
• NIST SP 800-160 - Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
• NIST SP 800-171 - Protecting Controlled Unclassified Information in non-federal Information Systems and Organizations

4.1 SCOPE

a. The labor categories, prices, terms and conditions stated under Special Item Number 54151HACS Highly Adaptive Cybersecurity Services (HACS) apply exclusively to Highly Adaptive Cybersecurity Services within the scope of this Multiple Award Schedule (MAS).

b. Services under this SIN are limited to Highly Adaptive Cybersecurity Services only. Software and hardware products are under different Special Item Numbers on Multiple Award Schedule (MAS) (e.g. 511210, 33411), and may be quoted along with services to provide a total solution.

c. This SIN provides ordering activities with access to Highly Adaptive Cybersecurity services only.

d. Highly Adaptive Cybersecurity Services provided under this SIN shall comply with all Cybersecurity certifications and industry standards as applicable pertaining to the type of services as specified by ordering agency.

e. SCOPE:

54151HACS Highly Adaptive Cybersecurity Services (HACS) - SUBJECT TO COOPERATIVE PURCHASING - includes proactive and reactive cybersecurity services that improve the customer’s enterprise-level security posture.

The scope of this category includes proactive and reactive cybersecurity services that improve customer enterprise-level security posture. Services to identify and protect a customer's information resources, detect and respond to cybersecurity events or incidents, and recover capabilities or services impaired by any incidents that emerge. It encompasses a wide range of fields that include, but are not limited to, Risk Management Framework (RMF) services, information assurance (IA), virus detection, network management, situational awareness and incident response, secure web hosting, and backup and security services.

The seven-step RMF includes preparation, information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. RMF activities may also include Information Security Continuous Monitoring Assessment (ISCMA) which evaluate organization-wide ISCM implementations, and also Federal Incident Response Evaluations (FIREs), which assess an organization’s incident management functions.
The scope of this category also includes Security Operations Center (SOC) services. The SOC scope includes services such as: 24x7x365 monitoring and analysis, traffic analysis, incident response and coordination, penetration testing, anti-virus management, intrusion detection and prevention, and information sharing.

HACS vendors are able to identify and protect a customer’s information resources, detect and respond to cybersecurity events or incidents, and recover capabilities or services impaired by any incidents that emerge. Offerors may request to be placed in the following subcategories.

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

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

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

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

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

f. 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.
4.2 Order

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

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

4.3 Performance of Services

a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity. All Contracts will be fully funded.

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

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

d. Any Contractor travel required in the performance of Highly Adaptive Cybersecurity 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 the GSA City Pair Program for travel in support of any contracts. All travel will be agreed upon with the client prior to the Contractor's travel.

4.4 Inspection of Services

Inspection of services is in accordance with 552.212-4 - CONTRACT TERMS AND CONDITIONS– COMMERCIAL ITEMS (Jan 2017) & (ALTERNATE I-Jan 2017) for Time-and-Materials and Labor-Hour orders placed under this contract.

4.5 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 (May 2014) Rights in Data – General, may apply.

The Contractor shall comply with contract clause (52.204-21) to the Federal Acquisition Regulation (FAR) for the basic safeguarding of contractor information systems that process, store, or transmit Federal data received by the contract in performance of the contract. This includes contract documents and all information generated in the performance of the contract.
4.6 Responsibilities of the Ordering Activity

Subject to the ordering activity security regulations, the ordering activity shall permit Contractor access to all facilities necessary to perform the requisite Highly Adaptive Cybersecurity Services.

4.7 Independent Contractor

All Highly Adaptive Cybersecurity 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.

4.8 Organizational Conflicts of Interest

a. Definitions.

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

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

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

b. To avoid an organizational or financial conflict of interest and to avoid prejudicing the best interests of the ordering activity, ordering activities may place restrictions on the Contractors, its affiliates, chief executives, directors, subsidiaries and subcontractors at any tier when placing orders against schedule contracts. Such restrictions shall be consistent with FAR 9.505 and shall be designed to avoid, neutralize, or mitigate organizational conflicts of interest that might otherwise exist in situations related to individual orders placed against the schedule contract. Examples of situations, which may require restrictions, are provided at FAR 9.508.

4.9 Invoices

The Contractor, upon completion of the work ordered, shall submit invoices for Highly Adaptive Cybersecurity 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.

4.10 Resumes

Resumes shall be provided to the GSA Contracting Officer or the user ordering activity upon request.
4.11 Approval of Subcontracts
The ordering activity may require that the Contractor receive, from the ordering activity Contracting Officer, written consent before placing any subcontract for furnishing any of the work called for in a task order.

4.12 Description of Highly Adaptive Cybersecurity Services and Pricing
Please refer to the labor category description and pricing incorporated into this pricelist.
5.0 Terms and Conditions Applicable To Information Technology Professional Services (SIN 54151S)

54151S - IT Professional Services and/or labor categories for database planning and design; systems analysis, integration, and design; programming, conversion and implementation support; network services, data/records management, and testing.

5.1 Scope

a. The prices, terms and conditions stated under Special Item Number 54151S Information Technology Professional Services apply exclusively to IT Professional Services within the scope of this Multiple Award Schedule (MAS).

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

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

5.2 Performance Incentives I-FSS-60 Performance Incentives (April 2000)

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

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

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

5.3 Order

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

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

5.4 Performance of Services

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

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

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

d. 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 the GSA City Pair Program for travel in support of any contracts.

5.5 Stop-Work Order (FAR 52.242-15) (Aug 1989)

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

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

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

1. 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
2. The Contractor asserts its right to the adjustment within 30 days after the end of the period of work stoppage; provided, that, if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon the claim submitted at any time before final payment under this contract.

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

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

5.6 Inspection of Services

In accordance with FAR 52.212-4 CONTRACT TERMS AND CONDITIONS--COMMERCIAL ITEMS (OCT 2018) (DEVIATION – FEB 2018) for Firm-Fixed Price orders and FAR 52.212-4
5.7 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.

5.8 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/IAM Professional Services.

5.9 Independent Contractor

All IT/IAM 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.

5.10 Organizational Conflicts of Interest

a. Definitions.

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

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

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

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

5.11 Invoices

The Contractor, upon completion of the work ordered, shall submit invoices for IT/IAM 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.
5.12 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 (OCT 2018) (ALTERNATE I – JAN 2017) 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 (OCT 2018) (ALTERNATE I – JAN 2017) applies to labor-hour orders placed under this contract. 52.216-31(Feb 2007) Time-and Materials/Labor-Hour Proposal Requirements—Commercial Item Acquisition. As prescribed in 16.601(e)(3), insert the following provision:

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

b. The offeror must specify fixed hourly rates in its offer that include wages, overhead, general and administrative expenses, and profit. The offeror must specify whether the fixed hourly rate for each labor category applies to labor performed by—
   1. The offeror;
   2. Subcontractors; and/or
   3. Divisions, subsidiaries, or affiliates of the offeror under a common control.

5.13 Resumes

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

5.14 Incidental Support Costs

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

5.15 Approval of Subcontracts

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

5.16 Description of IT Services and Pricing

Please refer to the labor category description and pricing incorporated into this pricelist.
6.0 Terms and Conditions Applicable To Identity, Credentialing and Access Management (ICAM) (SIN 541519ICAM)

541519ICAM - Managed service offerings for electronic credentials (assurance levels IAL, AAL, and FAL), identity and access management, authentication, and identity and access management professional services.

6.1 Scope

a. The prices, terms and conditions stated under Special Item Number 54151S Information Technology Professional Services apply exclusively to IT/IAM Professional Services within the scope of this Multiple Award Schedule (MAS).

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

6.2 Performance Incentives I-FSS-60 Performance Incentives (April 2000)

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

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

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

6.3 Order

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

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

6.4 Performance of Services

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

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

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

d. 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 the GSA City Pair Program for travel in support of any contracts.

6.5 Stop-Work Order (FAR 52.242-15) (Aug 1989)

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

1. Cancel the stop-work order; or

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

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

1. 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

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

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

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

6.6 Inspection of Services

6.7 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.

6.8 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/IAM Professional Services.

6.9 Independent Contractor

All IT/IAM 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.

6.10 Organizational Conflicts of Interest

a. Definitions.

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

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

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

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

6.11 Invoices

The Contractor, upon completion of the work ordered, shall submit invoices for IT/IAM 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.

6.12 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 (OCT 2018) (ALTERNATE I – JAN 2017) 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 (OCT 2018) (ALTERNATE I – JAN 2017) applies to labor-hour orders placed under this contract. 52.216-31(Feb 2007) Time-and Materials/Labor-Hour Proposal Requirements—Commercial Item Acquisition. As prescribed in 16.601(e)(3), insert the following provision:

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

b. The offeror must specify fixed hourly rates in its offer that include wages, overhead, general and administrative expenses, and profit. The offeror must specify whether the fixed hourly rate for each labor category applies to labor performed by—
   1. The offeror;
   2. Subcontractors; and/or
   3. Divisions, subsidiaries, or affiliates of the offeror under a common control.

6.13 Resumes

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

6.14 Incidental Support Costs

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

6.15 Approval of Subcontracts

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

6.16 Description of IT Services and Pricing

Please refer to the labor category description and pricing incorporated into this GSA pricelist.
7.0 Terms and Conditions Applicable To Health Information Technology Services
(SIN 54151HEAL)

54151HEAL Includes a wide range of Health IT services to include connected health, electronic health records, health information exchanges, health analytics, personal health information management, innovative Health IT solutions, health informatics, emerging Health IT research, and other Health IT services.

Vendor suitability for offering services through the new Health IT SIN must be in accordance with the following laws and standards when applicable to the specific task orders, including but not limited to:

- Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) and Special Publications
- Federal Information Security Management Act (FISMA) of 2002

7.1 SCOPE

a. The labor categories, prices, terms and conditions stated under Special Item Number 54151HEAL Health Information Technology Services apply exclusively to Health IT Services within the scope of this Multiple Award Schedule (MAS).

b. This SIN is limited to Health IT Services only. Software and hardware products are out of scope. Hardware and software can be acquired through different Special Item Numbers on.

c. This SIN provides ordering activities with access to Health IT services.

d. Health IT Services provided under this SIN shall comply with all Healthcare certifications and industry standards as applicable at the task order level.

e. 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.

7.2 Order

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

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

7.3 Performance of Services

a. The Contractor shall commence performance of services on the date agreed to by the
Contractor and the ordering activity. All Contracts will be fully funded.

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

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

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

7.4 Inspection of Services


7.5 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.

7.6 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/IAM Professional Services.

7.7 Independent Contractor

All IT/IAM 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.

7.8 Organizational Conflicts of Interest

e. 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.
f. 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.

7.9 Invoices

The Contractor, upon completion of the work ordered, shall submit invoices for IT/IAM 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.

7.10 Resumes

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

7.11 Incidental Support Costs

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

7.12 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.

7.13 Description of Health IT Services and Pricing

Please refer to the labor category description and pricing incorporated into this pricelist.
8.0 Labor Category Descriptions

8.1 SIN 54151HACS - Highly Adaptive Cyber Security Services (HACS)

8.1.1 Program Manager

Duties: Performs day-to-day management of delivery order projects for related technology projects that involve teams of data processing and other information systems management professionals who have previously been involved in analyzing, designing, integrating, testing, documenting, convening, extending, and implementing automated information and telecommunications systems. Demonstrates proven skills in those technical areas addressed by the delivery order to be managed. organizes, directs, and coordinates the planning and production of all activities associated with assigned deliverables. Establishes and alters, as necessary, corporate management structure to direct effective contract support activities. Demonstrates good written and oral communications.

Experience: Must have 10 years of IT experience, including at least 7 years of IT and/or telecommunications system management experience.

Education: Minimum bachelor’s Degree in Cybersecurity, Computer Science or related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor’s degree requirement.

8.1.2 Project Manager I

Duties: Provides overall direction to the formulation, development, implementation and delivery of a moderately complex project or one that is part of a larger program. Ensures that the project plan maintains tasks, schedules, estimates and status. Disseminates information to project members. Arranges for the assignment of responsibility to other supporting facilities, business areas, support functions and monitors their performance. May have supervisory responsibilities for hiring, terminating and reviewing project members. Should possess good communication skills.

Experience: At least 5 years of industry experience with at least two to three years as a project manager.

Education: Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.1.3 Project Manager II

Duties: Provides overall direction to the formulation, development, implementation and delivery of a complex project. Ensures that the project plan maintains tasks, schedules, estimates and status. Disseminates information to project members. Arranges for the assignment of responsibility to other supporting facilities, business areas, support functions and monitors their performance. Has supervisory responsibilities for hiring, terminating and reviewing project members. Should possess good communication skills.

Experience: At least 7 years of industry experience with at least three to five years as a project manager.

Education: Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.
8.1.4 Program & Policy Analyst 1

Duties: Proactively support and identify changes needed in programs and policy and to align and support strategic shifts in business strategy. Assist to ensure formal business policy issuances are complete, current, and operationally relevant. Provide input into the revision and/or development of programs and policies to comply with emerging national requirements.

Experience: At least 3 years relevant experience. Knowledge and understanding of public law, Executive Orders, Presidential Directives and Federal regulations governing programs and policies.

Education: Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.1.5 Program & Policy Analyst 2

Duties: Directly support and identify changes needed in programs and policy and to align and support strategic shifts in business strategy. Assist to ensure formal business policy issuances are complete, current, and operationally relevant. Provide input into the revision and/or development of programs and policies to comply with emerging national requirements.

Experience: Requires at least 5 years relevant experience. Knowledge and understanding of public law, Executive Orders, Presidential Directives and Federal regulations governing programs and policies.

Education: Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.1.6 Program & Policy Analyst 3

Duties: Provide leadership to proactively identify changes needed in programs and policy and to align and support strategic shifts in business strategy. Ensure formal business policy issuances are complete, current, and operationally relevant. Lead the revision and/or development of programs and policies to comply with emerging national requirements. Monitor on a continuing basis proposed and newly promulgated Federal legislation, Office of Management and Budget guidance, and other national level policy affecting programs and policies need to perform analysis and identify policy gaps. Identify program and policy changes necessary to improve acquisition and integrate these policies and procedures into the acquisition process.

Experience: Requires at least 8 years relevant experience. Knowledge and understanding of public law, Executive Orders, Presidential Directives and Federal regulations governing programs and policies.

Education: Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.1.7 Cyber Security Consultant

Duties: Performs tasks related to business analysis, architecture definition and review, database design assistance and review, assistance in data migration and integration definition, and application development.

Experience: Requires at least 7 years relevant experience for this job category.
Education: Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement. Masters and PhD recipients can count postgraduate education years towards overall experience.

8.1.8 Cyber Security Architect

Duties: Performs tasks related to business analysis, architecture definition and review, database design assistance and review, assistance in data migration and integration definition, and application development.

Experience: Requires at least 7 years relevant experience for this job category

Education: Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement. Masters and PhD recipients can count postgraduate education years towards overall experience.

8.1.9 Cyber Security Engineer 1

Duties: Under supervision provides support to cyber security operations, policy and threat mitigation. Perform duties utilizing cyber security tools, network topologies, intrusion detection, and secured networks. Support interpretation and implementation of cyber security regulations.

Experience: Requires at least 3 years relevant experience in a Cyber Security role.

Education: Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.1.10 Cyber Security Engineer 2

Duties: Provides support to cyber security operations, policy and threat mitigation. Perform duties utilizing cyber security tools, network topologies, intrusion detection, and secured networks. Integrates metrics into the security posture of the organization, identifies areas of weakness and vulnerability and recommends changes to meet security standards. Interpret, implements and monitors compliance to cyber security regulations.

Experience: Requires at least 5 years relevant experience in a Cyber Security role.

Education: Minimum Bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.1.11 Cyber Security Engineer 3

Duties: Provides leadership to cyber security operations, policy and threat mitigation. Oversees cyber security tools, network topologies, intrusion detection, and secured networks. Reviews applicability of metrics used for assessment of security posture of the organization, acts on areas of weakness and vulnerability and leads implementation of changes to meet security standards. Provide technical direction and guidance to other Cyber Security Engineers, Information Technology and the organization to align with regulatory and security requirements.

Experience: Requires at least 8 years relevant experience in a Cyber Security role.
Education: Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.1.12 Cyber Security Analyst 1
Duties: Under supervision provides day-to-day support to cyber security operations. Gathers data and perform technical and operational analysis of cyber security operations, reporting, and management. Supports presentations and facilitates discussion of security operations with senior management. Draft communications, reports, and analysis documentation.

Experience: Requires at least 3 years relevant experience in a Cyber Security role.

Education: Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.1.13 Cyber Security Analyst 2
Duties: Provides day-to-day support to cyber security operations. Gathers and interprets data and perform technical and operational analysis of cyber security operations, reporting, and management. Develops presentations and facilitates discussion of security operations with senior management. Draft communications, reports, and analysis documentation.

Experience: Requires at least 5 years relevant experience in a Cyber Security role.

Education: Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.1.14 Cyber Security Analyst 3
Duties: Provides leadership in the day-to-day support to cyber security operations. Reviews and interprets data and perform technical and operational analysis of cyber security operations, reporting, and management. Leads presentations and facilitates discussion of security operations with senior management.

Experience: Requires at least 8 years relevant experience in a Cyber Security role.

Education: Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.1.15 Cyber Security Specialist 1
Duties: Under general supervision, performs procedures necessary to ensure the safety of information systems assets and to protect systems from intentional or inadvertent access or destruction. Assists in performing multiple duties, such as installation, configuration, maintenance and administration of various information assurance systems, to include Firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), and Security Information and Event Management (SIEM) systems. Performing security analysis, problem reporting, tracking and documenting resolutions and performance issues.

Experience: Possesses at least 3 years of relevant hands-on experience and possesses a security clearance.
Education: Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor’s degree requirement. Certifications in one or more CISA, CEH, Security+, CCNA, MCP, TippingPoint training or similar technologies. Working towards CISSP certification

8.1.16 Cyber Security Specialist 2

Duties: Under general direction, performs all procedures necessary to ensure the safety of information systems assets and to protect systems from intentional or inadvertent access or destruction. Performing multiple engineering duties, such as installation, configuration, maintenance and administration of various information assurance systems, to include Firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), and Security Information and Event Management (SIEM) systems. Performing security analysis, problem reporting, tracking and documenting resolutions and performance issues. Monitoring, evaluating, and developing alternative utilization or configuration strategies and conducting, directing, and coordinating responses to cyber attacks, classified material incidents, virus infections and other information assurance and computer network defense activities. May require understanding of firewall theory and configuration.

Experience: Possesses at least 5 years of relevant hands-on experience and possesses a security clearance.

Education: Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor’s degree requirement. Certifications in one or more CISA, CEH, Security+, CCNA, MCP, TippingPoint training or similar technologies. Working towards CISSP certification.

8.1.17 Cyber Security Specialist 3

Duties: Leads all procedures necessary to ensure the safety of information systems assets and to protect systems from intentional or inadvertent access or destruction. Interfaces with user community to understand their security needs and implements procedures to accommodate them. Ensures that user community understands and adheres to necessary procedures to maintain security. Requires familiarity with domain structures, user authentication, and digital signatures. Conducts evaluation of the level of security required, and configuration.

Experience: Possesses at least 7 years of relevant hands-on experience and possesses a security clearance.

Education: Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor’s degree requirement. Certifications in one or more CISSP, CISA, CEH, Security+, CCNA, MCP, TippingPoint training or similar technologies.

8.1.18 Cyber Hunting and Threat Intelligence Manager/Lead

Duties: Lead the profiling of new and emerging threats to the IT landscape. Analyze and determine the scope of vulnerabilities in software, and determining how client will best defend themselves against these threats. Monitor third party security related websites, forums, and mailing lists for information regarding vulnerabilities and exploits. verify the vulnerabilities; correlate and collate the information; and develop, edit, and deliver security reports to enterprise-level customers. On occasion replicate reported vulnerabilities where appropriate to develop proof of concept and/or exploit tools against these vulnerabilities. Provide senior leadership to clients in the areas of Cyber Security Threats Prevention.
Experience: Possesses at least 9 years of commensurate experience and possesses a security clearance.

Education: Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor’s degree requirement. Certifications in one or more such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training and similar technologies.

8.1.19 Cyber Hunting and Threat Intelligence Analyst 1

Duties: Support the profiling of new and emerging threats to the IT landscape. Support the analysis of vulnerabilities in software, and determining how client will best defend themselves against these threats. Support monitoring of third party security related websites, forums, and mailing lists for information regarding vulnerabilities and exploits.

Experience: Possesses up to 3 years of commensurate experience and possesses a security clearance.

Education: Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor’s degree requirement. Certifications in one or more such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training.

8.1.20 Cyber Hunting and Threat Intelligence Analyst 2

Duties: Support the profiling of new and emerging threats to the IT landscape. Support the analysis of vulnerabilities in software, and determining how client will best defend themselves against these threats. Support monitoring of third party security related websites, forums, and mailing lists for information regarding vulnerabilities and exploits.

Experience: Possesses at least 3 years of commensurate experience and possesses a security clearance.

Education: Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor’s degree requirement. Certifications in one or more such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training.

8.1.21 Cyber Hunting and Threat Intelligence Analyst 3

Duties: Profile new and emerging threats to the IT landscape. Analyze and determine the scope of vulnerabilities in software, and determining how client will best defend themselves against these threats. Monitor third party security related websites, forums, and mailing lists for information regarding vulnerabilities and exploits. Verify the vulnerabilities; correlate and collate the information; and develop, edit, and deliver security reports to enterprise- level customers.

Experience: Possesses at least 5 years of commensurate experience and possesses a security clearance.

Education: Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor’s degree requirement. Certifications in one or more such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training.
8.1.22 Cyber Hunting and Threat Intelligence Analyst 4

Duties: Lead the profiling of new and emerging threats to the IT landscape. Analyze and determine the scope of vulnerabilities in software, and determining how client will best defend themselves against these threats. Monitor third party security related websites, forums, and mailing lists for information regarding vulnerabilities and exploits. verify the vulnerabilities; correlate and collate the information; and develop, edit, and deliver security reports to enterprise-level customers. On occasion replicate reported vulnerabilities where appropriate to develop proof of concept and/or exploit tools against these vulnerabilities.

Experience: Possesses at least 7 years of commensurate experience and possesses a security clearance.

Education: Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement. Certifications in one or more such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training and similar technologies.

8.1.23 Penetration Testing Manager / Lead

Duties: Leads management analysis processes, statistical methods, and advanced technical and analytical research techniques to develop security solutions and strategies based on client requirements with a law enforcement, professional security, or emergency preparedness services-based scope. Performing forensic analysis of digital information and other computer evidence. Providing specialized support by gathering, handling, examining, preparing, investigating, searching, retrieving, identifying and/or comparing digital and/or physical evidence. Understanding and using forensically sound procedures to determine results. Provides integral support in research and development, organizational and vulnerability assessments, intelligence and threat analysis, mission requirements determination, policy and procedures development, concept definition design, testing, integration verification and validation, documentation, implementation, and operations and maintenance. Works closely with stakeholders to determine requirements and ensure compliance with exceptions.

Experience: Possesses at least 9 years of commensurate experience and at least 2 years of hands-on experience as a senior level security operations analyst in a 24/7 Security Operations Center or a Computer Security Incident Response Team and possesses a security clearance.

Education: Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement. Certifications in one or more such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training and similar technologies.

8.1.24 Penetration Tester 1

Duties: Supports forensic analysis of digital information and other computer evidence by gathering, handling, examining, preparing, investigating, searching, retrieving, identifying and/or comparing digital and/or physical evidence. Supports research and development, organizational and vulnerability assessments, intelligence and threat analysis, mission requirements determination, policy and procedures development, concept definition design, testing, integration verification and validation, documentation, implementation, and operations and maintenance.

Experience: Possesses up to 3 years of commensurate experience and possesses a security clearance.
Education: Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement. Certifications in one or more such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training and similar technologies.

8.1.25 Penetration Tester 2

Duties: Supports forensic analysis of digital information and other computer evidence by gathering, handling, examining, preparing, investigating, searching, retrieving, identifying and/or comparing digital and/or physical evidence. Supports research and development, organizational and vulnerability assessments, intelligence and threat analysis, mission requirements determination, policy and procedures development, concept definition design, testing, integration verification and validation, documentation, implementation, and operations and maintenance.

Experience: Possesses at least 3 years of commensurate experience and possesses a security clearance.

Education: Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement. Certifications in one or more such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training and similar technologies.

8.1.26 Penetration Tester 3

Duties: Performs forensic analysis of digital information and other computer evidence. Providing specialized support by gathering, handling, examining, preparing, investigating, searching, retrieving, identifying and/or comparing digital and/or physical evidence. Understanding and using forensically sound procedures to determine results. Provides integral support in research and development, organizational and vulnerability assessments, intelligence and threat analysis, mission requirements determination, policy and procedures development, concept definition design, testing, integration verification and validation, documentation, implementation, and operations and maintenance. Works closely with stakeholders to determine requirements and ensure compliance with exceptions.

Experience: Possesses at least 5 years of commensurate experience and at least 2 years of hands-on experience as a security operations analyst in a 24/7 Security Operations Center or a Computer Security Incident Response Team and possesses a security clearance.

Education: Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement. Certifications in one or more such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training and similar technologies.

8.1.27 Penetration Tester 4

Duties: Leads management analysis processes, statistical methods, and advanced technical and analytical research techniques to develop security solutions and strategies based on client requirements with a law enforcement, professional security, or emergency preparedness services-based scope. Performing forensic analysis of digital information and other computer evidence. Providing specialized support by gathering, handling, examining, preparing, investigating, searching, retrieving, identifying and/or comparing digital and/or physical evidence. Understanding and using forensically sound procedures to determine results. Provides integral support in research and development, organizational and vulnerability
assessments, intelligence and threat analysis, mission requirements determination, policy and procedures development, concept definition design, testing, integration verification and validation, documentation, implementation, and operations and maintenance. Works closely with stakeholders to determine requirements and ensure compliance with exceptions.

Experience: Possesses at least 7 years of commensurate experience and at least 2 years of hands-on experience as a senior level security operations analyst in a 24/7 Security Operations Center or a Computer Security Incident Response Team and possesses a security clearance.

Education: Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement. Certifications in one or more such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training and similar technologies.

8.1.28 Incident Detection/Response Analyst 1

Duties: Supports activities to search network for indicators of compromise. Supports and provides immediate onsite services to the customer in the event of the identification of a compromise or a credible alert from an intrusion detection system. Supports live response data collection and analysis on hosts of interest in an investigation. Correlates and analyze relevant events from host and network device log files.

Experience: Possesses up to 3 years of commensurate experience and possesses a security clearance.

Education: Minimum bachelor’s degree in Computer Science, Engineering, Business or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement. Certifications in one or more such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training and similar technologies.

8.1.29 Incident Detection/Response Analyst 2

Duties: Performs activities to search network for indicators of compromise. Provides immediate onsite services to the customer in the event of the identification of a compromise or a credible alert from an intrusion detection system. Performs live response data collection and analysis on hosts of interest in an investigation. Correlates and analyze relevant events from host and network device log files. Performs incident response and malware analysis to investigate incidents and potential indicators of compromise. Helps determine the extent of the compromise, attributes of any malware and possible data exfiltrated. Researches and incorporates relevant threat intelligence during the investigation and in written and verbal reports.

Experience: Possesses at least 3 years of commensurate experience and possesses a security clearance.

Education: Minimum bachelor’s degree in Computer Science, Engineering, Business or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement. Certifications in one or more such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training and similar technologies.

8.1.30 Incident Detection/Response Analyst 3

Duties: Performs and supervises activities to search network for indicators of compromise. Provides immediate onsite services to the customer in the event of the identification of a compromise or a credible alert from an intrusion detection system. Performs live response data
collection and analysis on hosts of interest in an investigation. Correlates and analyze relevant events from host and network device log files. Performs incident response and malware analysis to investigate incidents and potential indicators of compromise. Determines the extent of the compromise, attributes of any malware and possible data exfiltrated. Researches and incorporates relevant threat intelligence during the investigation and in written and verbal reports. Develops, documents and manages containment strategy. Maintains current knowledge of tools and best-practices in advanced persistent threats; tools, techniques, and procedures of attackers; and forensics and incident response.

Experience: Possesses at least 7 years of commensurate experience and possesses a security clearance.

Education: Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement. Certifications in one or more such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training and similar technologies.

8.1.31 Risk and Vulnerability Assessment Analyst 1

Duties: Under general supervision, supports Risk and Vulnerability Assessment (RVA) services. Provide general support to network mapping, vulnerability scanning, phishing, wireless, web application, social engineering, operating system, domain security and other associated assessments.

Experience: Possesses up to 3 years of relevant hands-on experience and possesses a security clearance.

Education: Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement. Certifications in one or more such as CISA, CEH, Security+ or training on similar technologies. Working towards CISSP certification

8.1.32 Risk and Vulnerability Assessment Analyst 2

Duties: Provides support to perimeter, network, database, data security, network mapping, vulnerability scanning, phishing, wireless, web application, social engineering, operating system, domain security and other associated assessments.

Experience: Possesses at least 3 years of relevant hands-on experience and possesses a security clearance.

Education Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement. Certifications in one or more such as CISSP, CEH, CISA, GCFA, Security+ or similar technologies.

8.1.33 Risk and Vulnerability Assessment Analyst 3

Duties: Responsible for providing oversight and supervisory support to Risk and Vulnerability Assessment (RVA) services. Full range of duties include perimeter, network, database, data security, network mapping, vulnerability scanning, phishing, wireless, web application, social engineering, operating system, domain security and other associated assessments.

Experience: Possesses at least 7 years of relevant hands-on experience and possesses a security clearance.
Education: Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor’s degree requirement. Certifications in one or more such as CISSP, CEH, CISA, GCFA, Security+ or similar technologies.

8.1.34 Documentation Specialist 1


Experience: At least 2 years of experience formatting, writing, editing, and proofreading technical data in support of IT implementation projects and tasks.

Education: Minimum bachelor’s degree or 3 years additional related experience may be substituted for a Bachelor's degree requirement.

8.1.35 Documentation Specialist 2

Duties: Formats, writes, edits, proofreads technical data for use in documents. Ensures document meets specifications and complies with quality, format and style standards. Creates new documentation from related documentation, examination of subject system or procedure, and/or interviews.

Experience: At least 4 years of relevant experience.

Education: Minimum bachelor’s degree in English or a technical field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.1.36 Cyber Security Subject Matter Expert

Duties: Develops requirements from a project's inception to its conclusion in the subject matter area for moderately complex systems. Assists other senior consultants with analysis and evaluation and with the preparation of recommendations for system improvements, optimization, development, and/or maintenance efforts in the following specialties: information systems architecture; networking; telecommunications; automation; risk management; software; life-cycle management; software development methodologies; modeling and simulation.

Experience: At least 8 years of IT experience and at least 5 years directly related to the required area of expertise.

Education: Minimum bachelor’s degree in Cybersecurity, Computer Science, or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.2 SIN 54151S - Information Technology Professional Services

8.2.1 Program Administration Specialist I

Duties: The Program Administration Specialist I directly supports Project Manager by maintaining personnel and other files; prepares correspondence, schedules and coordinates travel. Assists in the preparation of documents and supports the development of contract deliverables and reports. Responsible for integrating the graphics generated with automated tools and the deliverable documents. Assists in preparation of management plans and reports. Performs analysis, development, and review program administrative operating procedures.
Experience: Requires at least 1-2 years relevant experience.

Education: B.S. or B.A. degree in or related fields (or equivalent experience).

**8.2.2 Project Controls II**

Duties: The Project Controls II will calculate network schedules and make use of project scheduling software. They should understand alternate scheduling techniques such as linear scheduling, problems with resource constraints and apply basic techniques of resource leveling to scheduling. They should possess the ability to apply work breakdown structures and cost load a schedule as well as perform earned value calculations. They should have experience with the basics of conceptual and detailed (quantity) estimating and understand broad concepts of cost and time control as related to phases of the project and project organization. Finally, they will understand and apply basic visualization of project controls, including visualizations of quantitative controls data.

Experience: Requires at least 4 years relevant experience.

Education: B.S. or B.A. degree in Computer Science, Engineering or related fields (or equivalent experience).

**8.2.3 Project Manager I**

Duties: Provides overall direction to the formulation, development, implementation and delivery of a moderately Complex project or one that is part of a larger program. Ensures that the project plan maintains tasks, schedules, estimates and status. Disseminates information to project members. Arranges for the assignment of responsibility to other supporting facilities, business areas, support functions and monitors their performance. May have supervisory responsibilities for hiring, terminating and reviewing project members. Should possess good communication skills.

Experience: At least five years of industry experience with at least two to three years as a project manager.

Education: B.A. or B.S. degree in Computer Science, Engineering, Business or a related field.

* Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

**8.2.4 Project Manager II**

Duties: Provides overall direction to the formulation, development, implementation and delivery of a complex project. Ensures that the project plan maintains tasks, schedules, estimates and status. Disseminates information to project members. Arranges for the assignment of responsibility to other supporting facilities, business areas, support functions and monitors their performance. Has supervisory responsibilities for hiring, terminating and reviewing project members. Should possess good communication skills.

Experience: At least 7 years of industry experience with at least three to five years as a project manager.

Education: B.A. or B.S. degree in Computer Science, Engineering, Business or a related field.

* Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.
8.2.5 **Quality Assurance Manager**

Duties: Plans, directs and coordinates quality control-related activities. Responsible for ensuring that all hardware products and business processes represent the maximum quality and reliability attainable. Approves all quality control procedures, technical specifications and procurement of quality-related test equipment. Responsible for overall program design.

Experience: Requires at least 5- years relevant experience for this job category.

Education: B.S. or B.A. degree in related field.

8.2.6 **Systems Architect**

Duties: Prepares and plans the overall software development environment. Responsible for providing overall systems design. Performs development tools selections. Performs benchmarking for optimizing the systems platforms. Develops prototypes and acts as the primary lead technical consultant in a software development environment.

Experience: At least 5 years of relevant experience.

Education: B.A. or BS, degree in Computer Science, Engineering or a related field or equivalent experience.

*Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.2.7 **Systems Programmer II**

Duties: Installs, debugs and tunes internal operating system software. May perform systems maintenance and upgrades. Monitors and times system hardware and software.

Experience: At least 3-4 years of relevant experience.

Education: B.A. or B.S. degree in Computer Science, Engineering, or a related field.

*Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.2.8 **Test Engineer I**

Duties: Design review, test plan creation, test case implementation, defect report creation and tracking, and documentation review. Work with other testing team members to accomplish specific product testing tasks Review product requirements. Develop, maintain, and execute test cases. Create and maintain datasets. Create and execute automation scripts. Isolate defects and enter software defect reports. Continual review and improvement of testing process and implementation. Analyze and report progress to Test Manager

Experience: Requires at least 1-3 years relevant experience for this job category

Education: B.S. or B.A. degree in related field (or equivalent experience).

8.2.9 **Business System Analyst**

General Experience: Business System Analyst possesses at least 6 years of experience in information systems design and implementation, change management efforts or business process redesign and may possess a security clearance. Functional Responsibility: Supports determination of operational objectives by studying business functions; gathering information; evaluating output requirements and formats. Supports solving organizational information problems and requirements by analyzing requirements; designing computer programs;
recommending system controls and protocols. Defines project requirements by identifying project milestones, phases, and elements; leads project team; establishing project budget.

Minimum Education: Bachelor’s Degree or 5 years additional related experience.

**8.2.10 Database Specialist (Senior)**

General Experience: Database Specialist (Senior) possesses 2 to 6 years of experience in information systems networks, operations, engineering and design and may possess a security clearance.

Functional Responsibility: Apply their strong analytical and technical skills to assist in implementing IT business solutions. An IT Administrator 2 may apply their core skills and/or specific IT skills on projects. They may direct small teams and interact with the clients at the supervisory level.

Minimum Education: Bachelor’s Degree or 3 years additional related experience.

**8.2.11 Systems Engineer**

General Experience: Systems Engineer possesses at least 6 years of experience in information systems networks, operations, engineering and design and may possess a security clearance.

Functional Responsibility: Apply their strong analytical and technical skills to assist in implementing IT business solutions. An IT Administrator 3 may apply their core skills and/or specific IT skills on projects. They direct teams and interact with the clients at the supervisory or program level.

Minimum Education: Bachelor’s Degree or 4 years additional related experience.

**8.2.12 Applications Developer (Journeyman)**

General Experience: Applications Developer (Journeyman) possesses 2 to 6 years of experience in information systems implementations, change management efforts or business process redesign and may possess a security clearance.

Functional Responsibility: Apply their strong analytical and technical skills to assist in implementing IT business solutions. An IT Consultant 2 may apply their core skills and/or specific IT skills on projects. They may direct small teams and interact with the clients at the supervisory level.

Minimum Education: Bachelor’s Degree or 3 years additional related experience.

**8.2.13 Applications Developer (Senior)**

General Experience: Applications Developer (Senior) possesses at least 6 years of experience in information systems implementations, change management efforts or business process redesign and may possess a security clearance. Functional Responsibility: Apply their strong analytical and technical skills to assist in implementing IT business solutions. An IT Consultant 3 may apply their core skills and/or specific IT skills on projects. They direct teams and interact with the clients at the supervisory or program level.

Minimum Education: Bachelor’s Degree or 4 years additional related experience.
8.2.14 Quality Assurance Specialist (Journeyman)

General Experience: Quality Assurance Specialist (Journeyman) possesses at least 4 years of experience in leading information systems implementations, change management efforts or business process redesign and may possess a security clearance.

Functional Responsibility: Apply their broad management skills and functional and technical expertise to guide project teams in delivering IT solutions to the client. Ensures that the project plan maintains tasks, schedules, estimates and status. Disseminates information to project members. Arranges for the assignment of responsibility to other supporting facilities, business areas, support functions and monitors their performance. Has supervisory responsibilities for hiring, terminating and reviewing project members. Should possess good communication skills.

Minimum Education: Bachelor’s Degree or 4 years additional related experience.

8.2.15 Technical Writer 2

General Experience: Technical Writer 2 possesses between 2-5 years’ experience formatting, writing, editing, and proofreading technical data in support of IT implementation projects and tasks.


Minimum Education: Bachelor’s Degree or 3 years additional related experience.

8.2.16 Data Security Analyst 1

General Experience: Data Security Analyst 1 possesses up to 3 years of commensurate experience and possesses a security clearance.

Functional Responsibility: Under close supervision, performs procedures necessary to ensure the safety of information, systems assets and to protect systems from intentional or inadvertent access or destruction. Interfaces with user community to understand their security needs and implements procedures to accommodate them. Ensures that user community understands and adheres to necessary procedures to maintain security. Conducts accurate evaluation of the level of security required. Provides management with status reports.

Minimum Education: B.A. or B.S. degree in Computer Science, Engineering or a related field or equivalent experience., IAT or IAM Level I Security+, Security Tools Training, MCP.

8.2.17 Data Security Analyst 2

General Experience: Data Security Analyst 2 possesses at least 3 years of commensurate experience and possesses a security clearance.

Functional Responsibility: Under close supervision, performs procedures necessary to ensure the safety of information, systems assets and to protect systems from intentional or inadvertent access or destruction. Interfaces with user community to understand their security needs and implements procedures to accommodate them. Ensures that user community understands and adheres to necessary procedures to maintain security. Conducts accurate evaluation of the level of security required. Provides management with status reports.

Minimum Education: B.A. or B.S. degree in Computer Science, Engineering or a related field or equivalent experience., IAT or IAM Level I Security+, Security Tools Training, MCP.
8.2.18 Data Security Analyst 3
General Experience: Data Security Analyst 3 possesses at least 5 years of commensurate experience and possesses a security clearance.

Functional Responsibility: Under direct supervision, performs procedures necessary to ensure the safety of information, systems assets and to protect systems from intentional or inadvertent access or destruction. Interfaces with user community to understand their security needs and implements procedures to accommodate them. Ensures that user community understands and adheres to necessary procedures to maintain security. Conducts accurate evaluation of the level of security required. Provides management with status reports.

Minimum Education: B.A. or B.S. degree in Computer Science, Engineering or a related field or equivalent experience. IAT or IAM Level I Security+, Security Tools Training, MCP.

8.2.19 Data Security Analyst 4
General Experience: Data Security Analyst 4 possesses at least 7 years of commensurate experience and possesses a security clearance.

Functional Responsibility: Performs procedures necessary to ensure the safety of information, systems assets and to protect systems from intentional or inadvertent access or destruction. Interfaces with user community to understand their security needs and implements procedures to accommodate them. Ensures that user community understands and adheres to necessary procedures to maintain security. Conducts accurate evaluation of the level of security required. Provides management with status reports.

Minimum Education: B.A. or B.S. degree in Computer Science, Engineering or a related field or equivalent experience. IAT or IAM Level I Security+, Security Tools Training, MCP.

8.2.20 Data Security Analyst 5
General Experience: Data Security Analyst 5 possesses at least 9 years of commensurate experience and possesses a security clearance.

Functional Responsibility: Performs procedures necessary to ensure the safety of information, systems assets and to protect systems from intentional or inadvertent access or destruction. Interfaces with user community to understand their security needs and implements procedures to accommodate them. Ensures that user community understands and adheres to necessary procedures to maintain security. Conducts accurate evaluation of the level of security required. Provides management with status reports.

Minimum Education: B.A. or B.S. degree in Computer Science, Engineering or a related field or equivalent experience. IAT or IAM Level I Security+, Security Tools Training, MCP.

8.2.21 Threat Analyst 1
General Experience: Threat Analyst 1 possesses up to 3 years of commensurate experience and possesses a security clearance.

Functional Responsibility: Support the profiling of new and emerging threats to the IT landscape. Support the analysis of vulnerabilities in software, and determining how client will best defend themselves against these threats. Support monitoring of third party security related websites, forums, and mailing lists for information regarding vulnerabilities and exploits.
Minimum Education: B.A. or B.S. Degree in Computer Science, Engineering, Business or a related field, some certifications such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training.

8.2.22 Threat Analyst 2

General Experience: Threat Analyst 2 possesses at least 3 years of commensurate experience and possesses a security clearance.

Functional Responsibility: Support the profiling of new and emerging threats to the IT landscape. Support the analysis of vulnerabilities in software, and determining how client will best defend themselves against these threats. Support monitoring of third party security related websites, forums, and mailing lists for information regarding vulnerabilities and exploits.

Minimum Education: B.A. or B.S. Degree in Computer Science, Engineering, Business or a related field, some certifications such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training.

8.2.23 Threat Analyst 3

General Experience: Threat Analyst 3 possesses at least 5 years of commensurate experience and possesses a security clearance.

Functional Responsibility: Profile new and emerging threats to the IT landscape. Analyze and determine the scope of vulnerabilities in software, and determining how client will best defend themselves against these threats. Monitor third party security related websites, forums, and mailing lists for information regarding vulnerabilities and exploits. Verify the vulnerabilities; correlate and collate the information; and develop, edit, and deliver security reports to enterprise-level customers.

Minimum Education: B.A. or B.S. Degree in Computer Science, Engineering, Business or a related field, certifications such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training and similar technologies.

8.2.24 Threat Analyst 4

General Experience: Threat Analyst 4 possesses at least 7 years of commensurate experience and possesses a security clearance.

Functional Responsibility: Lead the profiling of new and emerging threats to the IT landscape. Analyze and determine the scope of vulnerabilities in software, and determining how client will best defend themselves against these threats. Monitor third party security related websites, forums, and mailing lists for information regarding vulnerabilities and exploits. Verify the vulnerabilities; correlate and collate the information; and develop, edit, and deliver security reports to enterprise-level customers. On occasion replicate reported vulnerabilities where appropriate to develop proof of concept and/or exploit tools against these vulnerabilities.

Minimum Education: B.A. or B.S. Degree in Computer Science, Engineering, Business or a related field, certifications such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training and similar technologies.

8.2.25 Threat Analyst 5

General Experience: Threat Analyst 5 possesses at least 9 years of commensurate experience and possesses a security clearance.
Functional Responsibility: Lead the profiling of new and emerging threats to the IT landscape. Analyze and determine the scope of vulnerabilities in software, and determining how client will best defend themselves against these threats. Monitor third party security related websites, forums, and mailing lists for information regarding vulnerabilities and exploits. Verify the vulnerabilities; correlate and collate the information; and develop, edit, and deliver security reports to enterprise-level customers. On occasion replicate reported vulnerabilities where appropriate to develop proof of concept and/or exploit tools against these vulnerabilities. Provide senior leadership to clients in the areas of Cyber Security Threats Prevention.

Minimum Education: B.A. or B.S. Degree in Computer Science, Engineering, Business or a related field, certifications such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training and similar technologies.

8.2.26 Forensics Analyst 1

General Experience: Forensics Analyst 1 possesses up to 3 years of commensurate experience and possesses a security clearance.

Functional Responsibility: Supports forensic analysis of digital information and other computer evidence by gathering, handling, examining, preparing, investigating, searching, retrieving, identifying and/or comparing digital and/or physical evidence. Supports research and development, organizational and vulnerability assessments, intelligence and threat analysis, mission requirements determination, policy and procedures development, concept definition design, testing, integration verification and validation, documentation, implementation, and operations and maintenance.

Minimum Education: B.A. or B.S. Degree in Computer Science, Engineering, Business or a related field, some certifications such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training and similar technologies.

8.2.27 Forensics Analyst 2

General Experience: Forensics Analyst 2 possesses at least 3 years of commensurate experience and possesses a security clearance.

Functional Responsibility: Supports forensic analysis of digital information and other computer evidence by gathering, handling, examining, preparing, investigating, searching, retrieving, identifying and/or comparing digital and/or physical evidence. Supports research and development, organizational and vulnerability assessments, intelligence and threat analysis, mission requirements determination, policy and procedures development, concept definition design, testing, integration verification and validation, documentation, implementation, and operations and maintenance.

Minimum Education: B.A. or B.S. Degree in Computer Science, Engineering, Business or a related field, some certifications such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training and similar technologies.

8.2.28 Forensics Analyst 3

General Experience: Forensics Analyst 3 possesses at least 5 years of commensurate experience and at least 2 years of hands-on experience as a security operations analyst in a 24/7 Security Operations Center or a Computer Security Incident Response Team and possesses a security clearance.
Functional Responsibility: Performs forensic analysis of digital information and other computer evidence. Providing specialized support by gathering, handling, examining, preparing, investigating, searching, retrieving, identifying and/or comparing digital and/or physical evidence. Understanding and using forensically sound procedures to determine results. Provides integral support in research and development, organizational and vulnerability assessments, intelligence and threat analysis, mission requirements determination, policy and procedures development, concept definition design, testing, integration verification and validation, documentation, implementation, and operations and maintenance. Works closely with stakeholders to determine requirements and ensure compliance with exceptions.

Minimum Education: B.A. or B.S. Degree in Computer Science, Engineering, Business or a related field, certifications such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training and similar technologies.

8.2.29 Forensics Analyst 4

General Experience: Forensics Analyst 4 possesses at least 7 years of commensurate experience and at least 2 years of hands-on experience as a senior level security operations analyst in a 24/7 Security Operations Center or a Computer Security Incident Response Team and possesses a security clearance.

Functional Responsibility: Leads management analysis processes, statistical methods, and advanced technical and analytical research techniques to develop security solutions and strategies based on client requirements with a law enforcement, professional security, or emergency preparedness services-based scope. Performing forensic analysis of digital information and other computer evidence. Providing specialized support by gathering, handling, examining, preparing, investigating, searching, retrieving, identifying and/or comparing digital and/or physical evidence. Understanding and using forensically sound procedures to determine results. Provides integral support in research and development, organizational and vulnerability assessments, intelligence and threat analysis, mission requirements determination, policy and procedures development, concept definition design, testing, integration verification and validation, documentation, implementation, and operations and maintenance. Works closely with stakeholders to determine requirements and ensure compliance with exceptions.

Minimum Education: B.A. or B.S. Degree in Computer Science, Engineering, Business or a related field, certifications such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training and similar technologies.

8.2.30 Forensics Analyst 5

General Experience: Forensics Analyst 5 possesses at least 9 years of commensurate experience and at least 2 years of hands-on experience as a senior level security operations analyst in a 24/7 Security Operations Center or a Computer Security Incident Response Team and possesses a security clearance.

Functional Responsibility: Leads management analysis processes, statistical methods, and advanced technical and analytical research techniques to develop security solutions and strategies based on client requirements with a law enforcement, professional security, or emergency preparedness services-based scope. Performing forensic analysis of digital information and other computer evidence. Providing specialized support by gathering, handling, examining, preparing, investigating, searching, retrieving, identifying and/or comparing digital and/or physical evidence. Understanding and using forensically sound procedures to determine results. Provides integral support in research and development, organizational and vulnerability assessments, intelligence and threat analysis, mission requirements determination, policy and procedures development, concept definition design, testing, integration verification and validation, documentation, implementation, and operations and maintenance. Works closely with stakeholders to determine requirements and ensure compliance with exceptions.
assessments, intelligence and threat analysis, mission requirements determination, policy and procedures development, concept definition design, testing, integration verification and validation, documentation, implementation, and operations and maintenance. Works closely with stakeholders to determine requirements and ensure compliance with exceptions.

Minimum Education: B.A. or B.S. Degree in Computer Science, Engineering, Business or a related field, certifications such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training and similar technologies.

8.2.31 Security Assurance Analyst 1

General Experience: Security Assurance Analyst 1 possesses up to 3 years of relevant hands-on experience and possesses a security clearance.

Functional Responsibility: Under general supervision, performs procedures necessary to ensure the safety of information systems assets and to protect systems from intentional or inadvertent access or destruction. Assists in performing multiple duties, such as installation, configuration, maintenance and administration of various information assurance systems, to include Firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), and Security Event and Information Management (SEIM) systems. Performing security analysis, problem reporting, tracking and documenting resolutions and performance issues.

Minimum Education: CISA, CEH, Security+, CCNA, MCP, TippingPoint training and similar technologies. Working towards CISSP certification

8.2.32 Security Assurance Analyst 2

General Experience: Security Assurance Analyst 2 possesses at least 3 years of relevant hands-on experience and possesses a security clearance.

Functional Responsibility: Under general supervision, performs procedures necessary to ensure the safety of information systems assets and to protect systems from intentional or inadvertent access or destruction. Assists in performing multiple duties, such as installation, configuration, maintenance and administration of various information assurance systems, to include Firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), and Security Event and Information Management (SEIM) systems. Performing security analysis, problem reporting, tracking and documenting resolutions and performance issues.

Minimum Education: CISA, CEH, Security+, CCNA, MCP, TippingPoint training and similar technologies. Working towards CISSP certification

8.2.33 Security Assurance Analyst 3

General Experience: Security Assurance Analyst 3 possesses at least 5 years of relevant hands-on experience and possesses a security clearance.

Functional Responsibility: Under general direction, performs all procedures necessary to ensure the safety of information systems assets and to protect systems from intentional or inadvertent access or destruction. Performing multiple engineering duties, such as installation, configuration, maintenance and administration of various information assurance systems, to include Firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), and Security Event and Information Management (SEIM) systems. Performing security analysis, problem reporting, tracking and documenting resolutions and performance issues. Monitoring, evaluating, and developing alternative utilization or configuration strategies and conducting, directing, and coordinating responses to cyber attacks, classified material incidents, virus infections and other information
assurance and computer network defense activities. May require understanding of firewall theory
and configuration.

Minimum Education: B.A. or B.S. Degree in Computer Science, Engineering, Business or a
related field. CISA, CEH, Security+, CCNA, MCP, TippingPoint training and similar technologies.
Working towards CISSP certification

8.2.34 Security Assurance Analyst 4

General Experience: Security Assurance Analyst 4 possesses at least 7 years of relevant
hands-on experience and possesses a security clearance.

Functional Responsibility: Leads all procedures necessary to ensure the safety of information
systems assets and to protect systems from intentional or inadvertent access or destruction.
Interfaces with user community to understand their security needs and implements procedures to
accommodate them. Ensures that user community understands and adheres to necessary
procedures to maintain security. Requires familiarity with domain structures, user authentication,
and digital signatures. Conducts evaluation of the level of security required. and configuration.

Minimum Education: B.A. or B.S. Degree in Computer Science, Engineering, Business or a
related field. Certifications in one or more CISSP, CISA, CEH, Security+, CCNA, MCP,
TippingPoint training and similar technologies.

8.2.35 Security Assurance Analyst 5

General Experience: Security Assurance Analyst 5 possesses at least 9 years of relevant
hands-on experience and possesses a security clearance.

Functional Responsibility: Leads all procedures necessary to ensure the safety of information
systems assets and to protect systems from intentional or inadvertent access or destruction.
Interfaces with user community to understand their security needs and implements procedures to
accommodate them. Ensures that user community understands and adheres to necessary
procedures to maintain security. Requires familiarity with domain structures, user authentication,
and digital signatures. Conducts evaluation of the level of security required. and configuration.

Minimum Education: B.A. or B.S. Degree in Computer Science, Engineering, Business or a
related field. Certifications in one or more CISSP, CISA, CEH, Security+, CCNA, MCP,
TippingPoint training and similar technologies.

8.2.36 Business Analyst 1

Duties: Supports determination of operational objectives by studying business functions;
gathering information; evaluating output requirements and formats. Supports solving
organizational information problems and requirements by analyzing requirements; designing
computer programs; recommending system controls and protocols. Defines project
requirements by identifying project milestones, phases, and elements; forming project team;
establishing project budget.

Experience: At least 3 years of relevant experience.

Education: B.A. or B.S. degree in Computer Science, Engineering, Business or a related field.
Five (5) years of direct related experience in a related field may be substituted for a Bachelor's
degree requirement
8.2.37 Business Analyst 2

Duties: Determines operational objectives by studying business functions; gathering information; evaluating output requirements and formats. Solves organizational information problems and requirements by analyzing requirements; designing computer programs; recommending system controls and protocols. Defines project requirements by identifying project milestones, phases, and elements; forming project team; establishing project budget.

Experience: At least 5 years of relevant experience.

Education: B.A. or B.S. degree in Computer Science, Engineering, Business or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement

8.2.38 Consultant 1

Duties: Performs tasks related to business analysis, architecture definition and review, database design assistance and review, assistance in data migration and integration definition, and application development.

Experience: Requires at least 7 years relevant experience for this job category

Education: Minimum B.S. or B.A. degree in related field. Masters and PhD recipients can count post-graduate education years towards overall experience.

8.2.39 Database Administrator 1

Duties: Performs activities related to database design, implementation and maintenance. Maintains data dictionaries and central data repository. Supports application system development life cycle. May develop policies and procedures relating to database management, security, maintenance and utilization. May be responsible for database backup and recovery procedures, access security and database integrity, physical data storage design and data storage management.

Experience: At least 3 years of relevant experience.

Education: B.A. or B.S. Degree at Computer Science, Engineering, Business or a related field.

• Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.2.40 Database Administrator 2

Duties: Performs activities related to database design, implementation and maintenance. Performs logical and physical design of databases. Maintains data dictionaries and central data repository. Supports application system development life cycle. May develop policies and procedures relating to database management, security, maintenance and utilization. May be responsible for database backup and recovery procedures, access security and database integrity, physical data storage design and data storage management.

Experience: At least 7 years of relevant experience.

Education: B.A. or B.S. Degree in Computer Science, Engineering, Business or a related field.

*Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.
8.2.41 Information Assurance 1

Duties: Performs security and vulnerability testing, analysis, and reporting using various security tools. Reviews and analyzes assessments and vulnerability matrices and provides recommendations for risk mitigation. Develops and maintains security policies and procedures, including system security plans, continuity of operations plans, rules of behavior, and various other security related documentation in accordance with federal regulations and policies. Develops certification and accreditation packages. May require certification in at least one of the following:

- NSA IAM - National Security Agency's INFOSEC Assessment Methodology
- CCISP - Certified Critical Infrastructure Security Professional
- CISM - Certified Information Security Manager
- CISSP - Certified Information Systems Security Professional
- SSCP - Systems Security Certified Practitioner
- GIAC - Global Information Assurance Certification
- CSP - RSA Certified Security Professional
- CPP Certified Protection Professional

Experience: Requires at least 3 years relevant experience for this job category

Education: Minimum B.S. or B.A. degree in related field.

8.2.42 Information Assurance 3

Duties: Performs security and vulnerability testing, analysis, and reporting using various security tools. Reviews and analyzes assessments and vulnerability matrices and provides recommendations for risk mitigation. Develops and maintains security policies and procedures, including system security plans, continuity of operations plans, rules of behavior, and various other security related documentation in accordance with federal regulations and policies. Develops certification and accreditation packages. May require certification in one or more of the following:

- NSA IAM - National Security Agency's INFOSEC Assessment Methodology
- CCISP - Certified Critical Infrastructure Security Professional
- CISMI - Certified Information Security Manager
- CISSP - Certified Information Systems Security Professional
- SSCP - Systems Security Certified Practitioner
- GIAC - Global Information Assurance Certification
- CSP - RSA Certified Security Professional
- CPP - Certified Protection Professional

Experience: Requires at least 8 years relevant experience for this job category

Education: Minimum B.S. or B.A. degree in related field. Masters and PhD recipients can count past-graduate education years towards overall experience.
8.2.43 **Network Administrator 1**

Duties: Assists in performing network administration functions for single location Local Area Network. May manage access, passwords, software, addresses, data, records and other network functions.

Experience: This is the entry level position for this job category.

Education: Associate's Degree in Computer Science, Engineering or a related field, equivalent technical school or equivalent experience.

8.2.44 **Network Administrator 2**

Duties: Performing network administration functions for single location Local Area Network. May manage access, passwords, software, addresses, data, records and other network functions.

Experience: At least 2 years of relevant experience.

Education: Associate's Degree in Computer Science, Engineering or a related field, equivalent technical school or equivalent experience.

8.2.45 **Network Administrator 3**

Duties: Performing network administration functions for multiple location Local Area Networks or Wide Area Networks. Manages access, passwords, software, addresses, data, records and other network functions.

Experience: At least 4 years of relevant experience.

Education: Associate's Degree in Computer Science, Engineering or a related field, equivalent technical school or equivalent experience.

8.2.46 **Network Architect**

Duties: Must be able to lead team in developing application, development, network, and technical architectures for mid-range client/server and mainframe applications. Develops and executes architecture strategies and performs feasibility studies and integration analyses. Experience supervising and providing guidance in implementing various architectures.

Experience: At least 9 years of relevant experience.

Education: BA. or B.S. degree in Computer Science, Engineering or a related field or equivalent experience.

* Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.2.47 **Network Engineer 1**

Duties: The Network Engineer plans, supports and evaluates complex existing network systems and make recommendations for resources required to maintain and/or expand service levels. This resource will provide highly skilled technical assistance in network planning, engineering and architecture. Plans and incorporates how new network resources and applications will exist on the network. Provide monthly metrics for network availability and bandwidth usage as well as other metrics as requested. Responsible for network capacity planning, user support, and escalation of issues to upper tiers. Use network management tools to discover, map and maintain the network. Responsible for network equipment OS and version upgrades. Maintain Internet and Extranet connectivity; handles day-to-day Firewall administration, as well as VPN
connectivity. Monitor and maintain network interfaces to insure its highest level of performance and makes modifications and enhancements as needed. Responsible for documenting procedures and keeping network diagrams and related material up to date. Handle user problems, questions, and request on network issues. Work with other groups within IS to resolve network related issues as needed.

Experience: Requires at least 2 years relevant experience.

Education: B.S. or B.A. degree in Computer Science, Engineering or related fields (or equivalent experience).

8.2.48 Program Manager

Duties: Performs day-to-day management of delivery order projects for ERP technology projects that involve teams of data processing and other information systems management professionals who have previously been involved in analyzing, designing, integrating, testing, documenting, convening, extending, and implementing automated information and telecommunications systems. Demonstrates proven skills in those technical areas addressed by the delivery order to be managed. organizes, directs, and coordinates the planning and production of all activities associated with assigned deliverables. Establishes and alters, as necessary, corporate management structure to direct effective contract support activities. Demonstrates good written and oral communications.

Experience: Must have 10 years of IT experience, including at least 7 years of IT and/or telecommunications system management experience.

Education: B.A. or B.S. degree. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.2.49 Programmer 1

Duties: Under close supervision support the design, code, development, test and document application programs. Support modification to existing programs and procedures.

Experience: This is the entry level position for this job category.

Education: B.A. or B.S. degree in Computer Science, Engineering or a related field or an equivalent degree. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.2.50 Programmer 3

Duties: Support the design, code, development, test and document application programs. Support modification to existing programs and procedures. Support creation of procedural forms and documentation, including flow charts and system documentation. Provide assistance to lower level individuals within the same job category.

Experience: At least 4 years of relevant experience.

Education: B.A. or B.S. degree in Computer Science, Engineering or a related field or an equivalent degree. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.2.51 Programmer 5

Duties: Leads the design, coding, development, testing and documentation of application programs. Lead the modifications to, and maintenance of, existing programs and procedures.
Specify creation of procedural forms and documentation, including flow charts and system documentation. Lead associated task team efforts.

Experience: At least 7 years of relevant experience.

Education: B.A. or B.S. degree in Computer Science, Engineering or a related field or an equivalent degree. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

**8.2.52 Subject Matter Expert 1**

Duties: Develops requirements from a project's inception to its conclusion in the subject matter area for moderately complex systems. Assists other senior consultants with analysis and evaluation and with the preparation of recommendations for system improvements, optimization, development, and/or maintenance efforts in the following specialties: information systems architecture; networking; telecommunications; automation; risk management; software; life-cycle management; software development methodologies; modeling and simulation.

Experience: At least 8 years of IT experience and at least 5 years directly related to the required area of expertise.

Education: B.A. or B.S. degree. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

**8.2.53 Systems Administrator 1**

Duties: Assists with the installation, maintenance and usage of a system under supervision. Installs software and troubleshoots user and system problems.

Experience: This is the entry level position for this job category.

Education: Associate's Degree in Computer Science, Engineering or a related field.

**8.2.54 Systems Administrator 3**

Duties: Responsible for the installation, maintenance and usage of a system under supervision. Install software and troubleshoot user and system problems. Maintain system security. Implement policies, procedures and standards.

Experience: At least 5 years of relevant experience.

Education: BA. or B.S. degree in Computer Science, Engineering or a related field or equivalent experience. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

**8.2.55 Systems Analyst 1**

Duties: Under close supervision gathers facts, analyses data, compares alternatives in terms of cost, time and availability of equipment/personnel. Supports determination and resolution of data processing problems and coordinates work.

Experience: This is the entry level position for this job category.

Education: B.A. or B.S. degree in Computer Science, Engineering, Business or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.
8.2.56  Systems Analyst 3

Duties: Applies systems analysis and design techniques to complex computer systems in a broad area. Competent in all phases of systems analysis techniques, concepts and methods. Has knowledge of available system software, computer equipment, regulations, practices, etc. in a subject matter area. Recognizes probable conflicts and integrating diverse data sources. Maintains and modifies complex systems or develops new subsystems. Recommends optimum approach and develops system design.

Experience: At least 5 years of relevant experience.

Education: B.A. or B.S. degree in Computer Science, Engineering, Business or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor’s degree requirement.

8.2.57  Systems Analyst 4

Duties: Applies expert systems analysis and design techniques to complex computer systems in an area. Has broad knowledge of data sources/flaw, interactions of complex systems, and capabilities/limitations of systems software and computer equipment. Establishes framework of new computer systems from feasibility studies to past implementation evaluation. Recognizes probable conflicts and integrating diverse data sources. Produces innovative solutions for a variety of complex problems. Prepares overall project recommendations.

Experience: At least 7 years of relevant experience.

Education: B.A. or B.S. degree in Computer Science, Engineering, Business or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor’s degree requirement.

8.2.58  Systems Engineer 1

Duties: Provides technical support in system architecture, system design, system integration and technical management. Assists in providing technical input to the systems engineering process. May assist in developing and implementing installation plans. May assist in preparation and presentation of systems assurance reviews. Identifies requirements and deficiencies in hardware and software products.

Experience: At least 2 years of relevant experience.

Education: B.A. or B.S. degree in Computer Science, Engineering or a related field or equivalent experience. Five (5) years of direct related experience in a related field may be substituted for a Bachelor’s degree requirement.

8.2.59  Systems Engineer 3

Duties: Provides technical support in system architecture, system design, system integration and technical management. Assists in providing technical input to the systems engineering process. Leads teams in developing application and technical plans. Guide customers in the installation and use of strategic products through education and guidance, first-rise and tuning assistance problem solving and critical situation resolution.

Experience: At least 7 years of relevant experience.

Education: B.A. or B.S. degree in Computer Science, Engineering or a related field or equivalent experience. Five (5) years of direct related experience in a related field may be substituted for a Bachelor’s degree requirement.
8.2.60 Systems Engineer 4

Duties: Provides technical leadership in system architecture, system design, system integration and technical management. Assists in providing technical input to the systems engineering process. Leads teams in developing application and technical plans. Guide customers in the installation and use of strategic products through education and guidance, first-use and tuning assistance problem solving and critical situation resolution.

Experience: At least 8 years of relevant experience.

Education: B.A. or B.S. degree in Computer Science, Engineering or a related field or equivalent experience. Five (5) years of direct related experience may be substituted for a Bachelor's degree requirement.

8.2.61 Technical Writer 3

Duties: Formats, writes, edits, proofreads technical data for use in documents. Ensures document meets specifications and complies with quality, format and style standards. Creates new documentation from related documentation, examination of subject system or procedure, and/or interviews.

Experience: At least 4 years of relevant experience.

Education: BA. or B.S. degree in English, a related field or a technical field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.2.62 Test Engineer 2

Duties: Design review, test plan creation, test case implementation, defect report creation and Packing, and documentation review. Work with other testing team members to accomplish specific product testing tasks. Review product requirements, Develop, maintain, and execute test cases. Create and maintain datasets. Create and execute automation scripts. Isolate defects and enter software defect reports. Continual review and improvement of testing process and implementation. Analyze and report progress to Test Manager

Experience: Requires at least 7 years relevant experience for this job category

Education: B.S. or B.A. degree in related field (or equivalent experience).

8.2.63 Testing Specialist

Duties: Must be capable of designing and executing ADP software tests and evaluating results to ensure compliance with applicable regulations. Must be able to prepare test scripts and all required test documentation. Must be able to design and prepare all needed test data. Analyze internal security within systems. Reviews test results and evaluates for conformance to design.

Experience: At least 2 years or software testing experience (integration and acceptance).

Education: B.A. or B.S. degree or 3 years of equivalent experience in a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.2.64 Training Specialist 2

Duties: Analyze training needs to develop new Information Technology training programs or modify and improve existing programs. Conduct or arrange for ongoing technical training and personal development classes for staff members. Conduct orientation sessions and arrange on-
the-jab training. Conduct surveys to identify training needs based on projected production processes, changes, and other factors. Develop and organize training manuals, multimedia visual aids, and other educational materials. Develop testing and evaluation procedures.

Experience: Requires at least 7 years relevant experience for this job category
Education: Minimum B.S. or B.A. degree in related field (or equivalent experience).

8.2.65 Business Process Analyst 1

Duties: Assist in the integration of program activities into a detailed strategic plan and programmatic level schedule. The Analyst shall assist in generating and maintaining detailed networked schedules.

Experience: Requires at least 1 year relevant experience.
Education: Minimum B.S. or B.A. degree in related field (or equivalent experience).

8.2.66 Business Process Analyst 2

Duties: Integrate program activities into detailed strategic plans and programmatic level schedules including

integrating high-level mission milestones, operations and implementation milestones and engineering milestones along with preparation activities, maintenance activities, resource requirements and costs. Assist in the setup of tools and procedures to collect, evaluate and report on program metrics. Shall also generate and maintain a detailed networked schedule that includes key activities, key critical events, completion dates for contractually required documents, preparation plans, preparation activities and rolled-up activities/milestones from implementation support and reviews.

Experience: Requires at least 3 years relevant experience.
Education: Minimum B.S. or B.A. degree in related field (or equivalent experience).

8.2.67 Business Process Engineer 1

Duties: Assist in translation, design and optimization of process flows and analytical solutions implemented in software systems. Assist in modeling and implementing complex workflows in a Business Process Management Suite (BPMS) type of tool. Assist in translating and communicating complex concepts to a specified audience.

Experience: Requires at least 4 years relevant experience.
Education: Minimum B.S. or B.A. degree in related field (or equivalent experience).

8.2.68 Business Process Engineer 2

Duties: Assist in translation, design and optimization of process flows and analytical solutions implemented in software systems. Model and implement complex workflows in a Business Process Management Suite (BPMS) type of tool. Translate and communicate complex concepts to broad audiences. Support liaison relationships with other multi-functional groups.

Experience: Requires at least 6 years relevant experience.
Education: Minimum B.S. or B.A. degree in related field (or equivalent experience).
8.2.69 Cyber Analyst 1
Duties: Under supervision provides day-to-day support to cyber security operations. Gathers data and perform technical and operational analysis of cyber security operations, reporting, and management. Supports presentations and facilitates discussion of security operations with senior management. Draft communications, reports, and analysis documentation.

Experience: Requires at least 3 years relevant experience in a Cyber Security role.

Education: Minimum B.S. or B.A. degree in related field.

8.2.70 Cyber Analyst 2
Duties: Provides day-to-day support to cyber security operations. Gathers and interprets data and perform technical and operational analysis of cyber security operations, reporting, and management. Develops presentations and facilitates discussion of security operations with senior management. Draft communications, reports, and analysis documentation.

Experience: Requires at least 5 years relevant experience in a Cyber Security role.

Education: Minimum B.S. or B.A. degree in related field.

8.2.71 Cyber Analyst 3
Duties: Provides leadership in the day-to-day support to cyber security operations. Reviews and interprets data and perform technical and operational analysis of cyber security operations, reporting, and management. Leads presentations and facilitates discussion of security operations with senior management.

Experience: Requires at least 8 years relevant experience in a Cyber Security role.

Education: Minimum B.S. or B.A. degree in related field.

8.2.72 Cyber Engineer 1
Duties: Under supervision provides support to cyber security operations, policy and threat mitigation. Perform duties utilizing cyber security tools, network topologies, intrusion detection, and secured networks. Support interpretation and implementation of cyber security regulations.

Experience: Requires at least 3 years relevant experience in a Cyber Security role.

Education: Minimum B.S. or B.A. degree in related field.

8.2.73 Cyber Engineer 2
Duties: Provides support to cyber security operations, policy and threat mitigation. Perform duties utilizing cyber security tools, network topologies, intrusion detection, and secured networks. Integrates metrics into the security posture of the organization, identifies areas of weakness and vulnerability and recommends changes to meet security standards. Interpret, implements and monitors compliance to cyber security regulations.

Experience: Requires at least 5 years relevant experience in a Cyber Security role.

Education: Minimum B.S. or B.A. degree in related field.

8.2.74 Cyber Engineer 3
Duties: Provides leadership to cyber security operations, policy and threat mitigation. Oversees cyber security tools, network topologies, intrusion detection, and secured networks. Reviews applicability of metrics used for assessment of security posture of the organization, acts on areas
of weakness and vulnerability and leads implementation of changes to meet security standards. Provide technical direction and guidance to other Cyber Security Engineers, Information Technology and the organization to align with regulatory and security requirements.

Experience: Requires at least 8 years relevant experience in a Cyber Security role.

Education: Minimum B.S. or B.A. degree in related field.

8.2.75 Security Engineer 1

Duties: Under supervision supports the design and implementation of solutions for intrusion detection and notification, security auditing, alerting, and response, virus detection and removal, password complexity enforcement, and media protection. Support the status of system security patch deployments. Support the update of Standard Operating Procedures for the implemented security controls, prepares and conducts staff security awareness training, and develops budget and schedule plans for security-related activities.

Experience: Requires at least 3 years relevant experience in a security role.

Education: Minimum B.S. or B.A. degree in related field.

8.2.76 Security Engineer 2

Duties: Designs and implements solutions for intrusion detection and notification, security auditing, alerting, and response, virus detection and removal, password complexity enforcement, and media protection. Maintain status of system security patch deployments. Develops and updates Standard Operating Procedures for the implemented security controls, prepares and conducts staff security awareness training, and develops budget and schedule plans for security-related activities. We expect the candidate to be a working manager, both leading development activities and performing recurring security-related activities to ensure implementation, sustainment, and effectiveness of implemented security controls.

Experience: Requires at least 5 years relevant experience in a security role.

Education: Minimum B.S. or B.A. degree in related field.

8.2.77 Security Engineer 3

Duties: Provides leadership in the design and implementation of solutions for intrusion detection and notification, security auditing, alerting, and response, virus detection and removal, password complexity enforcement, and media protection. Review status of system security patch deployments. Review Standard Operating Procedures for the implemented security controls, prepares and conducts staff security awareness training, and evaluates budget and schedule plans for security-related activities. Serve as a working manager, both leading development activities and performing recurring security-related activities to ensure implementation, sustainment, and effectiveness of implemented security controls.

Experience: Requires at least 8 years relevant experience in a security role.

Education: Minimum B.S. or B.A. degree in related field.

8.2.78 Data Warehouse Analyst 1

Duties: Under supervision support the development, maintenance and management of the data warehouse, including the logical and physical design, database management, acquisition of data, and overall implementation.
Experience: Requires at least 3 years relevant experience in data warehouse and data mart applications.

Education: Minimum B.S. or B.A. degree in IT or other related discipline.

8.2.79 Data Warehouse Engineer 1

Duties: Under supervision support the design, development and maintain data integration services, data visualization, and APIs and tools that deliver data warehouse and big data services to the Practice Fusion team and external partners.

Experience: Requires at least 3 years relevant experience in IT or related role.

Education: Minimum B.S. or B.A. degree in IT or other related discipline.

8.2.80 Disaster Recovery/COOP/Contingency Administrator 2

Duties: Develop, implement and maintain the IT Disaster Recovery Program (DR) and Business Continuity Plan. The person will work with a team to plan and develop an IT Disaster Recovery Program in alignment with the Business Continuity of Operations Plan. Program activities include coordinating technical and logistical planning for IT systems and infrastructure, selection of an IT DR site, negotiating IT DR site contract, planning migration and conducting incident management activities in response to disasters.

Experience: Requires at least 5 years relevant experience including application development and IT operations; procurement, contracting, RFI, RFP, or RFQ process; selecting Data Center or Disaster Recovery sites; and with continuity of operations planning, business impact analyses.

Education: Minimum B.S. or B.A. degree in IT or other related discipline.

8.2.81 Program & Policy Analyst 1

Duties: Proactively support and identify changes needed in programs and policy and to align and support strategic shifts in business strategy. Assist to ensure formal business policy issuances are complete, current, and operationally relevant. Provide input into the revision and/or development of programs and policies to comply with emerging national requirements.

Experience: Requires at least 3 years relevant experience. Knowledge and understanding of public law, Executive Orders, Presidential Directives and Federal regulations governing programs and policies.

Education: Minimum B.S. or B.A. degree in IT or other related discipline.

8.2.82 Program & Policy Analyst 3

Duties: Provide leadership to proactively identify changes needed in programs and policy and to align and support strategic shifts in business strategy. Ensure formal business policy issuances are complete, current, and operationally relevant. Lead the revision and/or development of programs and policies to comply with emerging national requirements. Monitor on a continuing basis proposed and newly promulgated Federal legislation, Office of Management and Budget guidance, and other national level policy affecting programs and policies need to perform analysis and identify policy gaps. Identify program and policy changes necessary to improve acquisition and integrate these policies and procedures into the acquisition process.

Experience: Requires at least 8 years relevant experience. Knowledge and understanding of public law, Executive Orders, Presidential Directives and Federal regulations governing programs and policies.
Education: Minimum B.S. or B.A. degree in IT or other related discipline.

8.2.83 Certification and Accreditation Analyst 1

Duties: Provide support to all activities needed to obtain certification and accreditation on all the networks, equipment and systems at all classification levels under the purview of the Office of the Administrative Assistant (OAA) Designated Approving Authority (DAA).

Experience: Requires at least 3 years relevant experience. Knowledge and understanding of public law, Executive Orders, Presidential Directives and Federal regulations governing programs and policies.

Education: Minimum B.S. or B.A. degree in IT or other related discipline.

8.2.84 Certification and Accreditation Analyst 3

Duties: Provide leadership to all activities needed to obtain certification and accreditation on all the networks, equipment and systems at all classification levels under the purview of the Office of the Administrative Assistant (OAA) Designated Approving Authority (DAA). Administer the Connection Approval Program and Tenant Security Process in accordance with Army, DoD, Joint, Intelligence Community regulation or policy. Provide technical support to DoD information system programs for life cycle security support, from inception of the program through initial accreditation. Develop a methodology and procedures to be followed by accreditation personnel while providing life cycle security support. Participate in formal and ad hoc certification and accreditation working groups where directed. Provide technical documentation required for the site certification and accreditation process. Monitor the implementation of and compliance with, DIACAP C&A standards to ensure uniform application of the standards and consistency in security of accredited DoD information systems.

Experience: Requires at least 8 years relevant experience. Knowledge and understanding of public law, Executive Orders, Presidential Directives and Federal regulations governing programs and policies.

Education: Minimum B.S. or B.A. degree in IT or other related discipline.

8.2.85 Administrative Assistant 2

Duties: Answer the phone and track office supplies. Routine clerical work including typing documents, organizing meetings, tracking paper and electronic files. Proofreading and editing documents that are highly technical in nature created by others to ensure proper format, grammar, and style.

Experience: Requires at least 5 years relevant experience including desktop PC software (Windows).

Education: Minimum High School or GED.

8.2.86 Contracts Administrator 2

Duties: Administers, extends, negotiates and terminates standard and nonstandard contracts. Perform proposal preparation, contract negotiation, contract administration, and customer contact activities to provide for proper contract acquisition and fulfillment in accordance with established policies, legal requirements and specifications. Conduct the review of estimates of material, equipment services, production costs, performance requirements, and delivery schedules to ensure accuracy and completeness.

Experience: Requires at least 6 years relevant experience.
Education: Minimum B.S. or B.A. degree in Business, Finance or related field.

8.2.87 Financial Analyst 1

Duties: Under supervision input of financial data using desktop tools and validate data following input. Create ad hoc reports as directed.

Experience: Requires at least 2 years relevant experience including desktop PC software (Windows).

Education: Minimum B.S. or B.A. degree in Business or Finance.

8.2.88 Financial Analyst 3

Duties: Lead in the creation of strategically tailored financial reports. Conduct targeted review of status and identify points of risk, what-if analysis. Identify alternative strategies for addressing risk. Perform hard core analysis, fact verification, study and research as well as planning and decision making on financial analysis.

Experience: Requires at least 10 years relevant experience including desktop PC software (Windows).

Education: Minimum B.S. or B.A. degree in Business or Finance.

8.2.89 Facility Engineer 1

Duties: Support the programming and coordinating the inspection and the repairs. Take part in the testing and calibration of electrical and mechanical systems. Provide support to demonstrating, building and enforcing the best exercises for all projects and functions within the facility.

Experience: Requires at least 3 years relevant experience.

Education: Minimum B.S. or B.A. degree in a related field or an additional 4 years related experience.

8.3 SIN 54151HEAL - Health Information Technology Services

8.3.1 IT Health Services Project Controls II

Experience: Requires at least 4 years relevant experience.

Functional Responsibilities: Calculates network schedules and make use of project scheduling software. They should understand alternate scheduling techniques such as linear scheduling, problems with resource constraints and apply basic techniques of resource leveling to scheduling. They should possess the ability to apply work breakdown structures and cost load a schedule as well as perform earned value calculations. They should have experience with the basics of conceptual and detailed (quantity) estimating and understand broad concepts of cost and time control as related to phases of the project and project organization. Finally, they will understand and apply basic visualization of project controls, including visualizations of quantitative controls data. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: B.S. or B.A. degree in Computer Science, Engineering or related fields (or equivalent experience).
8.3.2  IT Health Services Project Manager I

Experience: At least five years of industry experience with at least two to three years as a project manager.

Functional Responsibilities: Provides overall direction to the formulation, development, implementation and delivery of a moderately complex project or one that is part of a larger program. Ensures that the project plan maintains tasks, schedules, estimates and status. Disseminates information to project members. Arranges for the assignment of responsibility to other supporting facilities, business areas, support functions and monitors their performance. Has supervisory responsibilities for hiring, terminating and reviewing project members. Should possess good communication skills. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: B.A. or B.S. degree in Computer Science, Engineering, Business or a related field. * Five (5) years of direct related experience in a related field may be substituted for a Bachelor’s degree requirement.

8.3.3  IT Health Services Project Manager II

Experience: At least 7 years of industry experience with at least three to five years as a project manager.

Functional Responsibilities: Provides overall direction to the formulation, development, implementation and delivery of a complex project. Ensures that the project plan maintains tasks, schedules, estimates and status. Disseminates information to project members. Arranges for the assignment of responsibility to other supporting facilities, business areas, support functions and monitors their performance. Has supervisory responsibilities for hiring, terminating and reviewing project members. Should possess good communication skills. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: B.A. or B.S. degree in Computer Science, Engineering, Business or a related field. * Five (5) years of direct related experience in a related field may be substituted for a Bachelor’s degree requirement.

8.3.4  IT Health Services Quality Assurance Manager

Experience: Requires at least 5 years relevant experience for this job category.

Functional Responsibilities: Plans, directs and coordinates quality control-related activities. Responsible for ensuring that all hardware products and business processes represent the maximum quality and reliability attainable. Approves all quality control procedures, technical specifications and procurement of quality-related test equipment. Responsible for overall program design. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this
category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: B.S. or B.A. degree in related field.

8.3.5 IT Health Systems Architect

Experience: At least 5 years of relevant experience.

Functional Responsibilities: Prepares and plans the overall software development environment. Performs development tools selections. Performs benchmarking for optimizing the systems platforms. Develops prototypes and acts as the primary lead technical consultant in a software development environment. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: B.A. or BS, degree in Computer Science, Engineering or a related field or equivalent experience.

*Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.3.6 IT Health Systems Programmer II

Experience: At least 3 years of relevant experience.

Functional Responsibilities: Installs, debugs and tunes internal operating system software. Performs systems maintenance and upgrades. Monitors and times system hardware and software. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: B.A. or B.S. degree in Computer Science, Engineering, or a related field.

*Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.3.7 IT Health Services Test Engineer I

Experience: Requires at least 1 year of relevant experience for this job category.

Functional Responsibilities: Design review, test plan creation, test case implementation, defect report creation and tracking, and documentation review. Work with other testing team members to accomplish specific product testing tasks. Review product requirements. Develop, maintain, and execute test cases. Create and maintain datasets. Create and execute automation scripts. Isolate defects and enter software defect reports. Continual review and improvement of testing process and implementation. Analyze and report progress to Test Manager. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.
Education: B.S. or B.A. degree in related field (or equivalent experience).

8.3.8 IT Health Database Specialist (Senior)

Experience: Database Specialist (Senior) possesses 2 years of experience in information systems networks, operations, engineering and design and may possess a security clearance.

Functional Responsibility: Apply their strong analytical and technical skills to assist in implementing IT business solutions. An IT Administrator 2 applies their core skills and/or specific IT skills on projects. They direct small teams and interact with the clients at the supervisory level. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Minimum Education: Bachelor’s Degree or 3 years additional related experience.

8.3.9 IT Health Systems Engineer

Experience: Systems Engineer possesses at least 6 years of experience in information systems networks, operations, engineering and design and may possess a security clearance.

Functional Responsibility: Apply their strong analytical and technical skills to assist in implementing IT business solutions. An IT Administrator 3 applies their core skills and/or specific IT skills on projects. They direct teams and interact with the clients at the supervisory or program level. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Minimum Education: Bachelor’s Degree or 4 years additional related experience.

8.3.10 IT Health Applications Developer (Journeyman)

Experience: Applications Developer (Journeyman) possesses 2 years of experience in information systems implementations, change management efforts or business process redesign and may possess a security clearance.

Functional Responsibility: Apply their strong analytical and technical skills to assist in implementing IT business solutions. An IT Consultant 2 may apply their core skills and/or specific IT skills on projects. They may direct small teams and interact with the clients at the supervisory level. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Minimum Education: Bachelor’s Degree or 3 years additional related experience.

8.3.11 IT Health Applications Developer (Senior)

Experience: Applications Developer (Senior) possesses at least 6 years of experience in information systems implementations, change management efforts or business process redesign and may possess a security clearance.
Functional Responsibility: Apply their strong analytical and technical skills to assist in implementing IT business solutions. An IT Consultant applies their core skills and/or specific IT skills on projects. They direct teams and interact with the clients at the supervisory or program level. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Minimum Education: Bachelor’s Degree or 4 years additional related experience.

8.3.12 IT Health Services Quality Assurance Specialist (Journeyman)

Experience: Quality Assurance Specialist (Journeyman) possesses at least 4 years of experience in leading information systems implementations, change management efforts or business process redesign and may possess a security clearance.

Functional Responsibility: Apply their broad management skills and functional and technical expertise to guide project teams in delivering IT solutions to the client. Ensures that the project plan maintains tasks, schedules, estimates and status. Disseminates information to project members. Arranges for the assignment of responsibility to other supporting facilities, business areas, support functions and monitors their performance. Has supervisory responsibilities for hiring, terminating and reviewing project members. Should possess good communication skills.

All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Minimum Education: Bachelor’s Degree or 4 years additional related experience.

8.3.13 IT Health Data Security Analyst 1

Experience: Data Security Analyst 1 possesses up to 3 years of commensurate experience and possesses a security clearance.

Functional Responsibility: Under close supervision, performs procedures necessary to ensure the safety of information, systems assets and to protect systems from intentional or inadvertent access or destruction. Interfaces with user community to understand their security needs and implements procedures to accommodate them. Ensures that user community understands and adheres to necessary procedures to maintain security. Conducts accurate evaluation of the level of security required. Provides management with status reports. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Minimum Education: B.A. or B.S. degree in Computer Science, Engineering or a related field or equivalent experience., IAT or IAM Level I Security+, Security Tools Training, MCP.

8.3.14 IT Health Data Security Analyst 2

Experience: Data Security Analyst 2 possesses at least 3 years of commensurate experience and possesses a security clearance.

Functional Responsibility: Under close supervision, performs procedures necessary to ensure the safety of information, systems assets and to protect systems from intentional or inadvertent
access or destruction. Interfaces with user community to understand their security needs and implements procedures to accommodate them. Ensures that user community understands and adheres to necessary procedures to maintain security. Conducts accurate evaluation of the level of security required. Provides management with status reports. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Minimum Education: B.A. or B.S. degree in Computer Science, Engineering or a related field or equivalent experience., IAT or IAM Level I Security+, Security Tools Training, MCP.

8.3.15 IT Health Data Security Analyst 3

Experience: Data Security Analyst 3 possesses at least 5 years of commensurate experience and possesses a security clearance.

Functional Responsibility: Under direct supervision, performs procedures necessary to ensure the safety of information, systems assets and to protect systems from intentional or inadvertent access or destruction. Interfaces with user community to understand their security needs and implements procedures to accommodate them. Ensures that user community understands and adheres to necessary procedures to maintain security. Conducts accurate evaluation of the level of security required. Provides management with status reports. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Minimum Education: B.A. or B.S. degree in Computer Science, Engineering or a related field or equivalent experience. IAT or IAM Level I Security+, Security Tools Training, MCP.

8.3.16 IT Health Data Security Analyst 4

Experience: Data Security Analyst 4 possesses at least 7 years of commensurate experience and possesses a security clearance.

Functional Responsibility: Performs procedures necessary to ensure the safety of information, systems assets and to protect systems from intentional or inadvertent access or destruction. Interfaces with user community to understand their security needs and implements procedures to accommodate them. Ensures that user community understands and adheres to necessary procedures to maintain security. Conducts accurate evaluation of the level of security required. Provides management with status reports. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Minimum Education: B.A. or B.S. degree in Computer Science, Engineering or a related field or equivalent experience. IAT or IAM Level I Security+, Security Tools Training, MCP.

8.3.17 IT Health Data Security Analyst 5

Experience: Data Security Analyst 5 possesses at least 9 years of commensurate experience and possesses a security clearance.
Functional Responsibility: Performs procedures necessary to ensure the safety of information, systems assets and to protect systems from intentional or inadvertent access or destruction. Interfaces with user community to understand their security needs and implements procedures to accommodate them. Ensures that user community understands and adheres to necessary procedures to maintain security. Conducts accurate evaluation of the level of security required. Provides management with status reports. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Minimum Education: B.A. or B.S. degree in Computer Science, Engineering or a related field or equivalent experience. IAT or IAM Level I Security+, Security Tools Training, MCP.

8.3.18 IT Health Services Threat Analyst 1

Experience: Threat Analyst 1 possesses up to 3 years of commensurate experience and possesses a security clearance.

Functional Responsibility: Support the profiling of new and emerging threats to the IT landscape. Support the analysis of vulnerabilities in software, and determining how client will best defend themselves against these threats. Support monitoring of third party security related websites, forums, and mailing lists for information regarding vulnerabilities and exploits. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Minimum Education: B.A. or B.S. Degree in Computer Science, Engineering, Business or a related field, some certifications such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training.

8.3.19 IT Health Services Threat Analyst 2

Experience: Threat Analyst 2 possesses at least 3 years of commensurate experience and possesses a security clearance.

Functional Responsibility: Support the profiling of new and emerging threats to the IT landscape. Support the analysis of vulnerabilities in software, and determining how client will best defend themselves against these threats. Support monitoring of third party security related websites, forums, and mailing lists for information regarding vulnerabilities and exploits. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Minimum Education: B.A. or B.S. Degree in Computer Science, Engineering, Business or a related field, some certifications such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training.

8.3.20 IT Health Services Threat Analyst 3

Experience: Threat Analyst 3 possesses at least 5 years of commensurate experience and possesses a security clearance.
Functional Responsibility: Profile new and emerging threats to the IT landscape. Analyze and determine the scope of vulnerabilities in software, and determining how client will best defend themselves against these threats. Monitor third party security related websites, forums, and mailing lists for information regarding vulnerabilities and exploits. Verify the vulnerabilities; correlate and collate the information; and develop, edit, and deliver security reports to enterprise-level customers. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Minimum Education: B.A. or B.S. Degree in Computer Science, Engineering, Business or a related field, certifications such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training and similar technologies.

8.3.21 IT Health Services Threat Analyst 4

Experience: Threat Analyst 4 possesses at least 7 years of commensurate experience and possesses a security clearance.

Functional Responsibility: Lead the profiling of new and emerging threats to the IT landscape. Analyze and determine the scope of vulnerabilities in software, and determining how client will best defend themselves against these threats. Monitor third party security related websites, forums, and mailing lists for information regarding vulnerabilities and exploits. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002. Verify the vulnerabilities; correlate and collate the information; and develop, edit, and deliver security reports to enterprise-level customers. On occasion replicate reported vulnerabilities where appropriate to develop proof of concept and/or exploit tools against these vulnerabilities. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Minimum Education: B.A. or B.S. Degree in Computer Science, Engineering, Business or a related field, certifications such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training and similar technologies.

8.3.22 IT Health Services Threat Analyst 5

Experience: Threat Analyst 5 possesses at least 9 years of commensurate experience and possesses a security clearance.

Functional Responsibility: Lead the profiling of new and emerging threats to the IT landscape. Analyze and determine the scope of vulnerabilities in software, and determining how client will best defend themselves against these threats. Monitor third party security related websites, forums, and mailing lists for information regarding vulnerabilities and exploits. Verify the vulnerabilities; correlate and collate the information; and develop, edit, and deliver security reports to enterprise-level customers. On occasion replicate reported vulnerabilities where appropriate to develop proof of concept and/or exploit tools against these vulnerabilities. Provide senior leadership to clients in the areas of Cyber Security Threats Prevention. All category
performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Minimum Education: B.A. or B.S. Degree in Computer Science, Engineering, Business or a related field, certifications such as CISSP, CEH, GCIH, GCIA, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training and similar technologies.

8.3.23 IT Health System Forensics Analyst 1

Experience: Forensics Analyst 1 possesses up to 3 years of commensurate experience and possesses a security clearance.

Functional Responsibility: Supports forensic analysis of digital information and other computer evidence by gathering, handling, examining, preparing, investigating, searching, retrieving, identifying and/or comparing digital and/or physical evidence. Supports research and development, organizational and vulnerability assessments, intelligence and threat analysis, mission requirements determination, policy and procedures development, concept definition design, testing, integration verification and validation, documentation, implementation, and operations and maintenance. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Minimum Education: B.A. or B.S. Degree in Computer Science, Engineering, Business or a related field, some certifications such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training and similar technologies.

8.3.24 IT Health System Forensics Analyst 2

Experience: Forensics Analyst 2 possesses at least 3 years of commensurate experience and possesses a security clearance.

Functional Responsibility: Supports forensic analysis of digital information and other computer evidence by gathering, handling, examining, preparing, investigating, searching, retrieving, identifying and/or comparing digital and/or physical evidence. Supports research and development, organizational and vulnerability assessments, intelligence and threat analysis, mission requirements determination, policy and procedures development, concept definition design, testing, integration verification and validation, documentation, implementation, and operations and maintenance. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Minimum Education: B.A. or B.S. Degree in Computer Science, Engineering, Business or a related field, some certifications such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training and similar technologies.

8.3.25 IT Health System Forensics Analyst 3

Experience: Forensics Analyst 3 possesses at least 5 years of commensurate experience and at least 2 years of hands-on experience as a security operations analyst in a 24/7 Security
Operations Center or a Computer Security Incident Response Team and possesses a security clearance.

Functional Responsibility: Performs forensic analysis of digital information and other computer evidence. Providing specialized support by gathering, handling, examining, preparing, investigating, searching, retrieving, identifying and/or comparing digital and/or physical evidence. Understanding and using forensically sound procedures to determine results. Provides integral support in research and development, organizational and vulnerability assessments, intelligence and threat analysis, mission requirements determination, policy and procedures development, concept definition design, testing, integration verification and validation, documentation, implementation, and operations and maintenance. Works closely with stakeholders to determine requirements and ensure compliance with exceptions. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Minimum Education: B.A. or B.S. Degree in Computer Science, Engineering, Business or a related field, certifications such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training and similar technologies.

8.3.26 IT Health System Forensics Analyst 4

Experience: Forensics Analyst 4 possesses at least 7 years of commensurate experience and at least 2 years of hands-on experience as a senior level security operations analyst in a 24/7 Security Operations Center or a Computer Security Incident Response Team and possesses a security clearance.

Functional Responsibility: Leads management analysis processes, statistical methods, and advanced technical and analytical research techniques to develop security solutions and strategies based on client requirements with a law enforcement, professional security, or emergency preparedness services-based scope. Performing forensic analysis of digital information and other computer evidence. Providing specialized support by gathering, handling, examining, preparing, investigating, searching, retrieving, identifying and/or comparing digital and/or physical evidence. Understanding and using forensically sound procedures to determine results. Provides integral support in research and development, organizational and vulnerability assessments, intelligence and threat analysis, mission requirements determination, policy and procedures development, concept definition design, testing, integration verification and validation, documentation, implementation, and operations and maintenance. Works closely with stakeholders to determine requirements and ensure compliance with exceptions. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Minimum Education: B.A. or B.S. Degree in Computer Science, Engineering, Business or a related field, certifications such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training and similar technologies.

8.3.27 IT Health System Forensics Analyst 5

Experience: Forensics Analyst 5 possesses at least 9 years of commensurate experience and at least 2 years of hands-on experience as a senior level security operations analyst in a 24/7
Security Operations Center or a Computer Security Incident Response Team and possesses a security clearance.

Functional Responsibility: Leads management analysis processes, statistical methods, and advanced technical and analytical research techniques to develop security solutions and strategies based on client requirements with a law enforcement, professional security, or emergency preparedness services-based scope. Performing forensic analysis of digital information and other computer evidence. Providing specialized support by gathering, handling, examining, preparing, investigating, searching, retrieving, identifying and/or comparing digital and/or physical evidence. Understanding and using forensically sound procedures to determine results. Provides integral support in research and development, organizational and vulnerability assessments, intelligence and threat analysis, mission requirements determination, policy and procedures development, concept definition design, testing, integration verification and validation, documentation, implementation, and operations and maintenance. Works closely with stakeholders to determine requirements and ensure compliance with exceptions. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Minimum Education: B.A. or B.S. Degree in Computer Science, Engineering, Business or a related field, certifications such as CISSP, CEH, GCIA, GCIH, CCNA/CCNP, CCSP, MCSE, IDP and SIEM training and similar technologies.

8.3.28 IT Health System Security Assurance Analyst 1

Experience: Security Assurance Analyst 1 possesses up to 3 years of relevant hands-on experience and possesses a security clearance.

Functional Responsibility: Under general supervision, performs procedures necessary to ensure the safety of information systems assets and to protect systems from intentional or inadvertent access or destruction. Assists in performing multiple duties, such as installation, configuration, maintenance and administration of various information assurance systems, to include Firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), and Security Event and Information Management (SEIM) systems. Performing security analysis, problem reporting, tracking and documenting resolutions and performance issues. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Minimum Education: CISA, CEH, Security+, CCNA, MCP, TippingPoint training and similar technologies. Working towards CISSP certification

8.3.29 IT Health System Security Assurance Analyst 2

Experience: Security Assurance Analyst 2 possesses at least 3 years of relevant hands-on experience and possesses a security clearance.

Functional Responsibility: Under general supervision, performs procedures necessary to ensure the safety of information systems assets and to protect systems from intentional or inadvertent access or destruction. Assists in performing multiple duties, such as installation, configuration, maintenance and administration of various information assurance systems, to include Firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), and Security Event and Information
Management (SEIM) systems. Performing security analysis, problem reporting, tracking and documenting resolutions and performance issues. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Minimum Education: CISA, CEH, Security+, CCNA, MCP, TippingPoint training and similar technologies. Working towards CISSP certification

**8.3.30 IT Health System Security Assurance Analyst 3**

Experience: Security Assurance Analyst 3 possesses at least 5 years of relevant hands-on experience and possesses a security clearance.

Functional Responsibility: Under general direction, performs all procedures necessary to ensure the safety of information systems assets and to protect systems from intentional or inadvertent access or destruction. Performing multiple engineering duties, such as installation, configuration, maintenance and administration of various information assurance systems, to include Firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), and Security Event and Information Management (SEIM) systems. Performing security analysis, problem reporting, tracking and documenting resolutions and performance issues. Monitoring, evaluating, and developing alternative utilization or configuration strategies and conducting, directing, and coordinating responses to cyber attacks, classified material incidents, virus infections and other information assurance and computer network defense activities. Requires understanding of firewall theory and configuration. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Minimum Education: B.A. or B.S. Degree in Computer Science, Engineering, Business or a related field. CISA, CEH, Security+, CCNA, MCP, TippingPoint training and similar technologies. Working towards CISSP certification

**8.3.31 IT Health System Security Assurance Analyst 4**

Experience: Security Assurance Analyst 4 possesses at least 7 years of relevant hands-on experience and possesses a security clearance.

Functional Responsibility: Leads all procedures necessary to ensure the safety of information systems assets and to protect systems from intentional or inadvertent access or destruction. Interfaces with user community to understand their security needs and implements procedures to accommodate them. Ensures that user community understands and adheres to necessary procedures to maintain security. Requires familiarity with domain structures, user authentication, and digital signatures. Conducts evaluation of the level of security required and configuration. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Minimum Education: B.A. or B.S. Degree in Computer Science, Engineering, Business or a related field. Certifications in one or more CISSP, CISA, CEH, Security+, CCNA, MCP, TippingPoint training and similar technologies.
8.3.32 IT Health System Security Assurance Analyst 5

Experience: Security Assurance Analyst 5 possesses at least 9 years of relevant hands-on experience and possesses a security clearance.

Functional Responsibility: Leads all procedures necessary to ensure the safety of information systems assets and to protect systems from intentional or inadvertent access or destruction. Interfaces with user community to understand their security needs and implements procedures to accommodate them. Ensures that user community understands and adheres to necessary procedures to maintain security. Requires familiarity with domain structures, user authentication, and digital signatures. Conducts evaluation of the level of security required and configuration. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Minimum Education: B.A. or B.S. Degree in Computer Science, Engineering, Business or a related field. Certifications in one or more CISSP, CISA, CEH, Security+, CCNA, MCP, TippingPoint training and similar technologies.

8.3.33 IT Health System/Services Consultant 1

Experience: Requires at least 7 years relevant experience for this job category

Functional Responsibility: Performs tasks related to business analysis, architecture definition and review, database design assistance and review, assistance in data migration and integration definition, and application development. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: Minimum B.S. or B.A. degree in related field. Masters and PhD recipients can count post-graduate education years towards overall experience.

8.3.34 IT Health System Database Administrator 1

Experience: At least 3 years of relevant experience.

Functional Responsibility: Performs activities related to database design, implementation and maintenance. Maintains data dictionaries and central data repository. Supports application system development life cycle. Develops policies and procedures relating to database management, security, maintenance and utilization. Is responsible for database backup and recovery procedures, access security and database integrity, physical data storage design and data storage management. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: B.A. or B.S. Degree at Computer Science, Engineering, Business or a related field.

• Five (5) years of direct related experience in a related field may be substituted for a Bachelor’s degree requirement.
8.3.35 IT Health System Database Administrator 2

Experience: At least 7 years of relevant experience.

Functional Responsibility: Performs activities related to database design, implementation and maintenance. Performs logical and physical design of databases. Maintains data dictionaries and central data repository. Supports application system development life cycle. Develops policies and procedures relating to database management, security, maintenance and utilization. Is responsible for database backup and recovery procedures, access security and database integrity, physical data storage design and data storage management. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: B.A. or B.S. Degree in Computer Science, Engineering, Business or a related field.

*Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.3.36 IT Health System Information Assurance 1

Experience: Requires at least 3 years relevant experience for this job category

Functional Responsibility: Performs security and vulnerability testing, analysis, and reporting using various security tools. Reviews and analyzes assessments and vulnerability matrices and provides recommendations for risk mitigation. Develops and maintains security policies and procedures, including system security plans, continuity of operations plans, rules of behavior, and various other security related documentation in accordance with federal regulations and policies. Develops certification and accreditation packages. May need certification in at least one of the following:

- NSA IAM - National Security Agency's INFOSEC Assessment Methodology
- CCISP - Certified Critical Infrastructure Security Professional
- CISM - Certified Information Security Manager
- CISSP - Certified Information Systems Security Professional
- SSCP - Systems Security Certified Practitioner
- GIAC - Global Information Assurance Certification
- CSP - RSA Certified Security Professional
- CPP Certified Protection Professional

All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: Minimum B.S. or B.A. degree in related field.

8.3.37 IT Health System Information Assurance 3

Experience: Requires at least 8 years relevant experience for this job category
Functional Responsibility: Performs security and vulnerability testing, analysis, and reporting using various security tools. Reviews and analyzes assessments and vulnerability matrices and provides recommendations for risk mitigation. Develops and maintains security policies and procedures, including system security plans, continuity of operations plans, rules of behavior, and various other security related documentation in accordance with federal regulations and policies. Develops certification and accreditation packages. May need certification in one or more of the following:

- NSA IAM - National Security Agency's INFOSEC Assessment Methodology
- CCISP - Certified Critical Infrastructure Security Professional
- CISM - Certified Information Security Manager
- CISSP - Certified Information Systems Security Professional
- SSCP - Systems Security Certified Practitioner
- GIAC - Global Information Assurance Certification
- CSP - RSA Certified Security Professional
- CPP - Certified Protection Professional

All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: Minimum B.S. or B.A. degree in related field. Masters and PhD recipients can count past-graduate education years towards overall experience.

8.3.38 IT Health System Network Administrator 1

Experience: This is the entry level position for this job category.

Functional Responsibility: Assists in performing network administration functions for single location Local Area Network. Manages access, passwords, software, addresses, data, records and other network functions. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: Associate's Degree in Computer Science, Engineering or a related field, equivalent technical school or equivalent experience.

8.3.39 IT Health System Network Administrator 2

Experience: At least 2 years of relevant experience.

Functional Responsibility: Performing network administration functions for single location Local Area Network manages access, passwords, software, addresses, data, records and other network functions. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this
category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: Associate's Degree in Computer Science, Engineering or a related field, equivalent technical school or equivalent experience.

8.3.40 IT Health System Network Administrator 3

Experience: At least 4 years of relevant experience.

Functional Responsibility: Performing network administration functions for multiple location Local Area Networks or Wide Area Networks. Manages access, passwords, software, addresses, data, records and other network functions. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: Associate's Degree in Computer Science, Engineering or a related field, equivalent technical school or equivalent experience.

8.3.41 IT Health System Network Architect

Experience: At least 9 years of relevant experience.

Functional Responsibility: Must be able to lead team in developing application, development, network, and technical architectures for mid-range client/server and mainframe applications. Develops and executes architecture strategies and performs feasibility studies and integration analyses. Experience supervising and providing guidance in implementing various architectures. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: BA. or B.S. degree in Computer Science, Engineering or a related field or equivalent experience.

* Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.3.42 IT Health System Network Engineer 1

Experience: Requires at least 2 years relevant experience.

Functional Responsibility: The Network Engineer plans, supports and evaluates complex existing network systems and make recommendations for resources required to maintain and/or expand service levels. This resource will provide highly skilled technical assistance in network planning, engineering and architecture. Plans and incorporates how new network resources and applications will exist on the network. Provide monthly metrics for network availability and bandwidth usage as well as other metrics as requested. Responsible for network capacity planning, user support, and escalation of issues to upper tiers. Use network management tools to discover, map and maintain the network. Responsible for network equipment OS and version upgrades. Maintain Internet and Extranet connectivity; handles day-to-day Firewall administration, as well as VPN connectivity. Monitor and maintain network interfaces to insure its highest level of performance and makes modifications and enhancements as needed. Responsible for documenting procedures and keeping network diagrams and related material up
to date. Handle user problems, questions, and request on network issues. Work with other groups within IS to resolve network related issues as needed. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: B.S. or B.A. degree in Computer Science, Engineering or related fields (or equivalent experience).

8.3.43 IT Health Services Program Manager

Experience: Must have 10 years of IT experience, including at least 7 years of IT and/or telecommunications system management experience.

Functional Responsibility: Performs day-to-day management of delivery order projects for ERP technology projects that involve teams of data processing and other information systems management professionals who have previously been involved in analyzing, designing, integrating, testing, documenting, convening, extending, and implementing automated information and telecommunications systems. Demonstrates proven skills in those technical areas addressed by the delivery order to be managed. organizes, directs, and coordinates the planning and production of all activities associated with assigned deliverables. Establishes and alters, as necessary, corporate management structure to direct effective contract support activities. Demonstrates good written and oral communications. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: B.A. or B.S. degree. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.3.44 IT Health Systems Programmer 1

Experience: This is the entry level position for this job category.

Functional Responsibility: Under close supervision support the design, code, development, test and document application programs. Support modification to existing programs and procedures. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: B.A. or B.S. degree in Computer Science, Engineering or a related field or an equivalent degree. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.3.45 IT Health Systems Programmer 3

Experience: At least 4 years of relevant experience.

Functional Responsibility: Support the design, code, development, test and document application programs. Support modification to existing programs and procedures. Support creation of procedural forms and documentation, including flow charts and system documentation. Provide assistance to lower level individuals within the same job category. All
category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: B.A. or B.S. degree in Computer Science, Engineering or a related field or an equivalent degree. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.3.46 IT Health Systems Programmer 5

Experience: At least 7 years of relevant experience.

Functional Responsibility: Leads the design, coding, development, testing and documentation of application programs. Lead the modifications to, and maintenance of, existing programs and procedures. Specify creation of procedural forms and documentation, including flow charts and system documentation. Lead associated task team efforts. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: B.A. or B.S. degree in Computer Science, Engineering or a related field or an equivalent degree. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.3.47 IT Health Services Subject Matter Expert 1

Experience: At least 8 years of IT experience and at least 5 years directly related to the required area of expertise.

Functional Responsibility: Develops requirements from a project's inception to its conclusion in the subject matter area for s moderately complex systems. Assists other senior consultants with analysis and evaluation and with the preparation of recommendations for system improvements, optimization, development, and/or maintenance efforts in the following specialties: information systems architecture; networking; telecommunications; automation; risk management; software; life-cycle management; software development methodologies; modeling and simulation. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: B.A. or B.S. degree. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.3.48 IT Health Systems Administrator 1

Experience: This is the entry level position for this job category.

Functional Responsibility: Assists with the installation, maintenance and usage of a system under supervision. Installs software and troubleshoots user and system problems. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.
Education: Associate's Degree in Computer Science, Engineering or a related field.

8.3.49 IT Health Systems Administrator 3

Experience: At least 5 years of relevant experience.

Functional Responsibility: Responsible for the installation, maintenance and usage of a system under supervision. Install software and troubleshoot user and system problems. Maintain system security. Implement policies, procedures and standards. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: B.A. or B.S. degree in Computer Science, Engineering or a related field or equivalent experience. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.3.50 IT Health Services Systems Analyst 1

Experience: This is the entry level position for this job category.

Functional Responsibility: Under close supervision gathers facts, analyses data, compares alternatives in terms of cost, time and availability of equipment/personnel. Supports determination and resolution of data processing problems and coordinates work. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: B.A. or B.S. degree in Computer Science, Engineering, Business or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.3.51 IT Health Services Systems Analyst 3

Experience: At least 5 years of relevant experience.

Functional Responsibility: Applies systems analysis and design techniques to complex computer systems in a broad area. Competent in all phases of systems analysis techniques, concepts and methods. Has knowledge of available system software, computer equipment, regulations, practices, etc. in a subject matter area Recognizes probable conflicts and integrating diverse data sources. Maintains and modifies complex systems or develops new subsystems. Recommends optimum approach and develops system design. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: B.A. or B.S. degree in Computer Science, Engineering, Business or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.
8.3.52 IT Health Services Systems Analyst 4

Experience: At least 7 years of relevant experience.

Functional Responsibility: Applies expert systems analysis and design techniques to complex computer systems in an area. Has broad knowledge of data sources/flaw, interactions of complex systems, and capabilities/limitations of systems software and computer equipment. Establishes framework of new computer systems from feasibility studies to past implementation evaluation. Recognizes probable conflicts and integrating diverse data sources. Produces innovative solutions for a variety of complex problems. Prepares overall project recommendations. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: B.A. or B.S. degree in Computer Science, Engineering, Business or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.3.53 IT Health Services Systems Engineer 1

Experience: At least 2 years of relevant experience.

Functional Responsibility: Provides technical support in system architecture, system design, system integration and technical management. Assists in providing technical input to the systems engineering process. Assists in developing and implementing installation plans. Assists in preparation and presentation of systems assurance reviews. Identifies requirements and deficiencies in hardware and software products. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: B.A. or B.S. degree in Computer Science, Engineering or a related field or equivalent experience. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.3.54 IT Health Services Systems Engineer 3

Experience: At least 7 years of relevant experience.

Functional Responsibility: Provides technical support in system architecture, system design, system integration and technical management. Assists in providing technical input to the systems engineering process. Leads teams in developing application and technical plans. Guide customers in the installation and use of strategic products through education and guidance, first-rise and tuning assistance problem solving and critical situation resolution. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: B.A. or B.S. degree in Computer Science, Engineering or a related field or equivalent experience. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.
8.3.55 IT Health Services Systems Engineer 4

Experience: At least 8 years of relevant experience.

Functional Responsibility: Provides technical leadership in system architecture, system design, system integration and technical management. Assists in providing technical input to the systems engineering process. Leads teams in developing application and technical plans. Guide customers in the installation and use of strategic products through education and guidance, first-use and tuning assistance problem solving and critical situation resolution. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: B.A. or B.S. degree in Computer Science, Engineering or a related field or equivalent experience. Five (5) years of direct related experience ma related field may be substituted for a Bachelor's degree requirement.

8.3.56 IT Health Services Test Engineer 2

Experience: Requires at least 7 years relevant experience for this job category

Functional Responsibility: Design review, test plan creation, test case implementation, defect report creation and Packing, and documentation review. Work with other testing team members to accomplish specific product testing tasks. Review product requirements, Develop, maintain, and execute test cases. Create and maintain datasets. Create and execute automation scripts. Isolate defects and enter software defect reports. Continual review and improvement of testing process and implementation. Analyze and report progress to Test Manager. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: B.S. or B.A. degree in related field (or equivalent experience).

8.3.57 IT Health Services Testing Specialist

Experience: At least 2 years or software testing experience (integration and acceptance).

Functional Responsibility: Must be capable of designing and executing ADP software tests and evaluating results to ensure compliance with applicable regulations. Must be able to prepare test scripts and all required test documentation. Must be able to design and prepare all needed test data. Analyze internal security within systems. Reviews test results and evaluates for conformance to design. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: B.A. or B.S. degree or 3 years of equivalent experience in a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

8.3.58 IT Health Systems Training Specialist 2

Experience: Requires at least 7 years relevant experience for this job category
Functional Responsibility: Analyze training needs to develop new Information Technology training programs or modify and improve existing programs. Conduct or arrange for ongoing technical training and personal development classes for staff members. Conduct orientation sessions and arrange on-the-job training. Conduct surveys to identify training needs based on projected production processes, changes, and other factors. Develop and organize training manuals, multimedia visual aids, and other educational materials. Develop testing and evaluation procedures. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: Minimum B.S. or B.A. degree in related field (or equivalent experience).

8.3.59 IT Health Systems Cyber Analyst 1

Experience: Requires at least 3 years relevant experience in a Cyber Security role.

Functional Responsibility: Under supervision provides day-to-day support to cyber security operations. Gathers data and perform technical and operational analysis of cyber security operations, reporting, and management. Supports presentations and facilitates discussion of security operations with senior management. Draft communications, reports, and analysis documentation. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: Minimum B.S. or B.A. degree in related field.

8.3.60 IT Health Systems Cyber Analyst 2

Experience: Requires at least 5 years relevant experience in a Cyber Security role.

Functional Responsibility: Provides day-to-day support to cyber security operations. Gathers and interprets data and perform technical and operational analysis of cyber security operations, reporting, and management. Develops presentations and facilitates discussion of security operations with senior management. Draft communications, reports, and analysis documentation. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: Minimum B.S. or B.A. degree in related field.

8.3.61 IT Health Systems Cyber Analyst 3

Experience: Requires at least 8 years relevant experience in a Cyber Security role.

Functional Responsibility: Provides leadership in the day-to-day support to cyber security operations. Reviews and interprets data and perform technical and operational analysis of cyber security operations, reporting, and management. Leads presentations and facilitates discussion of security operations with senior management. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services.
Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: Minimum B.S. or B.A. degree in related field.

8.3.62 IT Health Systems Cyber Engineer 1

Experience: Requires at least 3 years relevant experience in a Cyber Security role.

Functional Responsibility: Under supervision provides support to cyber security operations, policy and threat mitigation. Perform duties utilizing cyber security tools, network topologies, intrusion detection, and secured networks. Support interpretation and implementation of cyber security regulations. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: Minimum B.S. or B.A. degree in related field.

8.3.63 IT Health Systems Cyber Engineer 2

Experience: Requires at least 5 years relevant experience in a Cyber Security role.

Functional Responsibility: Provides support to cyber security operations, policy and threat mitigation. Perform duties utilizing cyber security tools, network topologies, intrusion detection, and secured networks. Integrates metrics into the security posture of the organization, identifies areas of weakness and vulnerability and recommends changes to meet security standards. Interpret, implements and monitors compliance to cyber security regulations. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: Minimum B.S. or B.A. degree in related field.

8.3.64 IT Health Systems Cyber Engineer 3

Experience: Requires at least 8 years relevant experience in a Cyber Security role.

Functional Responsibility: Provides leadership to cyber security operations, policy and threat mitigation. Oversees cyber security tools, network topologies, intrusion detection, and secured networks. Reviews applicability of metrics used for assessment of security posture of the organization, acts on areas of weakness and vulnerability and leads implementation of changes to meet security standards. Provide technical direction and guidance to other Cyber Security Engineers, Information Technology and the organization to align with regulatory and security requirements. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: Minimum B.S. or B.A. degree in related field.

8.3.65 IT Health Systems Security Engineer 1

Experience: Requires at least 3 years relevant experience in a security role.
Functional Responsibility: Under supervision supports the design and implementation of solutions for intrusion detection and notification, security auditing, alerting, and response, virus detection and removal, password complexity enforcement, and media protection. Support the status of system security patch deployments. Support the update of Standard Operating Procedures for the implemented security controls, prepares and conducts staff security awareness training, and develops budget and schedule plans for security-related activities. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: Minimum B.S. or B.A. degree in related field.

8.3.66  IT Health Systems Security Engineer 2

Experience: Requires at least 5 years relevant experience in a security role.

Functional Responsibility: Designs and implements solutions for intrusion detection and notification, security auditing, alerting, and response, virus detection and removal, password complexity enforcement, and media protection. Maintain status of system security patch deployments. Develops and updates Standard Operating Procedures for the implemented security controls, prepares and conducts staff security awareness training, and develops budget and schedule plans for security-related activities. We expect the candidate to be a working manager, both leading development activities and performing recurring security-related activities to ensure implementation, sustainment, and effectiveness of implemented security controls. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: Minimum B.S. or B.A. degree in related field.

8.3.67  IT Health Systems Security Engineer 3

Experience: Requires at least 8 years relevant experience in a security role.

Functional Responsibility: Provides leadership in the design and implementation of solutions for intrusion detection and notification, security auditing, alerting, and response, virus detection and removal, password complexity enforcement, and media protection. Review status of system security patch deployments. Review Standard Operating Procedures for the implemented security controls, prepares and conducts staff security awareness training, and evaluates budget and schedule plans for security-related activities. Serve as a working manager, both leading development activities and performing recurring security-related activities to ensure implementation, sustainment, and effectiveness of implemented security controls. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: Minimum B.S. or B.A. degree in related field.
8.3.68 IT Health Systems Data Warehouse Analyst 1
Experience: Requires at least 3 years relevant experience in data warehouse and data mart applications.

Functional Responsibility: Under supervision support the development, maintenance and management of the data warehouse, including the logical and physical design, database management, acquisition of data, and overall implementation. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: Minimum B.S. or B.A. degree in IT or other related discipline.

8.3.69 IT Health Systems Data Warehouse Engineer 1
Experience: Requires at least 3 years relevant experience in IT or related role.

Functional Responsibility: Under supervision support the design, development and maintain data integration services, data visualization, and APIs and tools that deliver data warehouse and big data services to the Practice Fusion team and external partners. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: Minimum B.S. or B.A. degree in IT or other related discipline.

8.3.70 IT Health Systems Program & Policy Analyst 1
Experience: Requires at least 3 years relevant experience. Knowledge and understanding of public law, Executive Orders, Presidential Directives and Federal regulations governing programs and policies.

Functional Responsibility: Proactively support and identify changes needed in programs and policy and to align and support strategic shifts in business strategy. Assist to ensure formal business policy issuances are complete, current, and operationally relevant. Provide input into the revision and/or development of programs and policies to comply with emerging national requirements. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: Minimum B.S. or B.A. degree in IT or other related discipline.

8.3.71 IT Health Systems Program & Policy Analyst 3
Experience: Requires at least 8 years relevant experience. Knowledge and understanding of public law, Executive Orders, Presidential Directives and Federal regulations governing programs and policies.

Functional Responsibility: Provide leadership to proactively identify changes needed in programs and policy and to align and support strategic shifts in business strategy. Ensure formal business policy issuances are complete, current, and operationally relevant. Lead the revision
and/or development of programs and policies to comply with emerging national requirements. Monitor on a continuing basis proposed and newly promulgated Federal legislation, Office of Management and Budget guidance, and other national level policy affecting programs and policies need to perform analysis and identify policy gaps. Identify program and policy changes necessary to improve acquisition and integrate these policies and procedures into the acquisition process. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: Minimum B.S. or B.A. degree in IT or other related discipline.

8.3.72 IT Health Systems Certification and Accreditation Analyst 1

Experience: Requires at least 3 years relevant experience. Knowledge and understanding of public law, Executive Orders, Presidential Directives and Federal regulations governing programs and policies.

Functional Responsibility: Provide support to all activities needed to obtain certification and accreditation on all the networks, equipment and systems at all classification levels under the purview of the Office of the Administrative Assistant (OAA) Designated Approving Authority (DAA). All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: Minimum B.S. or B.A. degree in IT or other related discipline.

8.3.73 IT Health Systems Certification and Accreditation Analyst 3

Experience: Requires at least 8 years relevant experience. Knowledge and understanding of public law, Executive Orders, Presidential Directives and Federal regulations governing programs and policies.

Functional Responsibility: Provide leadership to all activities needed to obtain certification and accreditation on all the networks, equipment and systems at all classification levels under the purview of the Office of the Administrative Assistant (OAA) Designated Approving Authority (DAA). Administer the Connection Approval Program and Tenant Security Process in accordance with Army, DoD, Joint, Intelligence Community regulation or policy. Provide technical support to DoD information system programs for life cycle security support, from inception of the program through initial accreditation. Develop a methodology and procedures to be followed by accreditation personnel while providing life cycle security support. Participate in formal and ad hoc certification and accreditation working groups where directed. Provide technical documentation required for the site certification and accreditation process. Monitor the implementation of and compliance with, DIACAP C&A standards to ensure uniform application of the standards and consistency in security of accredited DoD information systems. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: Minimum B.S. or B.A. degree in IT or other related discipline.
8.3.74 IT Health Systems Facility Engineer 1

Experience: Requires at least 3 years relevant experience.

Functional Responsibility: Support the programming and coordinating the inspection and the repairs. Take part in the testing and calibration of electrical and mechanical systems. Provide support to demonstrating, building and enforcing the best exercises for all projects and functions within the facility. All category performance is specific to Electronic Health Records, Health Analytics, Personal Health Information Management, Innovative Health IT Solutions, Health Informatics, Emerging Health IT Research and Other Health IT services. Performance of this category may be subject to: HITECH, HIPAA, NIST, FIPS and Special Publications FISMA of 2002.

Education: Minimum B.S. or B.A. degree in a related field or an additional 4 years related experience.
9.0 Labor Category Pricing

9.1 Highly Adaptive Cybersecurity Services (HACS) (SIN 54151HACS)

<table>
<thead>
<tr>
<th>GSA Labor Category</th>
<th>GSA Hourly Rate (including IFF)</th>
<th>SEPTEMBER 13, 2019 thru SEPTEMBER 12, 2020</th>
<th>SEPTEMBER 13, 2020 thru SEPTEMBER 12, 2021</th>
<th>SEPTEMBER 13, 2021 thru SEPTEMBER 12, 2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Manager</td>
<td>$163.21 $177.90</td>
<td>$166.47 $181.46</td>
<td>$169.80 $185.09</td>
<td></td>
</tr>
<tr>
<td>Project Manager I</td>
<td>$137.03 $137.03</td>
<td>$139.77 $139.77</td>
<td>$142.57 $142.57</td>
<td></td>
</tr>
<tr>
<td>Project Manager II</td>
<td>$149.12 $149.12</td>
<td>$152.10 $152.10</td>
<td>$155.14 $155.14</td>
<td></td>
</tr>
<tr>
<td>Program &amp; Policy Analyst I</td>
<td>$89.02 $97.03</td>
<td>$90.80 $98.97</td>
<td>$92.62 $100.95</td>
<td></td>
</tr>
<tr>
<td>Program &amp; Policy Analyst II</td>
<td>$103.36 $112.04</td>
<td>$105.43 $114.28</td>
<td>$107.54 $116.57</td>
<td>$104.57 $112.60</td>
</tr>
<tr>
<td>Program &amp; Policy Analyst III</td>
<td>$119.49 $130.24</td>
<td>$121.88 $132.84</td>
<td>$124.32 $135.50</td>
<td></td>
</tr>
<tr>
<td>Cyber Security Consultant</td>
<td>$275.65 $300.46</td>
<td>$281.16 $306.47</td>
<td>$286.78 $312.60</td>
<td></td>
</tr>
<tr>
<td>Cyber Security Architect</td>
<td>$275.65 $300.46</td>
<td>$281.16 $306.47</td>
<td>$286.78 $312.60</td>
<td></td>
</tr>
<tr>
<td>Cyber Security Engineer I</td>
<td>$94.96 $103.51</td>
<td>$96.86 $105.58</td>
<td>$98.80 $107.69</td>
<td></td>
</tr>
<tr>
<td>Cyber Security Engineer II</td>
<td>$111.28 $121.30</td>
<td>$113.51 $123.73</td>
<td>$115.78 $126.20</td>
<td></td>
</tr>
<tr>
<td>Cyber Security Engineer III</td>
<td>$128.59 $140.16</td>
<td>$131.16 $142.96</td>
<td>$133.78 $145.82</td>
<td></td>
</tr>
<tr>
<td>Cyber Security Analyst I</td>
<td>$89.02 $97.03</td>
<td>$90.80 $98.97</td>
<td>$92.62 $100.95</td>
<td></td>
</tr>
<tr>
<td>Cyber Security Analyst II</td>
<td>$103.36 $112.04</td>
<td>$105.43 $114.28</td>
<td>$107.54 $116.57</td>
<td></td>
</tr>
<tr>
<td>Cyber Security Analyst III</td>
<td>$119.49 $130.24</td>
<td>$121.88 $132.84</td>
<td>$124.32 $135.50</td>
<td></td>
</tr>
<tr>
<td>Cyber Security Specialist I</td>
<td>$99.98 $109.87</td>
<td>$101.98 $112.07</td>
<td>$104.02 $114.31</td>
<td></td>
</tr>
<tr>
<td>Cyber Security Specialist II</td>
<td>$111.96 $122.04</td>
<td>$114.20 $124.48</td>
<td>$116.48 $126.97</td>
<td></td>
</tr>
<tr>
<td>Cyber Security Specialist III</td>
<td>$125.11 $137.48</td>
<td>$127.61 $140.23</td>
<td>$130.16 $143.03</td>
<td></td>
</tr>
<tr>
<td>Cyber Hunting and Threat Intelligence Manager / Lead</td>
<td>$191.58 $208.81</td>
<td>$195.41 $212.99</td>
<td>$199.32 $217.25</td>
<td></td>
</tr>
<tr>
<td>Cyber Hunting and Threat Intelligence Analyst I</td>
<td>$83.39 $90.90</td>
<td>$85.06 $92.72</td>
<td>$86.76 $94.57</td>
<td></td>
</tr>
<tr>
<td>Cyber Hunting and Threat Intelligence Analyst II</td>
<td>$101.77 $110.94</td>
<td>$103.81 $113.16</td>
<td>$105.89 $115.42</td>
<td></td>
</tr>
<tr>
<td>Cyber Hunting and Threat Intelligence Analyst III</td>
<td>$129.72 $141.39</td>
<td>$132.31 $144.22</td>
<td>$134.96 $147.10</td>
<td></td>
</tr>
<tr>
<td>Cyber Hunting and Threat Intelligence Analyst IV</td>
<td>$158.39 $172.65</td>
<td>$161.56 $176.10</td>
<td>$164.79 $179.62</td>
<td></td>
</tr>
<tr>
<td>Penetration Testing Manager / Lead</td>
<td>$159.67 $174.04</td>
<td>$162.86 $177.52</td>
<td>$166.12 $181.07</td>
<td></td>
</tr>
<tr>
<td>Penetration Tester I</td>
<td>$98.72 $107.61</td>
<td>$100.69 $109.76</td>
<td>$102.70 $111.96</td>
<td></td>
</tr>
<tr>
<td>Penetration Tester II</td>
<td>$116.30 $127.81</td>
<td>$118.63 $130.37</td>
<td>$121.00 $132.98</td>
<td></td>
</tr>
<tr>
<td>Penetration Tester III</td>
<td>$136.77 $149.09</td>
<td>$139.51 $152.07</td>
<td>$142.30 $155.11</td>
<td></td>
</tr>
<tr>
<td>Penetration Tester IV</td>
<td>$148.01 $162.65</td>
<td>$150.97 $165.90</td>
<td>$153.99 $169.22</td>
<td></td>
</tr>
<tr>
<td>Incident Detection/Response Analyst I</td>
<td>$99.55 $109.40</td>
<td>$101.54 $111.59</td>
<td>$103.57 $113.82</td>
<td></td>
</tr>
<tr>
<td>Incident Detection/Response Analyst II</td>
<td>$134.19 $146.27</td>
<td>$136.87 $149.20</td>
<td>$139.61 $152.18</td>
<td></td>
</tr>
<tr>
<td>Incident Detection/Response Analyst III</td>
<td>$150.73 $165.63</td>
<td>$153.74 $168.94</td>
<td>$156.81 $172.32</td>
<td></td>
</tr>
<tr>
<td>Risk and Vulnerability Assessment Analyst I</td>
<td>$99.55 $109.40</td>
<td>$101.54 $111.59</td>
<td>$103.57 $113.82</td>
<td></td>
</tr>
<tr>
<td>Risk and Vulnerability Assessment Analyst II</td>
<td>$134.19 $146.27</td>
<td>$136.87 $149.20</td>
<td>$139.61 $152.18</td>
<td></td>
</tr>
<tr>
<td>Risk and Vulnerability Assessment Analyst III</td>
<td>$150.73 $165.63</td>
<td>$153.74 $168.94</td>
<td>$156.81 $172.32</td>
<td></td>
</tr>
<tr>
<td>Documentation Specialist I</td>
<td>$80.06 $87.26</td>
<td>$81.66 $89.01</td>
<td>$83.29 $90.79</td>
<td></td>
</tr>
<tr>
<td>Documentation Specialist II</td>
<td>$96.58 $105.27</td>
<td>$98.51 $107.38</td>
<td>$100.48 $109.53</td>
<td></td>
</tr>
<tr>
<td>Cyber Security SME</td>
<td>$168.34 $183.49</td>
<td>$171.71 $187.16</td>
<td>$175.14 $190.90</td>
<td></td>
</tr>
</tbody>
</table>
### 9.2 Information Technology Professional Services (SIN 54151S)

<table>
<thead>
<tr>
<th>GSA Labor Category Title</th>
<th>GSA Hourly Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Administration Specialist I</td>
<td>$53.19</td>
</tr>
<tr>
<td>Project Controls II</td>
<td>$116.88</td>
</tr>
<tr>
<td>Project Manager I</td>
<td>$137.03</td>
</tr>
<tr>
<td>Project Manager II</td>
<td>$149.12</td>
</tr>
<tr>
<td>Quality Assurance Manager</td>
<td>$112.20</td>
</tr>
<tr>
<td>Systems Architect</td>
<td>$141.20</td>
</tr>
<tr>
<td>Systems Programmer II</td>
<td>$124.46</td>
</tr>
<tr>
<td>Test Engineer I</td>
<td>$76.83</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GSA Labor Category Title</th>
<th>GSA Hourly Rate Customer Site</th>
<th>GSA Hourly Rate Xator Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Security Analyst 1</td>
<td>$74.56</td>
<td>$81.27</td>
</tr>
<tr>
<td>Data Security Analyst 2</td>
<td>$88.11</td>
<td>$96.04</td>
</tr>
<tr>
<td>Data Security Analyst 3</td>
<td>$105.45</td>
<td>$114.93</td>
</tr>
<tr>
<td>Data Security Analyst 4</td>
<td>$130.01</td>
<td>$141.69</td>
</tr>
<tr>
<td>Data Security Analyst 5</td>
<td>$145.18</td>
<td>$158.24</td>
</tr>
<tr>
<td>Threat Analyst 1</td>
<td>$83.39</td>
<td>$90.90</td>
</tr>
<tr>
<td>Threat Analyst 2</td>
<td>$101.77</td>
<td>$110.94</td>
</tr>
<tr>
<td>Threat Analyst 3</td>
<td>$129.72</td>
<td>$141.39</td>
</tr>
<tr>
<td>Threat Analyst 4</td>
<td>$158.39</td>
<td>$172.65</td>
</tr>
<tr>
<td>Threat Analyst 5</td>
<td>$191.58</td>
<td>$208.81</td>
</tr>
<tr>
<td>Forensics Analyst 1</td>
<td>$98.72</td>
<td>$107.61</td>
</tr>
<tr>
<td>Forensics Analyst 2</td>
<td>$116.30</td>
<td>$127.81</td>
</tr>
<tr>
<td>Forensics Analyst 3</td>
<td>$136.77</td>
<td>$149.09</td>
</tr>
<tr>
<td>Forensics Analyst 4</td>
<td>$148.01</td>
<td>$162.65</td>
</tr>
<tr>
<td>Forensics Analyst 5</td>
<td>$159.67</td>
<td>$174.04</td>
</tr>
<tr>
<td>Security Assurance Analyst 1</td>
<td>$82.97</td>
<td>$90.43</td>
</tr>
<tr>
<td>Security Assurance Analyst 2</td>
<td>$99.98</td>
<td>$109.87</td>
</tr>
<tr>
<td>Security Assurance Analyst 3</td>
<td>$111.96</td>
<td>$122.04</td>
</tr>
<tr>
<td>Security Assurance Analyst 4</td>
<td>$125.11</td>
<td>$137.48</td>
</tr>
<tr>
<td>Security Assurance Analyst 5</td>
<td>$142.52</td>
<td>$155.35</td>
</tr>
<tr>
<td>Quality Assurance Specialist (Journeyman)</td>
<td>$106.79</td>
<td>$116.40</td>
</tr>
<tr>
<td>Business System Analyst</td>
<td>$104.55</td>
<td>$113.97</td>
</tr>
<tr>
<td>Technical Writer 2</td>
<td>$80.06</td>
<td>$87.26</td>
</tr>
<tr>
<td>Applications Developer (Journeyman)</td>
<td>$92.70</td>
<td>$101.05</td>
</tr>
<tr>
<td>Applications Developer (Senior)</td>
<td>$114.66</td>
<td>$124.98</td>
</tr>
<tr>
<td>Database Specialist (Senior)</td>
<td>$82.83</td>
<td>$90.29</td>
</tr>
<tr>
<td>Systems Engineer</td>
<td>$90.03</td>
<td>$98.13</td>
</tr>
<tr>
<td>Administrative Assistant 2</td>
<td>$54.40</td>
<td>$59.30</td>
</tr>
<tr>
<td>Business Analyst I</td>
<td>$111.28</td>
<td>$121.30</td>
</tr>
<tr>
<td>Business Analyst II</td>
<td>$127.40</td>
<td>$138.87</td>
</tr>
<tr>
<td>GSA Labor Category Title</td>
<td>GSA Hourly Rate Customer Site</td>
<td>GSA Hourly Rate Xator Site</td>
</tr>
<tr>
<td>-------------------------------------------------------------</td>
<td>------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Business Process Analyst 1</td>
<td>$103.86</td>
<td>$113.21</td>
</tr>
<tr>
<td>Business Process Analyst 2</td>
<td>$118.70</td>
<td>$129.38</td>
</tr>
<tr>
<td>Business Process Engineer 1</td>
<td>$108.80</td>
<td>$118.59</td>
</tr>
<tr>
<td>Business Process Engineer 2</td>
<td>$126.11</td>
<td>$137.46</td>
</tr>
<tr>
<td>Certification and Accreditation Analyst 1</td>
<td>$96.93</td>
<td>$105.65</td>
</tr>
<tr>
<td>Certification and Accreditation Analyst 3</td>
<td>$124.63</td>
<td>$135.85</td>
</tr>
<tr>
<td>Consultant 1</td>
<td>$263.85</td>
<td>$287.59</td>
</tr>
<tr>
<td>Contracts Administrator 2</td>
<td>$84.08</td>
<td>$91.65</td>
</tr>
<tr>
<td>Cyber Analyst 1</td>
<td>$79.63</td>
<td>$86.80</td>
</tr>
<tr>
<td>Cyber Analyst 2</td>
<td>$91.99</td>
<td>$100.27</td>
</tr>
<tr>
<td>Cyber Analyst 3</td>
<td>$109.79</td>
<td>$119.67</td>
</tr>
<tr>
<td>Cyber Engineer 1</td>
<td>$94.96</td>
<td>$103.51</td>
</tr>
<tr>
<td>Cyber Engineer 2</td>
<td>$111.28</td>
<td>$121.30</td>
</tr>
<tr>
<td>Cyber Engineer 3</td>
<td>$128.59</td>
<td>$140.16</td>
</tr>
<tr>
<td>Data Warehouse Analyst 1</td>
<td>$90.01</td>
<td>$98.11</td>
</tr>
<tr>
<td>Data Warehouse Engineer 1</td>
<td>$92.98</td>
<td>$101.35</td>
</tr>
<tr>
<td>Database Administrator 1</td>
<td>$93.97</td>
<td>$102.43</td>
</tr>
<tr>
<td>Database Administrator 2</td>
<td>$118.70</td>
<td>$129.38</td>
</tr>
<tr>
<td>Disaster Recovery/COOP/Contingency</td>
<td>$103.86</td>
<td>$113.21</td>
</tr>
<tr>
<td>Facility Engineer 1</td>
<td>$55.89</td>
<td>$60.92</td>
</tr>
<tr>
<td>Financial Analyst 1</td>
<td>$74.58</td>
<td>$81.29</td>
</tr>
<tr>
<td>Financial Analyst 3</td>
<td>$114.64</td>
<td>$124.96</td>
</tr>
<tr>
<td>Information Assurance 1</td>
<td>$98.91</td>
<td>$107.81</td>
</tr>
<tr>
<td>Information Assurance 3</td>
<td>$123.64</td>
<td>$134.77</td>
</tr>
<tr>
<td>Network Administrator 1</td>
<td>$64.29</td>
<td>$70.08</td>
</tr>
<tr>
<td>Network Administrator 2</td>
<td>$77.15</td>
<td>$84.09</td>
</tr>
<tr>
<td>Network Administrator 3</td>
<td>$94.96</td>
<td>$103.51</td>
</tr>
<tr>
<td>Network Architect</td>
<td>$155.79</td>
<td>$169.81</td>
</tr>
<tr>
<td>Network Engineer 1</td>
<td>$73.69</td>
<td>$80.32</td>
</tr>
<tr>
<td>Program &amp; Policy Analyst 1</td>
<td>$89.02</td>
<td>$97.03</td>
</tr>
<tr>
<td>Program &amp; Policy Analyst 3</td>
<td>$119.49</td>
<td>$130.24</td>
</tr>
<tr>
<td>Program Manager</td>
<td>$163.21</td>
<td>$177.90</td>
</tr>
<tr>
<td>Programmer 1</td>
<td>$65.28</td>
<td>$71.16</td>
</tr>
<tr>
<td>Programmer 3</td>
<td>$89.02</td>
<td>$97.03</td>
</tr>
<tr>
<td>Programmer 5</td>
<td>$128.59</td>
<td>$140.16</td>
</tr>
<tr>
<td>Security Engineer 1</td>
<td>$84.08</td>
<td>$91.65</td>
</tr>
<tr>
<td>Security Engineer 2</td>
<td>$113.75</td>
<td>$123.99</td>
</tr>
<tr>
<td>Security Engineer 3</td>
<td>$136.50</td>
<td>$148.79</td>
</tr>
<tr>
<td>Subject Matter Expert 1</td>
<td>$168.34</td>
<td>$183.49</td>
</tr>
<tr>
<td>Systems Administrator 1</td>
<td>$80.30</td>
<td>$87.53</td>
</tr>
<tr>
<td>Systems Administrator 3</td>
<td>$114.74</td>
<td>$125.07</td>
</tr>
<tr>
<td>GSA Labor Category Title</td>
<td>GSA Hourly Rate Customer Site</td>
<td>GSA Hourly Rate Xator Site</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Systems Analyst 1</td>
<td>$64.29</td>
<td>$70.08</td>
</tr>
<tr>
<td>Systems Analyst 3</td>
<td>$94.12</td>
<td>$102.59</td>
</tr>
<tr>
<td>Systems Analyst 4</td>
<td>$113.45</td>
<td>$123.66</td>
</tr>
<tr>
<td>Systems Engineer 1</td>
<td>$64.48</td>
<td>$70.28</td>
</tr>
<tr>
<td>Systems Engineer 3</td>
<td>$118.87</td>
<td>$129.57</td>
</tr>
<tr>
<td>Systems Engineer 4</td>
<td>$139.31</td>
<td>$151.85</td>
</tr>
<tr>
<td>Technical Writer 3</td>
<td>$96.58</td>
<td>$105.27</td>
</tr>
<tr>
<td>Test Engineer 2</td>
<td>$108.98</td>
<td>$118.79</td>
</tr>
<tr>
<td>Testing Specialist</td>
<td>$80.30</td>
<td>$87.53</td>
</tr>
<tr>
<td>Training Specialist 2</td>
<td>$84.08</td>
<td>$91.65</td>
</tr>
</tbody>
</table>

### 9.3 Health Information Technology Services (SIN 54151HEAL)

<table>
<thead>
<tr>
<th>GSA Labor Category Title</th>
<th>GSA Hourly Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Health Services Project Controls II</td>
<td>$116.88</td>
</tr>
<tr>
<td>IT Health Services Project Manager I</td>
<td>$137.03</td>
</tr>
<tr>
<td>IT Health Services Project Manager II</td>
<td>$149.12</td>
</tr>
<tr>
<td>IT Health Services Quality Assurance Manager</td>
<td>$112.20</td>
</tr>
<tr>
<td>IT Health Systems Architect</td>
<td>$141.20</td>
</tr>
<tr>
<td>IT Health Systems Programmer II</td>
<td>$124.46</td>
</tr>
<tr>
<td>IT Health Services Test Engineer I</td>
<td>$76.83</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GSA Labor Category Title</th>
<th>GSA Hourly Rate Customer Site</th>
<th>GSA Hourly Rate Xator Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Health Database Specialist (Senior)</td>
<td>$82.83</td>
<td>$90.29</td>
</tr>
<tr>
<td>IT Health Systems Engineer</td>
<td>$90.03</td>
<td>$98.13</td>
</tr>
<tr>
<td>IT Health Applications Developer (Journeyman)</td>
<td>$92.70</td>
<td>$101.05</td>
</tr>
<tr>
<td>IT Health Applications Developer (Senior)</td>
<td>$114.66</td>
<td>$124.98</td>
</tr>
<tr>
<td>IT Health Services Quality Assurance Specialist (Journeyman)</td>
<td>$106.79</td>
<td>$116.40</td>
</tr>
<tr>
<td>IT Health Data Security Analyst 1</td>
<td>$74.56</td>
<td>$81.27</td>
</tr>
<tr>
<td>IT Health Data Security Analyst 2</td>
<td>$88.11</td>
<td>$96.04</td>
</tr>
<tr>
<td>IT Health Data Security Analyst 3</td>
<td>$105.45</td>
<td>$114.93</td>
</tr>
<tr>
<td>IT Health Data Security Analyst 4</td>
<td>$130.01</td>
<td>$141.69</td>
</tr>
<tr>
<td>IT Health Data Security Analyst 5</td>
<td>$145.18</td>
<td>$158.24</td>
</tr>
<tr>
<td>IT Health Services Threat Analyst 1</td>
<td>$83.39</td>
<td>$90.90</td>
</tr>
<tr>
<td>IT Health Services Threat Analyst 2</td>
<td>$101.77</td>
<td>$110.94</td>
</tr>
<tr>
<td>IT Health Services Threat Analyst 3</td>
<td>$129.72</td>
<td>$141.39</td>
</tr>
<tr>
<td>IT Health Services Threat Analyst 4</td>
<td>$158.39</td>
<td>$172.65</td>
</tr>
<tr>
<td>IT Health Services Threat Analyst 5</td>
<td>$191.58</td>
<td>$208.81</td>
</tr>
<tr>
<td>IT Health System Forensics Analyst 1</td>
<td>$98.72</td>
<td>$107.61</td>
</tr>
<tr>
<td>GSA Labor Category Title</td>
<td>GSA Hourly Rate Customer Site</td>
<td>GSA Hourly Rate Xator Site</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>IT Health System Forensics Analyst 2</td>
<td>$116.30</td>
<td>$127.81</td>
</tr>
<tr>
<td>IT Health System Forensics Analyst 3</td>
<td>$136.77</td>
<td>$149.09</td>
</tr>
<tr>
<td>IT Health Systems Forensics Analyst 4</td>
<td>$148.01</td>
<td>$162.65</td>
</tr>
<tr>
<td>IT Health Systems Forensics Analyst 5</td>
<td>$159.67</td>
<td>$174.04</td>
</tr>
<tr>
<td>IT Health System Security Assurance Analyst 1</td>
<td>$82.97</td>
<td>$90.43</td>
</tr>
<tr>
<td>IT Health System Security Assurance Analyst 2</td>
<td>$99.98</td>
<td>$109.87</td>
</tr>
<tr>
<td>IT Health System Security Assurance Analyst 3</td>
<td>$111.96</td>
<td>$122.04</td>
</tr>
<tr>
<td>IT Health System Security Assurance Analyst 4</td>
<td>$125.11</td>
<td>$137.48</td>
</tr>
<tr>
<td>IT Health System Security Assurance Analyst 5</td>
<td>$142.52</td>
<td>$155.35</td>
</tr>
<tr>
<td>IT Health System/Services Consultant 1</td>
<td>$263.85</td>
<td>$287.59</td>
</tr>
<tr>
<td>IT Health System Database Administrator 1</td>
<td>$94.68</td>
<td>$102.43</td>
</tr>
<tr>
<td>IT Health System Database Administrator 2</td>
<td>$119.60</td>
<td>$129.38</td>
</tr>
<tr>
<td>IT Health System Information Assurance 1</td>
<td>$99.66</td>
<td>$107.81</td>
</tr>
<tr>
<td>IT Health System Information Assurance 3</td>
<td>$124.57</td>
<td>$134.77</td>
</tr>
<tr>
<td>IT Health System Network Administrator 1</td>
<td>$64.78</td>
<td>$70.08</td>
</tr>
<tr>
<td>IT Health System Network Administrator 2</td>
<td>$77.73</td>
<td>$84.09</td>
</tr>
<tr>
<td>IT Health System Network Administrator 3</td>
<td>$95.68</td>
<td>$103.51</td>
</tr>
<tr>
<td>IT Health System Network Architect</td>
<td>$156.97</td>
<td>$169.81</td>
</tr>
<tr>
<td>IT Health System Network Engineer 1</td>
<td>$74.25</td>
<td>$80.32</td>
</tr>
<tr>
<td>IT Health Services Program Manager</td>
<td>$164.44</td>
<td>$177.90</td>
</tr>
<tr>
<td>IT Health Systems Programmer 1</td>
<td>$65.77</td>
<td>$71.16</td>
</tr>
<tr>
<td>IT Health Systems Programmer 3</td>
<td>$89.69</td>
<td>$97.03</td>
</tr>
<tr>
<td>IT Health Systems Programmer 5</td>
<td>$129.56</td>
<td>$140.16</td>
</tr>
<tr>
<td>IT Health Services Subject Matter Expert 1</td>
<td>$169.61</td>
<td>$183.49</td>
</tr>
<tr>
<td>IT Health Systems Administrator 1</td>
<td>$80.91</td>
<td>$87.53</td>
</tr>
<tr>
<td>IT Health Systems Administrator 3</td>
<td>$115.61</td>
<td>$125.07</td>
</tr>
<tr>
<td>IT Health Services Systems Analyst 1</td>
<td>$64.78</td>
<td>$70.08</td>
</tr>
<tr>
<td>IT Health Services Systems Analyst 3</td>
<td>$94.83</td>
<td>$102.59</td>
</tr>
<tr>
<td>IT Health Services Systems Analyst 4</td>
<td>$114.31</td>
<td>$123.66</td>
</tr>
<tr>
<td>IT Health Services Systems Engineer 1</td>
<td>$64.97</td>
<td>$70.28</td>
</tr>
<tr>
<td>IT Health Services Systems Engineer 3</td>
<td>$119.77</td>
<td>$129.57</td>
</tr>
<tr>
<td>IT Health Services Systems Engineer 4</td>
<td>$140.36</td>
<td>$151.85</td>
</tr>
<tr>
<td>IT Health Services Test Engineer 2</td>
<td>$109.80</td>
<td>$118.79</td>
</tr>
<tr>
<td>IT Health Services Testing Specialist</td>
<td>$80.91</td>
<td>$87.53</td>
</tr>
<tr>
<td>IT Health Services Training Specialist 2</td>
<td>$84.72</td>
<td>$91.65</td>
</tr>
<tr>
<td>IT Health Systems Cyber Analyst 1</td>
<td>$80.23</td>
<td>$86.80</td>
</tr>
<tr>
<td>IT Health Systems Cyber Analyst 2</td>
<td>$92.69</td>
<td>$100.27</td>
</tr>
<tr>
<td>IT Health Systems Cyber Analyst 3</td>
<td>$110.62</td>
<td>$119.67</td>
</tr>
<tr>
<td>IT Health Systems Cyber Engineer 1</td>
<td>$95.68</td>
<td>$103.51</td>
</tr>
<tr>
<td>IT Health Systems Cyber Engineer 2</td>
<td>$112.12</td>
<td>$121.30</td>
</tr>
<tr>
<td>IT Health Systems Cyber Engineer 3</td>
<td>$129.56</td>
<td>$140.16</td>
</tr>
<tr>
<td>GSA Labor Category Title</td>
<td>GSA Hourly Rate Customer Site</td>
<td>GSA Hourly Rate Xator Site</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>IT Health Systems Security Engineer 1</td>
<td>$84.72</td>
<td>$91.65</td>
</tr>
<tr>
<td>IT Health Systems Security Engineer 2</td>
<td>$114.61</td>
<td>$123.99</td>
</tr>
<tr>
<td>IT Health Systems Security Engineer 3</td>
<td>$137.53</td>
<td>$148.79</td>
</tr>
<tr>
<td>IT Health Systems Data Warehouse Analyst 1</td>
<td>$90.69</td>
<td>$98.11</td>
</tr>
<tr>
<td>IT Health Systems Data Warehouse Engineer 1</td>
<td>$93.68</td>
<td>$101.35</td>
</tr>
<tr>
<td>IT Health Systems Program &amp; Policy Analyst 1</td>
<td>$89.69</td>
<td>$97.03</td>
</tr>
<tr>
<td>IT Health Systems Program &amp; Policy Analyst 3</td>
<td>$120.39</td>
<td>$130.24</td>
</tr>
<tr>
<td>IT Health Systems Certification and Accreditation Analyst 1</td>
<td>$97.66</td>
<td>$105.65</td>
</tr>
<tr>
<td>IT Health Systems Certification and Accreditation Analyst 3</td>
<td>$125.57</td>
<td>$135.85</td>
</tr>
<tr>
<td>IT Health Systems Facility Engineer 1</td>
<td>$56.31</td>
<td>$60.92</td>
</tr>
</tbody>
</table>