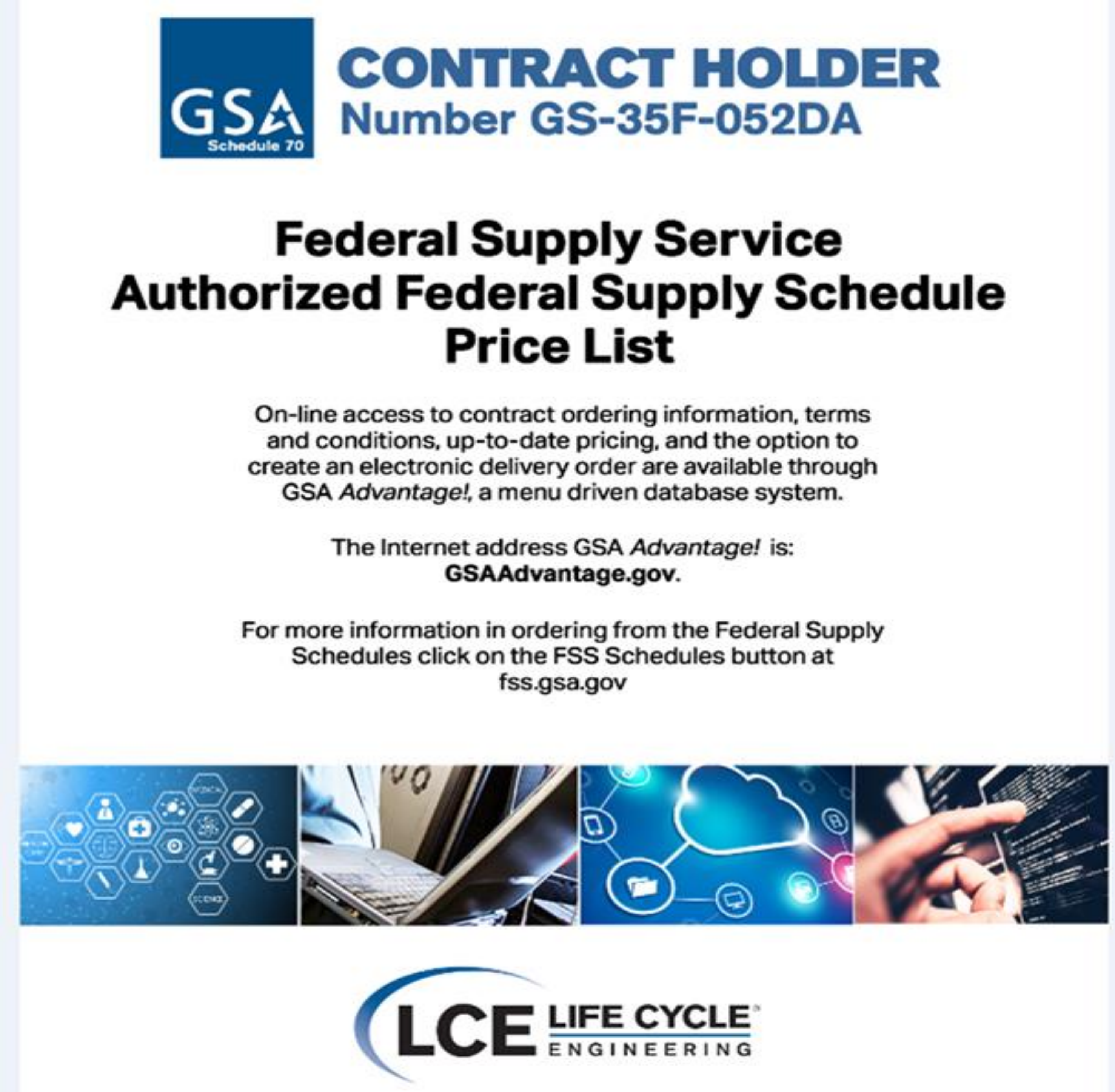

GSA Schedule 70

CONTRACT HOLDER
Number GS-35F-052DA

# Federal Supply Service Authorized Federal Supply Schedule Price List

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

The Internet address GSA *Advantage!* is:
**GSAAdvantage.gov.**

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

LCE LIFE CYCLE ENGINEERING

# MULTIPLE AWARD SCHEDULE

**Contract Number: GS-35-F-352DA through modification PS-A853 dated 25 January 2023**
**Contract Period: 12/18/15-12/17/2025**

## SPECIAL ITEM NO. 54151S- INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES

***NAICS Codes 541511, 541512, 541513, 541519***

- ✓ FPDS Code D301 IT Facility Operation and Maintenance
- ✓ FPDS Code D302 IT Systems Development Services
- ✓ FPDS Code D306 IT Systems Analysis Services
- ✓ FPDS Code D307 Automated Information Systems Design and Integration Services
- ✓ FPDS Code D308 Programming Services
- ✓ FPDS Code D310 IT Backup and Security Services
- ✓ FPDS Code D311 IT Data Conversion Services
- ✓ FPDS Code D316 IT Network Management Services
- ✓ FPDS Code D399 Other Information Technology Services, Not Elsewhere Classified

## SPECIAL ITEM NO. 54151HEAL – HEALTH INFORMATION TECHNOLOGY SERVICES

***NAICS Codes 541511, 541512, 541513, 541519***

- ✓ FPDS Code D302 IT and Telecom- Systems Development
- ✓ FPDS Code D306 IT and Telecom- Systems Analysis
- ✓ FPDS Code D307 IT and Telecom- IT Strategy and Architecture
- ✓ FPDS Code D308 IT and Telecom- Programming
- ✓ FPDS Code D310 IT and Telecom- Cyber Security and Data Backup
- ✓ FPDS Code D311 IT and Telecom- Data Conversion
- ✓ FPDS Code D313 IT and Telecom- Computer Aided Design/Computer Aided Manufacturing (CAD/CAM)
- ✓ FPDS Code D316 IT and Telecom- Telecommunications Network Management
- ✓ FPDS Code D317 IT and Telecom- Web-Based Subscription
- ✓ FPDS Code D399 IT and Telecom- Other IT and Telecommunications

## SPECIAL ITEM NO. 54151HACS – HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS)

***NAICS Codes 541511, 541512, 541513, 541519***

- ✓ FPDS Code D302 IT and Telecom- Systems Development
- ✓ FPDS Code D306 IT and Telecom- Systems Analysis
- ✓ FPDS Code D307 IT and Telecom- IT Strategy and Architecture
- ✓ FPDS Code D308 IT and Telecom- Programming
- ✓ FPDS Code D310 IT and Telecom- Cyber Security and Data Backup
- ✓ FPDS Code D311 IT and Telecom- Data Conversion
- ✓ FPDS Code D313 IT and Telecom- Computer Aided Design/Computer Aided Manufacturing (CAD/CAM)
- ✓ FPDS Code D316 IT and Telecom- Telecommunications Network Management
- ✓ FPDS Code D317 IT and Telecom- Web-Based Subscription
- ✓ FPDS Code D399 IT and Telecom- Other IT and Telecommunications

# TABLE OF CONTENTS

## CONTACT INFORMATION

| Contract Administrator | Sales & Marketing |
|---|---|
| **Kellam White** | **Bambi Hoyt** |
| **Vice President of Contracts** | **Vice President, Federal Solutions Group** |
| 4360 Corporate Rd. \| Charleston, SC 29405-7439 | 4360 Corporate Rd. \| Charleston, SC 29405-7445 |
| Phone: 843-744-7110 Ext. 7271 | Phone: 1(843) 744-7110 Ext. 7308 |
| Fax: 843-744-3971 | |
| kwhite@LCE.com | bhoyt@LCE.com |

**BUSINESS SIZE:** Other than Small

## COMPANY OVERVIEW

**Life Cycle Engineering (LCE)** was founded in 1976 and is headquartered in North Charleston, SC with offices in Washington DC, Philadelphia, PA, Pittsburgh, PA, and all major U.S. Navy fleet locations. LCE's professional staff of over 600 personnel is organized into two major groups: the Federal Services Group (FSG) and the Reliability Consulting Group (RCG).

### SUMMARY OF SERVICES

Life Cycle Engineering provides information technology and infrastructure support solutions to meet the demanding needs of our government clients by exceeding their expectations through innovation, our dedication to delivering projects on time and within budget, and our partnership approach. Our creativity and expertise help us deliver world-class solutions that support mission-critical business initiatives.

### Applied Information Technology

Applied Information Technology solutions that combine software development, systems engineering, quality assurance, cyber security, architecture, requirements, configuration management and Red Hat training.

### Engineering and Technical Services

Shipboard engineering and technical support services for U.S. and foreign navies, providing expertise in electrical and mechanical engineering, systems engineering and software development.

### Integrated Logistics Support (ILS) Services

Acquisition, logistics planning and life cycle support services for military ships and shipboard support systems, shipboard combat systems and aviation systems.

## CUSTOMER INFORMATION

1a. Awarded Special Item Number(s):

| SIN | Description |
|---|---|
| 54151S | Information Technology Professional (IT) Professional Services |
| 54151HEAL | Health Information Technology Services |
| 54151HACS | Highly Adaptive Cybersecurity Services (HACS) |

**Cooperative Purchasing (STLOC) and Disaster Recovery Purchasing (DR) are available

1b. Lowest Priced Model Number and Price for each SIN: (Government net price based on a unit of one)

1c. HOURLY RATES (Services only): Shown on page 21.

2. Maximum order: $500,000.00

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

3. Minimum order: $100

4. Geographic Coverage: Domestic, or 48 contiguous states, the District of Columbia, and Hawaii.

5. Point of Production: Not Applicable.

6. Discount from List Price: GSA Net Prices are shown on the attached GSA Pricelist. Negotiated discount has been applied and the IFF has been added.

7. Quantity Discount:

| | |
|---|---|
| 0.25% | Discount for single task orders over $200,000 |
| 0.5% | Discount for single task orders over $250,000 |
| 1.0% | Discount for single task orders over $1,000,000 |
| 1.5% | Discount for single task orders over $1,500,000 |
| 2.0% | Discount for single task orders over $2,000,000 |

8. Prompt Payment Terms: Net 30 days from receipt of invoice or date of acceptance, whichever is later.

9a. Government Purchase Cards are accepted below the micro purchase threshold.

9b. Government Purchase Cards are accepted above the micro purchase threshold.

10. Foreign Items: None

11a. Time of Delivery: The Contractor shall deliver to destination within the number of calendar days after receipt of order (ARO), as set forth below.

| SPECIAL ITEM NUMBER | DELIVERY TIME (Days ARO) |
|---|---|
| 54151S Information Technology Professional Services<br>54151HEAL- Health Information Technology Services<br>54151HACS-Highly Adaptive Cybersecurity Services(HACS) | 30 days or negotiated at the task order level |

11b. Expedited Delivery: Negotiated at the Task order Level

11c. Overnight/2 day Delivery: Negotiated at the Task order Level

11d. Urgent Requirements: Negotiated at the Task order Level

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. FOB Point: Destination

13a. Ordering Address:

Life Cycle Engineering, Inc.
4360 Corporate Road
North Charleston, SC, 29405-7439
(843) 744-7110 (Phone)
www.LCE.com

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

14. Payment Address:

    Life Cycle Engineering, Inc.
    4360 Corporate Road
    North Charleston, SC, 29405-7439
    (843) 744-7110 (Phone)
    www.lce.com

15. Warranty Provisions: Contractor's Standard Warranty.

16. Export Packing Charges: Not applicable.

17. Terms and Conditions of Government Purchase Card Acceptance: To be determined at time of award

18. Terms and Conditions of rental, maintenance, and repair: Not applicable.

19. Terms and Conditions of installation: Not applicable.

20. Terms and Conditions of repair parts indicating date of parts price lists and any discounts from list prices: Not applicable.

20b. Terms and Conditions of any other service parts: Not applicable.

21. List of Service and Distribution Points: Not applicable.

22. List of Participating Dealers: Not applicable.

23. Preventative Maintenance: Not applicable.

24a. **Section 508 Compliance for Electronic and Information Technology (EIT):** Section 508 compliance information on the supplies and services in this contract are available at the following website address (URL): http://LCE.com/.

The EIT standard can be found at: www.Section508.gov/.

25. SAM UEI: S95EAVECVJA7

26. Life Cycle Engineering, Inc. is registered in the System for Award Management (SAM) Database.

# TERMS AND CONDITIONS APPLICABLE TO INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES

## SPECIAL ITEM NUMBER 54151S

*******NOTE: All non-professional labor categories must be incidental to, and used solely to support professional services, and cannot be purchased separately. The availability or limitation of the IT Professional Labor types (with the education and/or experience) can occur for the GSA contract. In those instances LIFE CYCLE ENGINEERING, INC. will provide their response to the GSA customer requirements reflecting the substitution of education and/or experience. The acquiring Agency will have sole determination if the substitution(s) is considered acceptable prior to an award.***

## 1. SCOPE

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

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

## 2. PERFORMANCE INCENTIVES

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 in accordance with this clause.

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

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

## 3. ORDER

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

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

## 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/EC 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. Contract0rs cannot use GSA city pair contracts.

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

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

The Inspection of Services–Fixed Price (AUG 1996) (Deviation – May 2003) clause at FAR 52.246-4 applies to firm-fixed price orders placed under this contract. The Inspection–Time-and-Materials and Labor-Hour (JAN 1986) (Deviation – May 2003) clause at FAR 52.246-6 applies to time-and-materials and labor-hour orders placed under this contract.

## 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 (Deviation – May 2003) Rights in Data – General, may apply.

## 8. RESPONSIBILITIES OF THE ORDERING ACTIVITY

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

## 9. INDEPENDENT CONTRACTOR

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

## 10. ORGANIZATIONAL CONFLICTS OF INTEREST

a. Definitions:

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

- ✓ “Contractor and its affiliates” and “Contractor or its affiliates” refers to the Contractor, its chief executives, directors, officers, subsidiaries, affiliates, subcontractors at any tier, and consultants and any joint venture involving the Contractor, any entity into or with which the Contractor subsequently merges or affiliates, or any other successor or assignee of the Contractor.
- ✓ An “Organizational conflict of interest” exists when the nature of the work to be performed under a proposed ordering activity contract, without some restriction on ordering activities by the Contractor and its affiliates, may either
  - i. result in an unfair competitive advantage to the Contractor or its affiliates or
  - ii. impair the Contractor’s or its affiliates’ objectivity in performing contract work.

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

## 11. INVOICES

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

## 12. PAYMENTS

For firm-fixed price orders the ordering activity shall pay the Contractor, upon submission of proper invoices or vouchers, the prices stipulated in this contract for service rendered and accepted. Progress payments shall be made only when authorized by the order.

For time-and-materials orders, the Payments under Time-and-Materials and Labor-Hour Contracts at FAR 52.232-7 (DEC 2002), (Alternate II – Feb 2002) (Deviation – May 2003) 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 52.232-7 (DEC 2002), (Alternate II – Feb 2002) (Deviation – May 2003)) 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.

## 13. RESUMES

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

## 14. INCIDENTAL SUPPORT COSTS

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

## 15. APPROVAL OF SUBCONTRACTS

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

## 16. SERVICES PERFORMED

a. All services performed by the Contractor under the terms of this contract shall be as an independent Contractor, and not as an agent or employee of the ordering activity.
b. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity.

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

## 17. TRAVEL

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

## 18. WARRANTY

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

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

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

## 19. DESCRIPTION OF IT SERVICES AND PRICING

See pages 26-54 for the IT Professional Descriptions and Pricing.

# TERMS AND CONDITIONS APPLICABLE TO HEALTH INFORMATION TECHNOLOGY (IT) SERVICES

## SPECIAL ITEM NUMBER 54151HEAL

## 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 Information Technology Schedule.

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 IT Schedule 70 (e.g. 33411, 33411REF, 532420L, 532420R and 811212).

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.

## 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.

## 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 Health IT Services must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel. Contractors cannot use GSA city pair contracts. All travel will be agreed upon with the client prior to the Contractor's travel.

## 4. INSPECTION OF SERVICES

In accordance with FAR 52.212-4 CONTRACT TERMS AND CONDITIONS--COMMERCIAL ITEMS (MAR 2009) (DEVIATION I - FEB 2007) for Firm-Fixed Price orders and FAR 52.212-4 CONTRACT TERMS AND CONDITIONS −COMMERCIAL ITEMS (MAR 2009) (ALTERNATE I − OCT 2008) (DEVIATION I – FEB 2007) applies to Time-and-Materials and Labor-Hour Contracts orders placed under this contract.

## 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.

## 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 Health IT Services.

## 7. INDEPENDENT CONTRACTOR

All Health IT 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.

## 8. ORGANIZATIONAL CONFLICTS OF INTEREST

a. Definitions.

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

c. "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.

d. 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.

e. 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.

## 9. INVOICES

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

## 10. RESUMES

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

## 11. INCIDENTAL SUPPORT COSTS

Incidental support costs are not considered part of 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.

## 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.

## 13. SERVICES PERFORMED

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

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

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

d. Services offered SIN 54151HEAL shall 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)
- The National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) and Special Publications
- Federal Information Security Management Act (FISMA) of 2002

## 14. TRAVEL

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

## 15. WARRANTY

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

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

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

## 16. DESCRIPTION OF HEALTH IT SERVICES AND PRICING

See pages 26-54 for descriptions and pricing for Health IT Services.

# TERMS AND CONDITIONS APPLICABLE TO HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS) SPECIAL ITEM NUMBER 54151HACS

## 1. SCOPE

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 Information Technology Schedule. The following are the approved subcategories:

- **Risk and Vulnerability Assessments (RVA)**,
- **Penetration Testing**

a. Services under this SIN are limited to Highly Adaptive Cybersecurity Services only. Software and hardware products are under different Special Item Numbers on IT Schedule 70 ((e.g. 33411, 33411REF, 532420L, 532420R and 811212), and may be quoted along with services to provide a total solution.

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

c. 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.

## 2. 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 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.

Sub-Categories - (not all vendors have been placed within the following subcategories. To view a complete list of vendors, click on the SIN)

- 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.

- 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.
● 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.
● 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. 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.

## 3. 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. 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 GSA city pair contracts. All travel will be agreed upon with the client prior to the Contractor's travel.

## 5. 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.

## 6. 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.

## 7. 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.

## 8. 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.

## 9. 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.

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.

## 10. 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.

## 11. RESUMES

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

## 12. 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.

## 13. SERVICES PERFORMED

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

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

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

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

- Federal Acquisition Regulation (FAR) Part 52.204-21
- OMB Memorandum M-17-12 - Preparing for and Responding to a Breach of Personally Identifiable Information (PII)

- OMB Memorandum M- 19-03 - Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program
- 2017 Report to the President on Federal IT Modernization
- The Cybersecurity National Action Plan (CNAP)
- NIST SP 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems
- NIST SP 800-27A - Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
- NIST SP 800-30 - Guide for Conducting Risk Assessments
- NIST SP 800-35 - Guide to Information Technology Security Services
- NIST SP 800-37 - Risk Management Framework for Information Systems and Organizations: A Systems Life Cycle Approach for Security and Privacy
- NIST SP 800-39 - Managing Information Security Risk: Organization, Mission, and Information System View
- 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.

## 14. TRAVEL

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

## 15. WARRANTY

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

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

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

## 16. DESCRIPTION OF HIGHLY ADAPTIVE CYBERSECURITY SERVICES AND PRICING

See pages 26-54 for descriptions and pricing for Health IT Services

## LABOR RATES FOR SINS 54151S, 54151HEAL, 54151HACS

**Life Cycle Engineering, Inc.**
**GSA Price List with IFF**

| SIN | Labor Category | 12/18/2020 - 12/17/2021 | 12/18/2021 - 12/17/2022 | 12/18/2022 - 12/17/2023 | 12/18/2023 - 12/17/2024 | 12/18/2024 - 12/17/2025 |
|---|---|---|---|---|---|---|
| *54151S* | Program Manager I | $106.09 | $107.26 | $108.44 | $109.63 | $110.83 |
| *54151S* | Program Manager II | $137.67 | $139.18 | $140.71 | $142.26 | $143.82 |
| *54151S* | Program Manager III | $158.19 | $159.93 | $161.69 | $163.47 | $165.27 |
| *54151S* | Program Manager IV | $208.58 | $210.88 | $213.20 | $215.54 | $217.91 |
| *54151S* | Project Manager I | $86.11 | $87.06 | $88.02 | $88.99 | $89.96 |
| *54151S* | Project Manager II | $114.72 | $115.98 | $117.26 | $118.55 | $119.85 |
| *54151S* | Project Manager III | $156.43 | $158.15 | $159.89 | $161.65 | $163.43 |
| *54151S* | Subject Matter Expert I | $57.37 | $58.00 | $58.64 | $59.28 | $59.94 |
| *54151S* | Subject Matter Expert II | $89.69 | $90.68 | $91.67 | $92.68 | $93.70 |
| *54151S* | Subject Matter Expert III | $132.45 | $133.90 | $135.38 | $136.87 | $138.37 |
| *54151S* | Subject Matter Expert IV | $138.71 | $140.24 | $141.78 | $143.34 | $144.92 |
| *54151S* | Technical Writer | $70.49 | $71.27 | $72.05 | $72.85 | $73.65 |
| *54151S* | IT Specialist I | $67.03 | $67.76 | $68.51 | $69.26 | $70.02 |
| *54151S* | IT Specialist II | $108.28 | $109.47 | $110.67 | $111.89 | $113.12 |
| *54151S* | IT Specialist III | $140.79 | $142.34 | $143.91 | $145.49 | $147.09 |
| *54151S* | Jr IT Spec | $41.73 | $42.19 | $42.66 | $43.12 | $43.60 |
| *54151HEAL* | HIT Program Manager I | $106.09 | $107.26 | $108.44 | $109.63 | $110.83 |
| *54151HEAL* | HIT Program Manager II | $137.67 | $139.18 | $140.71 | $142.26 | $143.82 |
| *54151HEAL* | HIT Program Manager III | $158.19 | $159.93 | $161.69 | $163.47 | $165.27 |
| *54151HEAL* | HIT Program Manager IV | $208.58 | $210.88 | $213.20 | $215.54 | $217.91 |
| *54151HEAL* | HIT Project Manager I | $86.11 | $87.06 | $88.02 | $88.99 | $89.96 |
| *54151HEAL* | HIT Project Manager II | $114.72 | $115.98 | $117.26 | $118.55 | $119.85 |
| *54151HEAL* | HIT Project Manager III | $156.43 | $158.15 | $159.89 | $161.65 | $163.43 |
| *54151HEAL* | HIT Subject Matter Expert I | $57.37 | $58.00 | $58.64 | $59.28 | $59.94 |
| *54151HEAL* | HIT Subject Matter Expert II | $89.69 | $90.68 | $91.67 | $92.68 | $93.70 |
| *54151HEAL* | HIT Subject Matter Expert III | $132.45 | $133.90 | $135.38 | $136.87 | $138.37 |
| *54151HEAL* | HIT Subject Matter Expert IV | $138.71 | $140.24 | $141.78 | $143.34 | $144.92 |
| *54151HEAL* | HIT Technical Writer | $70.49 | $71.27 | $72.05 | $72.85 | $73.65 |
| *54151HEAL* | HIT IT Specialist I | $67.03 | $67.76 | $68.51 | $69.26 | $70.02 |
| *54151HEAL* | HIT IT Specialist II | $108.28 | $109.47 | $110.67 | $111.89 | $113.12 |
| *54151HEAL* | HIT IT Specialist III | $140.79 | $142.34 | $143.91 | $145.49 | $147.09 |
| *54151HEAL* | HIT Jr IT Specialist | $41.73 | $42.19 | $42.66 | $43.12 | $43.60 |
| *54151HACS* | HACS Cyber Program Manager I | $106.09 | $107.26 | $108.44 | $109.63 | $110.83 |
| *54151HACS* | HACS Cyber Program Manager II | $137.67 | $139.18 | $140.71 | $142.26 | $143.82 |
| *54151HACS* | HACS Cyber Program Manager III | $158.19 | $159.93 | $161.69 | $163.47 | $165.27 |
| *54151HACS* | HACS Cyber Program Manager IV | $208.58 | $210.88 | $213.20 | $215.54 | $217.91 |
| *54151HACS* | HACS Cyber Project Manager I | $86.11 | $87.06 | $88.02 | $88.99 | $89.96 |
| *54151HACS* | HACS Cyber Project Manager II | $114.72 | $115.98 | $117.26 | $118.55 | $119.85 |
| *54151HACS* | HACS Cyber Project Manager III | $156.43 | $158.15 | $159.89 | $161.65 | $163.43 |
| *54151HACS* | HACS Cyber Subject Matter Exert I | $57.37 | $58.00 | $58.64 | $59.28 | $59.94 |
| *54151HACS* | HACS Cyber Subject Matter Expert II | $89.69 | $90.68 | $91.67 | $92.68 | $93.70 |
| *54151HACS* | HACS Cyber Subject Matter Expert III | $132.45 | $133.90 | $135.38 | $136.87 | $138.37 |
| *54151HACS* | HACS Cyber Subject Matter Expert IV | $138.71 | $140.24 | $141.78 | $143.34 | $144.92 |
| *54151HACS* | HACS Cyber Technical Writer | $70.49 | $71.27 | $72.05 | $72.85 | $73.65 |
| *54151HACS* | HACS Cyber IT Specialist I | $67.03 | $67.76 | $68.51 | $69.26 | $70.02 |
| *54151HACS* | HACS Cyber IT Specialist II | $108.28 | $109.47 | $110.67 | $111.89 | $113.12 |
| *54151HACS* | HACS Cyber IT Specialist III | $140.79 | $142.34 | $143.91 | $145.49 | $147.09 |
| *54151HACS* | HACS Junior Cyber Specialist | $62.60 | $63.29 | $63.98 | $64.69 | $65.40 |

****The availability or limitation of the IT Professional Labor types (with the education and/or experience) can occur for the GSA contract. In those instances LIFE CYCLE ENGINEERING, INC. will provide their response to the GSA customer requirements reflecting the substitution of education and/or experience. The acquiring Agency will have sole determination if the substitution(s) is considered acceptable prior to an award.**

# LABOR CATEGORY DESCRIPTIONS FOR SIN 54151S INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES

## Program Manager I

**Minimum/General Experience and Years of Experience:** 5 years technical experience with at least 2 years managing complex IT, Cybersecurity, and/or Health IT programs.

**Functional Responsibility:** Performs overall management of contract support operations, possibly involving multiple projects or groups. Organizes, directs, and coordinates the planning and production of all contract support activities. Provides technical guidance and project management functions associated with client requirements including but not limited to: technical management of projects; budget monitoring; personnel recruitment to support client; and assistance in the development and writing of client work plans. PMs not only have responsibility for managing projects in IT, but also possess strong technical skills. Must be capable of leading projects that involve the successful management of teams composed of data processing and other information management professionals who have been involved in analysis, design, integration, testing, documenting, converting, extending, and implementing automated information and/or telecommunications systems.

**Minimum Educational Requirements:** A Bachelor's degree in Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## Program Manager II

**Minimum/General Experience and Years of Experience:** 10 years technical experience with at least 5 years managing complex IT, Cybersecurity, and/or Health IT programs.

**Functional Responsibility:** Performs overall management of contract support operations, possibly involving multiple projects or groups. Organizes, directs, and coordinates the planning and production of all contract support activities. Provides technical guidance and project management functions associated with client requirements, including but not limited to: technical management of projects; budget monitoring; personnel recruitment to support client; and the development and writing of client work plans. PMs are senior personnel who not only have responsibility for managing, projects in IT, but also possess strong technical skills. Must be capable of leading projects that involve the successful management of teams composed of data processing and other information management professionals who have been involved in analysis, design, integration, testing documenting, converting, extending, and implementing automated information and/or telecommunications systems.

**Minimum Educational Requirements:** A Bachelor's degree in Computer Science, Information Systems, and Engineering, Business or other related scientific, project or technical discipline.

## Program Manager III

**Minimum/General Experience and Years of Experience:** 15 years technical experience with at least 8 years managing complex IT, Cybersecurity, and/or Health IT programs.

**Functional Responsibility:** Performs overall management of contract support operations, possibly involving multiple projects or groups. Organizes, directs, and coordinates the planning and production of all contract support activities. Provides technical guidance and project management functions associated with client requirements, including but not limited to: technical management of projects; budget monitoring; personnel recruitment to support client; and the development and writing of client work plans. This professional manages multiple programs. PMs are senior personnel who not only have responsibility for managing, projects in IT, but also possess strong technical skills. Must be capable of leading projects that involve the successful management of teams composed of data processing and other information management professionals who have been involved in analysis, design, integration, testing, documenting, converting, extending, and implementing automated information and/or telecommunications systems.

**Minimum Educational Requirements:** MA/MS degree in Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## Program Manager IV

**Minimum/General Experience and Years of Experience:** 15+ years technical experience with at least 10 years managing complex IT, Cybersecurity, and/or Health IT programs.

**Functional Responsibility:** Performs overall management of contract support operations, possibly involving multiple projects or groups. Organizes, directs, and coordinates the planning and production of all contract support activities. Provides technical guidance and project management functions associated with client requirements, including but not limited to: technical management of projects; budget monitoring; personnel recruitment to support client; and the development and writing of client work plans. This professional manages multiple programs. PMs are senior personnel who not only have responsibility for managing, projects in IT, but also possess strong technical skills. These senior personnel are renowned experts in either functional domains (e.g., finance, personnel, acquisition, etc.) or technical disciplines (e.g., computer security, network engineering, etc.) with many years of experience. They generally have advanced degrees and extensive experience as technical leaders and/or senior Project Managers. Must be capable of leading projects that involve the successful management of teams composed of data processing and other information management professionals who have been involved in analysis, design, integration, testing, documenting, converting, extending, and implementing automated information and/or telecommunications systems.

**Minimum Educational Requirements:** MA/MS degree in Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## Project Manager I

**Minimum/General Experience and Years of Experience:** 5 years technical experience with at least 2 years managing IT, cybersecurity, and/or Health IT projects.

**Functional Responsibility:** Responsible for the overall management of assigned project task orders and for ensuring that the technical solutions in specific delivery orders are implemented in a timely manner. Organizes, directs, and coordinates the resources and planning of all task related activities associated with assigned delivery order projects. Provides technical guidance and project management functions associated with client requirements. They may manage IT projects.

**Minimum Educational Requirements:** A Bachelor's degree in Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## Project Manager II

**Minimum/General Experience and Years of Experience:** 10 years technical experience with at least 5 years managing IT, cybersecurity, and/or Health IT projects.

**Functional Responsibility:** Responsible for the overall management of assigned project task orders and for ensuring that the technical solutions in specific delivery orders are implemented in a timely manner. Organizes, directs, and coordinates the resources and planning of all task related activities associated with assigned delivery order projects. Provides technical guidance and project management functions associated with client requirements. They may manage IT projects.

**Minimum Educational Requirements:** A Bachelor's degree in Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## Project Manager III

**Minimum/General Experience and Years of Experience:** 15 years technical experience with at least 8 years managing IT and Health IT projects.

**Functional Responsibility:** Responsible for the overall management of assigned project task orders and for ensuring that the technical solutions in specific delivery orders are implemented in a timely manner. Organizes, directs, and coordinates the resources and planning of all task related activities associated with assigned delivery order projects. Provides technical guidance and project management functions associated with client requirements. They may manage IT  projects.

**Minimum Educational Requirements:** MA/MS degree in Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## Subject Matter Expert I

**Minimum/General Experience and Years of Experience:** At least 3 years of combined new and related older technical experience in the IT and Health IT field 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 simple to moderately complex IT 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; communications protocols; risk management/electronic analysis; software; life-cycle management; software development methodologies; and modeling and simulation.

**Minimum Educational Requirements:** Associates Degree in a project related field such as Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## Subject Matter Expert II

**Minimum/General Experience and Years of Experience:** At least 7 years of combined new and related older technical experience in the IT and Health IT field directly related to the required area of expertise.

**Functional Responsibility:** Defines the problems and analyzes and develops plans and requirements in the subject matter area for moderately complex to complex IT systems. Coordinates and manages the preparation of analysis, evaluations, and recommendations for proper implementation of programs and systems specifications in the following specialties: information systems architecture; networking; telecommunications; automation; communications protocols; risk management/electronic analysis; software; life-cycle management; software development methodologies; and modeling and simulation.

**Minimum Educational Requirements:** Associates Degree in a project related field such as Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## Subject Matter Expert III

**Minimum/General Experience and Years of Experience:** At least 10 years of combined new and related older technical experience in the IT, cybersecurity, and/or Health IT field directly related to the required area of expertise.

**Functional Responsibility:** Provides technical, managerial, and administrative direction for problem definition, analysis, requirements development and implementation for complex to extremely complex IT systems in the subject matter area. Makes recommendations and advises on organization-wide system improvements, optimization or maintenance efforts in the following specialties: information systems architecture; networking; telecommunications; automation; communications protocols; risk management/electronic analysis; software; life-cycle management; software development methodologies; and modeling and simulation.

**Minimum Educational Requirements:** BA/BS Degree in Business or project related field such as Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## Subject Matter Expert IV

**Minimum/General Experience and Years of Experience:** 15 years of combined new and related older technical experience in the IT, cybersecurity, and/or Health IT field directly related to the required area of expertise.

**Functional Responsibility:** Applies their advanced skills and experience in systems development, detailed knowledge of business processes, technical background and supervisory skills to implement business solutions. Provides technical, managerial, and administrative direction for problem definition, analysis, requirements development and implementation for complex to extremely complex IT systems in the subject matter area. Makes recommendations and advises on organization-wide system improvements, optimization or maintenance efforts in the following specialties: information systems architecture; networking; telecommunications; automation; communications protocols; risk management/electronic analysis; software; lifecycle management; software development methodologies; and modeling and simulation.

**Minimum Educational Requirements:** BA/BS Degree in Business or project related field such as Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## Technical Writer

**Minimum/General Experience and Years of Experience:** 2 years relevant IT, cybersecurity, and Health IT experience.

**Functional Responsibility:** Assists in collecting and organizing information for preparation of user manuals, training materials, installation guides, proposals, and reports. Edit functional descriptions, system specifications, user manuals, special reports, or any other customer deliverable or document. Assists in performing financial and administrative functions. Must demonstrate the ability to work independently or under only general direction.

**Minimum Educational Requirements:** BA/BS Degree in English, Technical Writing or other writing related field.

## IT Specialist I

**Minimum/General Experience and Years of Experience:** 3 years relevant IT, cybersecurity, and/or Health IT experience.

**Functional Responsibility in one or more of the following areas:** Database design or Information Assurance or application design or enterprise architecture or disaster recovery, or configuration management or forensic intrusion analysis or network analysis in IT. Applying a business wide set of disciplines for planning, analysis, design, construction, and maintenance of information systems business wide or across a major sector of the business. Gathering and organizing technical information about an organization's mission goals and needs, existing security products, and ongoing programs in the MLS arena. Performing risk analysis, which include risk assessment. Experience developing applications using advanced technologies, such as Internet protocols or web-based technology to include HTML, CGI applications, PERL or JavaScript, and Java. Develop, manage, maintain, and evaluate state-of-the-art computer hardware, software, and software development tools; evaluate their ability to support specific requirements and interface with other equipment and systems; determine potential and actual bottlenecks and propose recommendations for their elimination; and make recommendations for system improvements that will result in optimal hardware and software use. Analysis and definition of security requirements for multilevel security (MLS) issues. Designs, develops, engineers, and implements solutions to MLS requirements. Analyzes and defines security requirements for computer systems, which may include mainframes, workstations, and personal computers. Designs, develops, engineers, and implements solutions to security requirements. Responsible for integration and implementation of the computer system security solution.

**Minimum Educational Requirements:** Bachelor’s degree in related field such as Computer Science, Computer Engineering, Information Assurance, etc. and applicable discipline certification such as CISSP, CCNA, CCNP,  RHCSA, RHCE, GPEN, GSEC, MCSD, MCSA, OCA, OCP, OCE, etc.

## IT Specialist II

**Minimum/General Experience and Years of Experience:** 7 years relevant IT, cybersecurity, and/or Health IT experience.

**Functional Responsibility in one or more of the following areas**: Database design or Information Assurance or application design or enterprise architecture or disaster recovery, or configuration management or forensic intrusion analysis or network analysis in IT. Applying a business wide set of disciplines for planning, analysis, design, construction, and maintenance of information systems business wide or across a major sector of the business. Gathering and organizing technical information about an organization's mission goals and needs, existing security products, and ongoing programs in the MLS arena. Performing risk analysis, which include risk assessment. Experience developing applications using advanced technologies, such as Internet protocols or web-based technology to include HTML, CGI applications, PERL or JavaScript, and Java. Develop, manage, maintain, and evaluate state-of-the-art computer hardware, software, and software development tools; evaluate their ability to support specific requirements and interface with other equipment and systems; determine potential and actual bottlenecks and propose recommendations for their elimination; and make recommendations for system improvements that will result in optimal hardware and software use. Analysis and definition of security requirements for multilevel security (MLS) issues. Designs, develops, engineers, and implements solutions to MLS requirements. Designs, develops, engineers, and implements solutions that meet security requirements. Responsible for integration and implementation of the computer system security solution. Gathers and organizes technical information about an organization’s mission goals and needs, existing security products, and ongoing programs in computer security. Performs risk analyses of computer systems and applications during all phases of the system development life cycle.

**Minimum Educational Requirements:** Bachelor’s degree in related field such as Computer Science, Computer Engineering, Information Assurance, etc. and applicable discipline certification such as CISSP, CCNA, CCNP, RHCSA, RHCE, GPEN, GSEC, MCSD, MCSA, OCA, OCP, OCE, etc.

## IT Specialist III

**Minimum/General Experience and Years of Experience:** 10 years relevant IT, cybersecurity, and/or Health IT experience.

**Functional Responsibility in one or more of the following areas:** Database design or Information Assurance or application design or enterprise architecture or disaster recovery, or configuration management or forensic intrusion analysis or network analysis in IT, cybersecurity, and/or Health IT. Applying a business wide set of disciplines for planning, analysis, design, construction, and maintenance of information systems business wide or across a major sector of the business. Gathering and organizing technical information about an organization's mission goals and needs, existing security products, and ongoing programs in the MLS arena. Experience developing applications using advanced technologies, such as Internet protocols or web-based technology to include HTML, CGI applications, PERL or JavaScript, and Java. Developing, manage, maintain, and evaluate state-of-the-art computer hardware, software, and software development tools; evaluate their ability to support specific requirements and interface with other equipment and systems; determine potential and actual bottlenecks and propose recommendations for their elimination; and make recommendations for system improvements that will result in optimal hardware and software use. Leads the analysis and definition of security requirements for multilevel security (MLS) issues. Designs, develops, engineers, and implements solutions to MLS requirements. Leads the risk analyses of computer systems and applications during all phases of the system development life cycle.

**Minimum Educational Requirements:** MA/MS or Bachelor’s degree in related field such as Computer Science, Computer Engineering, Information Assurance, etc. and applicable discipline certification such as  CISSP, CCNA, CCNP, RHCSA, RHCE, GPEN, GSEC, MCSD, MCSA, OCA, OCP, OCE, etc.

## Junior IT Specialist

**Minimum/General Experience and Years of Experience:** 1 year relevant IT and Health IT experience.

**Functional Responsibility in one or more of the following areas:** Database administration or Information Assurance or configuration management or software development or system administration in IT. Analyzes security and software requirements for networks and systems. Designs, develops, engineers, and implements solutions that meet network, application, software, or security requirements. Responsible for integration and implementation of the network security solution. Performs vulnerability/risk analyses of computer systems and applications during all phases of the system development life cycle.

**Minimum Educational Requirements:** High School diploma

**Certification Requirements:** Applicable discipline certification such as Security+, CCNA-Security, GSEC, CEH, etc.

# LABOR CATEGORY DESCRIPTIONS FOR SIN 54151HEAL HEALTH INFORMATION TECHNOLOGY SERVICES (HITS)

## HIT Program Manager I

**Minimum/General Experience and Years of Experience:** 5 years technical experience with at least 2 years managing complex IT, Cybersecurity, and/or Health IT programs.

**Functional Responsibility:** Network Security design or Information Assurance or forensic intrusion analysis. Analyzes and defines security requirements for local and wide area networks. Designs, develops, engineers, and implements solutions that meet network and/or application security requirements according to Risk Management Framework (RMF) guidance. Responsible for integration and implementation of the network and application security solution. Performs vulnerability/risk analyses and remediation of computer systems and applications during all phases of the system development life cycle.

**Minimum Educational Requirements:** A Bachelor's degree in Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## HIT Program Manager II

**Minimum/General Experience and Years of Experience:** 10 years technical experience with at least 5 years managing complex IT, Cybersecurity, and/or Health IT programs.

**Functional Responsibility:** Performs overall management of contract support operations related to connected health, management of electronic health records, information exchanges and health analytics, personal health information management, innovative Health IT solutions, health information, and/or emerging Health IT research, possibly involving multiple projects or groups. Organizes, directs, and coordinates the planning and production of all contract support activities. Provides technical guidance and project management functions associated with client requirements including but not limited to: technical management of projects; budget monitoring; personnel recruitment to support client; and the development and writing of client work plans. PMs are senior personnel who not only have responsibility for managing projects in Health IT, but also possess strong technical skills. Must be capable of leading projects that involve the successful management of teams composed of data processing and other health information management professionals who have been involved in analysis, design, integration, testing, documenting, converting, extending, and implementing automated Health IT systems.

**Minimum Educational Requirements:** A Bachelor's degree in Computer Science, Information Systems, and Engineering, Business or other related scientific, project or technical discipline.

## HIT Program Manager III

**Minimum/General Experience and Years of Experience:** 15 years technical experience with at least 8 years managing complex IT, Cybersecurity, and/or Health IT programs.

**Functional Responsibility:** Performs overall management of contract support operations related to connected health, management of electronic health records, information exchanges and health analytics, personal health information management, innovative Health IT solutions, health information, and/or emerging Health IT research, possibly involving multiple projects or groups. Organizes, directs, and coordinates the planning and production of all contract support activities. Provides technical guidance and project management functions associated with client requirements, including but not limited to: technical management of projects; budget monitoring; personnel recruitment to support client; and the development and writing of client work plans. This professional manages multiple programs. PMs are senior personnel who not only have responsibility for managing projects in health information management, but also possess strong technical skills. Must be capable of leading projects that involve the successful management of teams composed of data processing and other health information management professionals who have been involved in analysis, design, integration, testing, documenting, converting, extending, and implementing automated Health IT systems.

**Minimum Educational Requirements:** MA/MS degree in Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## HIT Program Manager IV

**Minimum/General Experience and Years of Experience:** 15+ years technical experience with at least 10 years managing complex IT, Cybersecurity, and/or Health IT programs.

**Functional Responsibility:** Performs overall management of contract support operations related to connected health, management of electronic health records, information exchanges and health analytics, personal health information management, innovative Health IT solutions, health information, and/or emerging Health IT research, possibly involving multiple projects or groups. Organizes, directs, and coordinates the planning and production of all contract support activities. Provides technical guidance and project management functions associated with client requirements, including but not limited to: technical management of projects; budget monitoring; personnel recruitment to support client; and the development and writing of client work plans. This professional manages multiple programs. PMs are senior personnel who not only have responsibility for managing projects in Health IT, but also possess strong technical skills. These senior personnel are renowned experts in either functional domains (e.g., finance, personnel, acquisition, etc.) or technical disciplines (e.g., connected health systems, health records, information exchanges and health analytics, etc.) with many years of experience. They generally have advanced degrees and extensive experience as technical leaders and/or senior Project Managers. Must be capable of leading projects that involve the successful management of teams composed of Health IT professionals who have been involved in analysis, design, integration, testing, documenting, converting, extending, and implementing Health IT systems.

**Minimum Educational Requirements:** MA/MS degree in Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## HIT Project Manager I

**Minimum/General Experience and Years of Experience:** 5 years technical experience with at least 2 years managing IT, cybersecurity, and/or Health IT projects.

**Functional Responsibility:** Responsible for the overall management of assigned project task orders related to connected health, management of electronic health records, information exchanges and health analytics, personal health information management, or innovative Health IT solutions; and for ensuring that the technical solutions in specific delivery orders are implemented in a timely manner. Organizes, directs, and coordinates the Health IT resources and planning of all task related activities associated with assigned delivery order projects. Provides technical guidance and project management functions associated with client requirements, and may manage Health IT projects.

**Minimum Educational Requirements:** A Bachelor's degree in Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## HIT Project Manager II

**Minimum/General Experience and Years of Experience:** 10 years technical experience with at least 5 years managing IT, cybersecurity, and/or Health IT projects.

**Functional Responsibility:** Responsible for the overall management of assigned project task orders related to connected health, management of electronic health records, information exchanges and health analytics, personal health information management, or innovative Health IT solutions; and for ensuring that the technical solutions in specific delivery orders are implemented in a timely manner. Organizes, directs, and coordinates the Health IT resources and planning of all task related activities associated with assigned delivery order projects. Provides technical guidance and project management functions associated with client requirements, and may manage Health IT projects.

**Minimum Educational Requirements:** A Bachelor's degree in Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## HIT Project Manager III

**Minimum/General Experience and Years of Experience:** 15 years technical experience with at least 8 years managing IT and Health IT projects.

**Functional Responsibility:** Responsible for the overall management of assigned project task orders related to connected health, management of electronic health records, information exchanges and health analytics, personal health information management, or innovative Health IT solutions; and for ensuring that the technical solutions in specific delivery orders are implemented in a timely manner. Organizes, directs, and coordinates the Health IT resources and planning of all task related activities associated with assigned delivery order projects. Provides technical guidance and project management functions associated with client requirements, and may manage Health IT projects.

**Minimum Educational Requirements:** MA/MS degree in Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## HIT Subject  Matter Expert I

**Minimum/General Experience and Years of Experience:** At least 3 years of combined new and related older technical experience in the IT and Health IT field 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 simple to moderately complex Health IT 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; connected health; information exchanges and health analytics; healthcare management; managing PII data; healthcare information security; risk management/electronic analysis; software; life-cycle management; software development methodologies; and modeling and simulation.

**Minimum Educational Requirements:** Associates Degree in a project related field such as Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## HIT Subject Matter Expert II

**Minimum/General Experience and Years of Experience:** At least 7 years of combined new and related older technical experience in the IT and Health IT field directly related to the required area of expertise.

**Functional Responsibility:** Defines the problems and analyzes and develops plans and requirements in the subject matter area for moderately complex to complex Health IT systems. Coordinates and manages the preparation of analysis, evaluations, and recommendations for proper implementation of programs and systems specifications in the following specialties: information systems architecture; connected health; information exchanges and health analytics; healthcare management; managing PII data; healthcare information security; risk management/electronic analysis; software; life-cycle management; software development methodologies; and modeling and simulation.

**Minimum Educational Requirements:** Associates Degree in a project related field such as Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## HIT Subject Matter Expert III

**Minimum/General Experience and Years of Experience:** At least 10 years of combined new and related older technical experience in the IT, cybersecurity, and/or Health IT field directly related to the required area of expertise.

**Functional Responsibility:** Provides technical, managerial, and administrative direction for problem definition, analysis, requirements development and implementation for complex to extremely complex Health IT systems in the subject matter area. Makes recommendations and advises on organization-wide system improvements, optimization or maintenance efforts in the following specialties: information systems architecture; connected health; information exchanges and health analytics; healthcare management; managing PII data; healthcare information security; risk management/electronic analysis; software; life-cycle management; software development methodologies; and modeling and simulation.

**Minimum Educational Requirements:** BA/BS Degree in Business or project related field such as Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## HIT Subject  Matter Expert IV

**Minimum/General Experience and Years of Experience:** 15 years of combined new and related older technical experience in the IT, cybersecurity, and/or Health IT field directly related to the required area of expertise.

**Functional Responsibility:** Applies their advanced skills and experience in systems development, detailed knowledge of business processes, technical background and supervisory skills to implement business solutions. Provides technical, managerial, and administrative direction for problem definition, analysis, requirements development and implementation for complex to extremely complex Health IT systems in the subject matter area. Makes recommendations and advises on organization-wide system improvements, optimization or maintenance efforts in the following specialties: information systems architecture; connected health; information exchanges and health analytics; healthcare management; managing PII data; healthcare information security; risk management/electronic analysis; software; life-cycle management; software development methodologies; and modeling and simulation.

**Minimum Educational Requirements:** BA/BS Degree in Business or project related field such as Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## HIT Technical Writer

**Minimum/General Experience and Years of Experience:** 2 years relevant IT, cybersecurity, and Health IT experience.

**Functional Responsibility:** Assists in collecting and organizing information for preparation of health information management processes, Health IT research, user manuals, training materials, installation guides, proposals, and reports. Edit functional descriptions, system specifications, user manuals, special reports, or any other customer deliverable or document. Assists in performing financial and administrative functions. Must demonstrate the ability to work independently or under only general direction.

**Minimum Educational Requirements:** BA/BS Degree in English, Technical Writing or other writing related field.

## HIT IT Specialist I

**Minimum/General Experience and Years of Experience:** 3 years relevant IT, cybersecurity, and/or Health IT experience.

**Functional Responsibility in one or more of the following areas:** Database design or Information Assurance or application design or enterprise architecture or disaster recovery, or configuration management or forensic intrusion analysis or network analysis in Health IT. Applying a business wide set of disciplines for planning, analysis, design, construction, and maintenance of Health IT systems business wide or across a major sector of the business. Gathering and organizing technical information about an organization's mission goals and needs, existing security products, connected health information, health management workflows, and ongoing programs in the MLS arena. Performing risk analysis, which include risk assessment. Experience developing health-related applications using advanced technologies, such as Internet protocols or web-based technology to include HTML, CGI applications, PERL or JavaScript, and Java. Develop, manage, maintain, and evaluate state-of-the-art computer hardware, software, and software development tools; evaluate their ability to support specific requirements and interface with other equipment and systems; determine potential and actual bottlenecks and propose recommendations for their elimination; and make recommendations for system improvements that will result in optimal hardware and software use. Analysis and definition of security requirements for multilevel security (MLS) issues. Designs, develops, engineers, and implements solutions to MLS requirements. Analyzes and defines security requirements for computer systems, which may include mainframes, workstations, and personal computers. Designs, develops, engineers, and implements solutions to security requirements. Responsible for integration and implementation of the computer system security solution.

**Minimum Educational Requirements:** Bachelor’s degree in related field such as Computer Science, Computer Engineering, Information Assurance, etc. and applicable discipline certification such as CISSP, CCNA, CCNP,  RHCSA, RHCE, GPEN, GSEC, MCSD, MCSA, OCA, OCP, OCE, etc.

## HIT IT Specialist II

**Minimum/General Experience and Years of Experience:** 7 years relevant IT, cybersecurity, and/or Health IT experience.

**Functional Responsibility in one or more of the following areas**: Database design or Information Assurance or application design or enterprise architecture or disaster recovery, or configuration management or forensic intrusion analysis or network analysis in Health IT. Applying a business wide set of disciplines for planning, analysis, design, construction, and maintenance of Health IT systems business wide or across a major sector of the business. Gathering and organizing technical information about an organization's mission goals and needs, existing security products, connected health information, health management workflows, and ongoing programs in the MLS arena. Performing risk analysis, which include risk assessment. Experience developing health-related applications using advanced technologies, such as Internet protocols or web-based technology to include HTML, CGI applications, PERL or JavaScript, and Java. Develop, manage, maintain, and evaluate state-of-the-art computer hardware, software, and software development tools; evaluate their ability to support specific requirements and interface with other equipment and systems; determine potential and actual bottlenecks and propose recommendations for their elimination; and make recommendations for system improvements that will result in optimal hardware and software use. Analysis and definition of security requirements for multilevel security (MLS) issues. Designs, develops, engineers, and implements solutions to MLS requirements. Designs, develops, engineers, and implements solutions that meet security requirements. Responsible for integration and implementation of the computer system security solution. Gathers and organizes technical information about an organization's mission goals and needs, existing security products, and ongoing programs in computer security. Performs risk analyses of computer systems and applications during all phases of the system development life cycle.

**Minimum Educational Requirements:** Bachelor's degree in related field such as Computer Science, Computer Engineering, Information Assurance, etc. and applicable discipline certification such as CISSP, CCNA, CCNP, RHCSA, RHCE, GPEN, GSEC, MCSD, MCSA, OCA, OCP, OCE, etc.

## HIT IT Specialist III

**Minimum/General Experience and Years of Experience:** 10 years relevant IT, cybersecurity, and/or Health IT experience.

**Functional Responsibility in one or more of the following areas:** Database design or Information Assurance or application design or enterprise architecture or disaster recovery, or configuration management or forensic intrusion analysis or network analysis in Health IT. Applying a business wide set of disciplines for planning, analysis, design, construction, and maintenance of Health IT systems business wide or across a major sector of the business. Gathering and organizing technical information about an organization's mission goals and needs, existing security products, connected health information, health management workflows, and ongoing programs in the MLS arena. Performing risk analysis, which include risk assessment. Experience developing health-related applications using advanced technologies, such as Internet protocols or web-based technology to include HTML, CGI applications, PERL or JavaScript, and Java. Develop, manage, maintain, and evaluate state-of-the-art computer hardware, software, and software development tools; evaluate their ability to support specific requirements and interface with other equipment and systems; determine potential and actual bottlenecks and propose recommendations for their elimination; and make recommendations for system improvements that will result in optimal hardware and software use. Leads the analysis and definition of security requirements for multilevel security (MLS) issues. Designs, develops, engineers, and implements solutions to MLS requirements. Designs, develops, engineers, and implements solutions that meet security requirements. Leads the integration and implementation of the computer system security solution. Leads the reforms risk analyses of computer systems and applications during all phases of the system development life cycle.

**Minimum Educational Requirements:** MA/MS or Bachelor's degree in related field such as Computer Science, Computer Engineering, Information Assurance, etc. and applicable discipline certification such as CISSP, CCNA, CCNP, RHCSA, RHCE, GPEN, GSEC, MCSD, MCSA, OCA, OCP, OCE, etc.

## HIT Junior IT Specialist

**Minimum/General Experience and Years of Experience:** 1 year relevant IT and Health IT experience.

**Functional Responsibility in one or more of the following areas:** Database administration or Information Assurance or configuration management or software development or system administration in Health IT. Analyzes security and software requirements for networks and systems. Designs, develops, engineers, and implements Health IT solutions that meet network, application, software, or security requirements including systems for information exchanges and health analytics, personal health information management, and connected health. Responsible for integration and implementation of the network security solution. Performs vulnerability/risk analyses of computer systems and applications during all phases of the system development life cycle.

**Minimum Educational Requirements:** High School diploma

**Certification Requirements:** Applicable discipline certification such as Security+, CCNA-Security, GSEC, CEH, etc.

# LABOR CATEGORY DESCRIPTIONS FOR SIN 54151HACS HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS)

## HACS Program Manager I

**Minimum/General Experience and Years of Experience:** 5 years technical experience with at least 2 years managing complex IT, Cybersecurity, and/or Health IT programs.

**Functional Responsibility:** Performs overall management of contract support operations in a wide range of areas such as the seven-step Risk Management Framework (RMF) 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 focusing in the specific areas of Risk and Vulnerability Assessment and Penetration Testing, possibly involving multiple projects or groups. Organizes, directs, and coordinates the planning and production of all contract support activities. Provides technical guidance and project management functions associated with client requirements including but not limited to: technical management of projects; budget monitoring; personnel recruitment to support client; and assistance in the development and writing of client work plans. PMs not only have responsibility for managing projects in cybersecurity, but also possess strong technical skills. Must be capable of leading projects that involve the successful management of teams composed cybersecurity and other information management professionals who have been involved in securing, assessing, analysis, design, integration, testing, documenting, converting, extending, and implementing cybersecurity services for automated information and/or telecommunications systems.

**Minimum Educational Requirements:** A Bachelor's degree in Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## HACS Program Manager II

**Minimum/General Experience and Years of Experience:** 10 years technical experience with at least 5 years managing complex IT, Cybersecurity, and/or Health IT programs.

**Functional Responsibility:** Performs overall management of contract support operations in a wide range of areas such as the seven-step Risk Management Framework (RMF) 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 focusing in the specific areas of Risk and Vulnerability Assessment and Penetration Testing, possibly involving multiple projects or groups. Organizes, directs, and coordinates the planning and production of all contract support activities. Provides technical guidance and project management functions associated with client requirements including but not limited to: technical management of projects; budget monitoring; personnel recruitment to support client; and the development and writing of client work plans. PMs are senior personnel who not only have responsibility for managing cybersecurity projects, but also possess strong technical skills. Must be capable of leading projects that involve the successful management of teams composed of cybersecurity and other information management professionals who have been involved in securing, assessing, analysis, design, integration, testing, documenting, converting, extending, and implementing cybersecurity services for automated information and/or telecommunication systems.

**Minimum Educational Requirements:** A Bachelor's degree in Computer Science, Information Systems, and Engineering, Business or other related scientific, project or technical discipline.

## HACS Program Manager III

**Minimum/General Experience and Years of Experience:** 15 years technical experience with at least 8 years managing complex IT, Cybersecurity, and/or Health IT programs.

**Functional Responsibility:** Performs overall management of contract support operations in a wide range of areas such as the seven-step Risk Management Framework (RMF) 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 focusing in the specific areas of Risk and Vulnerability Assessment and Penetration Testing, possibly involving multiple projects or groups. Organizes, directs, and coordinates the planning and production of all contract support activities. Provides technical guidance and project management functions associated with client requirements, including but not limited to: technical management of projects; budget monitoring; personnel recruitment to support client; and the development and writing of client work plans. This professional manages multiple programs. PMs are senior personnel who not only have responsibility for managing projects in cybersecurity, but also possess strong technical skills. Must be capable of leading projects that involve the successful management of teams composed of cybersecurity and other information management professionals who have been involved in securing, assessing, analysis, design, integration, testing, documenting, converting, extending, and implementing cybersecurity services for automated information and/or telecommunications systems.

**Minimum Educational Requirements:** MA/MS degree in Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## HACS Program Manager IV

**Minimum/General Experience and Years of Experience:** 15+ years technical experience with at least 10 years managing complex IT, Cybersecurity, and/or Health IT programs.

**Functional Responsibility:** Performs overall management of contract support operations in a wide range of areas such as the seven-step Risk Management Framework (RMF) 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 focusing in the specific areas of Risk and Vulnerability Assessment and Penetration Testing, possibly involving multiple projects or groups. Organizes, directs, and coordinates the planning and production of all contract support activities. Provides technical guidance and project management functions associated with client requirements, including but not limited to: technical management of projects; budget monitoring; personnel recruitment to support client; and the development and writing of client work plans. This professional manages multiple programs. PMs are senior personnel who not only have responsibility for managing cybersecurity projects, but also possess strong technical skills. These senior personnel are renowned experts in either functional domains (e.g., finance, personnel, acquisition, etc.) or technical disciplines (e.g., RMF/A&A, penetration testing, incident response, network management, etc.) with many years of experience. They generally have advanced degrees and extensive experience as technical leaders and/or senior Project Managers. Must be capable of leading projects that involve the successful management of teams composed of cybersecurity professionals who have been involved in securing, assessing, analysis, design, integration, testing, documenting, converting, extending, and implementing cybersecurity services for automated information and/or telecommunications systems.

**Minimum Educational Requirements:** MA/MS degree in Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## HACS Project Manager I

**Minimum/General Experience and Years of Experience:** 5 years technical experience with at least 2 years managing IT, cybersecurity, and/or Health IT projects.

**Functional Responsibility:** Responsible for the overall management of assigned project task orders in a wide range of areas such as the seven-step Risk Management Framework (RMF) 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 focusing in the specific areas of Risk and Vulnerability Assessment and Penetration Testing; and for ensuring that the technical solutions in specific delivery orders are implemented in a timely manner. Organizes, directs, and coordinates the cybersecurity resources and planning of all task related activities associated with assigned delivery order projects. Provides technical guidance and project management functions associated with client requirements, and may manage cybersecurity IT projects.

**Minimum Educational Requirements:** A Bachelor's degree in Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## HACS Project Manager II

**Minimum/General Experience and Years of Experience:** 10 years technical experience with at least 5 years managing IT, cybersecurity, and/or Health IT projects.

**Functional Responsibility:** Responsible for the overall management of assigned project task orders in a wide range of areas such as the seven-step Risk Management Framework (RMF) 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 focusing in the specific areas of Risk and Vulnerability Assessment and Penetration Testing; and for ensuring that the technical solutions in specific delivery orders are implemented in a timely manner. Organizes, directs, and coordinates the cybersecurity resources and planning of all task related activities associated with assigned delivery order projects. Provides technical guidance and project management functions associated with client requirements, and may manage cybersecurity IT projects.

**Minimum Educational Requirements:** A Bachelor's degree in Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## HACS Project Manager III

**Minimum/General Experience and Years of Experience:** 15 years technical experience with at least 8 years managing IT and Health IT projects.

**Functional Responsibility:** Responsible for the overall management of assigned project task orders in a wide range of areas such as the seven-step Risk Management Framework (RMF) 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 focusing in the specific areas of Risk and Vulnerability Assessment and Penetration Testing; and for ensuring that the technical solutions in specific delivery orders are implemented in a timely manner. Organizes, directs, and coordinates the cybersecurity resources and planning of all task related activities associated with assigned delivery order projects.

Provides technical guidance and project management functions associated with client requirements, and may manage cybersecurity IT projects.

**Minimum Educational Requirements:** MA/MS degree in Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## HACS Subject Matter Expert I

**Minimum/General Experience and Years of Experience:** At least 3 years of combined new and related older technical experience in the IT and Health IT field 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 simple to moderately complex cybersecurity services for IT 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; Risk Management Framework (RMF); incident handling; vulnerability assessment and penetration testing; virus detection; network management; secure web hosting and backup; security services; Security Operations Center (SOC); security policy and implementation; develops; and secure software development methodologies.

**Minimum Educational Requirements:** Associates Degree in a project related field such as Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## HACS Subject Matter Expert II

**Minimum/General Experience and Years of Experience:** At least 7 years of combined new and related older technical experience in the IT and Health IT field directly related to the required area of expertise.

**Functional Responsibility:** Defines the problems and analyzes and develops plans and requirements in the subject matter area for moderately complex to complex cybersecurity services for IT systems. Coordinates and manages the preparation of analysis, evaluations, and recommendations for proper implementation of programs and systems specifications in the following specialties: information systems architecture; Risk Management Framework (RMF); incident handling; vulnerability assessment and penetration testing; virus detection; network management; secure web hosting and backup; security services; Security Operations Center (SOC); security policy and implementation; develops; and secure software development methodologies.

**Minimum Educational Requirements:** Associates Degree in a project related field such as Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## HACS Subject Matter Expert III

**Minimum/General Experience and Years of Experience:** At least 10 years of combined new and related older technical experience in the IT, cybersecurity, and/or Health IT field directly related to the required area of expertise.

**Functional Responsibility:** Provides technical, managerial, and administrative direction for problem definition, analysis, requirements development and implementation for complex to extremely complex cybersecurity services for IT systems in the subject matter area. Makes recommendations and advises on organization-wide system improvements, optimization or maintenance efforts in the following specialties: information systems architecture; Risk Management Framework (RMF); incident handling; vulnerability assessment and penetration testing; virus detection; network management; secure web hosting and backup; security services; Security Operations Center (SOC); security policy and implementation; develops; and secure software development methodologies.

**Minimum Educational Requirements:** BA/BS Degree in Business or project related field such as Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## HACS Subject Matter Expert IV

**Minimum/General Experience and Years of Experience:** 15 years of combined new and related older technical experience in the IT, cybersecurity, and/or Health IT field directly related to the required area of expertise.

**Functional Responsibility:** Applies their advanced skills and experience in secure systems development, detailed knowledge of business processes, technical background and supervisory skills to implement business solutions. Provides technical, managerial, and administrative direction for problem definition, analysis, requirements development and implementation for complex to extremely complex cybersecurity services for IT systems in the subject matter area. Makes recommendations and advises on organization-wide system improvements, optimization or maintenance efforts in the following specialties: information systems architecture; Risk Management Framework (RMF); incident handling; vulnerability assessment and penetration testing; virus detection; network management; secure web hosting and backup; security services; Security Operations Center (SOC); security policy and implementation; develops; and secure software development methodologies.

**Minimum Educational Requirements:** BA/BS Degree in Business or project related field such as Computer Science, Information Systems, Engineering, Business or other related scientific, project or technical discipline.

## HACS Technical Writer

**Minimum/General Experience and Years of Experience:** 2 years relevant IT, cybersecurity, and Health IT experience.

**Functional Responsibility:** Assists in collecting and organizing information for preparation of RMF artifacts, incident report write ups, cyber policy documents, user manuals, training materials, installation guides, proposals, and reports. Edit functional descriptions, system specifications, user manuals, special reports, or any other customer deliverable or document. Assists in performing financial and administrative functions. Must demonstrate the ability to work independently or under only general direction..

**Minimum Educational Requirements:** BA/BS Degree in English, Technical Writing or other writing related field.

## HACS IT Specialist I

**Minimum/General Experience and Years of Experience:** 3 years relevant IT, cybersecurity, and/or Health IT experience.

**Functional Responsibility in one or more of the following areas:** Secured database design or Information Assurance or secured application design or enterprise architecture or disaster recovery, or configuration management or forensic intrusion analysis or network analysis in IT systems. Applying a business wide set of disciplines for planning, analysis, design, securing, monitoring, testing, construction, and maintenance of information systems business wide or across a major sector of the business. Gathering and organizing technical information about an organization's mission goals and needs, existing security products and processes, and ongoing programs in the MLS arena. Performing risk analysis, which include risk assessment. Experience developing secure applications using secure coding best practices and advanced technologies, such as Internet protocols or web-based technology to include HTML, CGI applications, PERL or JavaScript, and Java. Develop, manage, maintain, secure and evaluate state-of-the-art computer hardware, software, and software development tools; evaluate their ability to support specific requirements within the Risk Management Framework (RMF) requirements and interface with other equipment and systems; determine potential and actual bottlenecks and propose recommendations for their elimination; and make recommendations for system improvements and vulnerability remediation that will result in optimal hardware and software use. Analysis and definition of security requirements for multilevel security (MLS) issues. Designs, develops, engineers, and implements solutions to MLS requirements. Analyzes and defines security requirements for computer systems, which may include mainframes, workstations, and personal computers. Designs, develops, engineers, and implements solutions to security requirements for applications, networks, and Security Operations Centers (SOCs). Responsible for integration and implementation of the computer system security solution including applicable steps of the RMF process.

**Minimum Educational Requirements:** Bachelor’s degree in related field such as Computer Science, Computer Engineering, Information Assurance, etc. and applicable discipline certification such as CISSP, CCNA, CCNP, RHCSA, RHCE, GPEN, GSEC, MCSD, MCSA, OCA, OCP, OCE, etc.

## HACS IT Specialist II

**Minimum/General Experience and Years of Experience:** 7 years relevant IT, cybersecurity, and/or Health IT experience.

**Functional Responsibility in one or more of the following areas**: Secured database design or Information Assurance or secured application design or enterprise architecture or disaster recovery, or configuration management or forensic intrusion analysis or network analysis in IT systems. Applying a business wide set of disciplines for planning, analysis, design, securing, monitoring, testing, construction, and maintenance of information systems business wide or across a major sector of the business. Gathering and organizing technical information about an organization's mission goals and needs, existing security products and processes, and ongoing programs in the MLS arena. Performing risk analysis, which include risk assessment and performing applicable steps of the RMF process to gain and/or maintain system accreditations. Experience developing secure applications using secure coding best practices and advanced technologies, such as Internet protocols or web-based technology to include HTML, CGI applications, PERL or JavaScript, and Java. Develop, manage, maintain, and evaluate state-of-the-art computer hardware, software, and software development tools; evaluate their ability to support specific requirements within the RMF and interface with other equipment and systems; determine potential and actual bottlenecks and propose recommendations for their elimination; and make recommendations for system improvements and vulnerability remediation steps that will result in optimal hardware and software use and security. Analysis and definition of security requirements for multilevel security (MLS) issues. Designs, develops, engineers, and implements solutions to MLS requirements. Designs, develops, engineers, and implements solutions that meet security requirements for applications, networks, and Security Operations Centers (SOCs). Responsible for integration and implementation of the computer system security solution including applicable steps of the RMF process. Gathers and organizes technical information about an organization’s mission goals and needs, existing security products, POA&M, and ongoing programs in computer security. Performs risk analyses of computer systems and applications during all phases of the system development life cycle.

**Minimum Educational Requirements:** Bachelor’s degree in related field such as Computer Science, Computer Engineering, Information Assurance, etc. and applicable discipline certification such as CISSP, CCNA, CCNP, RHCSA, RHCE, GPEN, GSEC, MCSD, MCSA, OCA, OCP, OCE, etc.

## HACS IT Specialist III

**Minimum/General Experience and Years of Experience:** 10 years relevant IT, cybersecurity, and/or Health IT experience.

**Functional Responsibility in one or more of the following areas:** Secured database design or Information Assurance or secured application design or enterprise architecture or disaster recovery, or configuration management or forensic intrusion analysis or network analysis in IT systems. Applying a business wide set of disciplines for planning, analysis, design, securing, monitoring, testing, construction, and maintenance of information systems business wide or across a major sector of the business. Gathering and organizing technical information about an organization's mission goals and needs, existing security products and processes, and ongoing programs in the MLS arena. Performing risk analysis, which include risk assessment and performing applicable steps of the RMF process to gain and/or maintain system accreditations. Experience developing secure applications using secure coding best practices and advanced technologies, such as Internet protocols or web-based technology to include HTML, CGI applications, PERL or JavaScript, and Java. Develop, manage, maintain, and evaluate state-of-the-art computer hardware, software, and software development tools; evaluate their ability to support specific requirements within the RMF and interface with other equipment and systems; determine potential and actual bottlenecks and propose recommendations for their elimination; and make recommendations for system improvements and vulnerability remediation steps that will result in optimal hardware and software use and security. Leads the analysis and definition of security requirements for multilevel security (MLS) issues. Designs, develops, engineers, and implements solutions to MLS requirements. Designs, develops, engineers, and implements solutions that meet security requirements for applications, networks, and Security Operations Centers (SOCs). Leads the integration and implementation of the computer system security solution including applicable steps of the RMF process. Gathers and organizes technical information about an organization's mission goals and needs, existing security products, POA&M, and ongoing programs in computer security. Leads risk analyses of computer systems and applications during all phases of the system development life cycle.

**Minimum Educational Requirements:** MA/MS or Bachelor's degree in related field such as Computer Science, Computer Engineering, Information Assurance, etc. and applicable discipline certification such as CISSP, CCNA, CCNP, RHCSA, RHCE, GPEN, GSEC, MCSD, MCSA, OCA, OCP, OCE, etc.

## HACS Junior Cyber Specialist

**Minimum/General Experience and Years of Experience:** 1 year relevant IT experience.

**Functional Responsibility in one or more of the following areas:** Network Security design or Information Assurance or forensic intrusion analysis. Analyzes and defines security requirements for local and wide area networks. Designs, develops, engineers, and implements solutions that meet network and/or application security requirements according to Risk Management Framework (RMF) guidance. Responsible for integration and implementation of the network and application security solution. Performs vulnerability/risk analyses and remediation of computer systems and applications during all phases of the system development life cycle.

**Minimum Educational Requirements:** High School diploma

**Certification Requirements:** Applicable discipline certification such as Security+, CCNA-Security, GSEC, CEH, etc.