AUTHORIZED FEDERAL SUPPLY SERVICE
INFORMATION TECHNOLOGY SCHEDULE PRICELIST
GENERAL PURPOSE COMMERCIAL INFORMATION TECHNOLOGY
EQUIPMENT, SOFTWARE AND SERVICES

Cyber Defense Technologies, LLC
22375 Broderick Drive, #115, Dulles, VA 20166
www.cyberdefensetechnologies.com | (Tel) 800.658.1846
Contract Administrator: William Kimble | William.Kimble@cyberdefensetechnologies.com
Business Size Status: Small Business Concern/SDVOSB.

General Services Administration
Contract Number: 47QTCA20D006K
Period Covered by Contract: 2/25/2020 – 2/24/2025
Pricelist current through Modification: A826.
Schedule Title: Multiple Award Schedule
Large Category: Information Technology
PSCs for Associated SINs: D310, D399

Online 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 for GSA Advantage! is: GSAAdvantage.gov.

For more information on ordering from Federal Supply Schedules click on the FSS Schedules button at fss.gsa.gov. Online access to contract ordering information, terms and conditions, up to date pricing, and the option to create an electronic delivery order are available through GSA Advantage!, a menu driven database system. The INTERNET address GSA Advantage! is: GSAAdvantage.gov.

For more information on ordering from Federal Supply Schedules click on the FSS Schedules button at fss.gsa.gov, Contract period.
Table of Contents
CUSTOMER INFORMATION............................................................................................................................................................. 3
TERMS AND CONDITIONS APPLICABLE TO HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS) (SPECIAL ITEM NUMBERS 54151HACS) ..................................................................................................................................................................... 5
TERMS AND CONDITIONS IT PROFESSIONAL SERVICES (SPECIAL ITEM NUMBER 54151S).................................................. 12
CUSTOMER INFORMATION

1a. Table of awarded special item numbers with appropriate cross-reference to item descriptions and awarded prices.

SIN 54151HACS and 54151S see Terms and Conditions.

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

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

See Terms and Conditions.

2. Maximum order. SIN 54151HACS and 54151S - $500,000

3. Minimum order. $100.00

4. Geographic coverage (delivery area). CONUS

5. Points of production (city, county, and State or foreign country). Same as Contractor Address

6. Discount from list prices or statement of net price. 2% - 7% from list price

7. Quantity discounts. None

8. Prompt payment terms. Note: Prompt payment terms must be followed by the statement "Information for Ordering Offices: Prompt payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions." 0.0% Discount

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

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

10. Foreign items (list items by country of origin). None

11a. Time of delivery. (Contractor insert number of days.) Negotiate with Contractor at task order level.

11b. Expedited Delivery. The Contractor will insert the sentence "Items available for expedited delivery are noted in this price list." under this heading. The Contractor may use a symbol of its choosing to highlight items in its price lists that have expedited delivery. Customer may contact the Contractor for expedited delivery

11c. Overnight and 2-day delivery. The Contractor will indicate whether overnight and 2-day delivery are available. Also, the Contractor will indicate that the schedule customer may contact the Contractor for rates for overnight and 2-day delivery. Customer may contact the Contractor for rates for overnight and 2-day delivery.
11d. Urgent Requirements. The Contractor will note in its price list the “Urgent Requirements” clause of its contract and advise agencies that they can also contact the Contractor’s representative to effect a faster delivery.

Customer may contact the Contractor to effect a faster delivery

12. F.O.B. point. N/A - Services

13a. Ordering address. Same as Contractor address

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

14. Payment address. Same as Contractor address

15. Warranty provision. Standard

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

17. Terms and conditions of Government purchase card acceptance (any thresholds above the micro-purchase level). N/A

18. Terms and conditions of rental, maintenance, and repair. N/A

19. Terms and conditions of installation. N/A

20. Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices. N/A

20a. Terms and conditions for any other services. N/A

21. List of service and distribution points. N/A

22. List of participating dealers. N/A

23. Preventive maintenance. N/A

24a. Special attributes such as environmental attributes. N/A

24b. If applicable, indicate that Section 508 compliance information is available on Electronic and Information Technology (EIT) supplies and services and show where full details can be found (e.g. contractor’s website or other location.) The EIT standards can be found at: www.Section508.gov/.

25. Data Universal Number System (DUNS) number. 033454696

26. Notification regarding registration is registered in the System for Award Management (SAM) Database. 7K6K4
Vendor suitability for offering services through the Highly Adaptive Cybersecurity Services (HACS) SIN must be in accordance with the following laws and standards when applicable to the specific task orders, including but not limited to:

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

1. SCOPE  
a. The labor categories, prices, terms and conditions stated under Special Item Number 132-45 Highly Adaptive Cybersecurity Services (HACS) apply exclusively to Highly Adaptive Cybersecurity Services within the scope of this Information Technology Schedule.  
b. 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. 132-32, 132-33, 132-8), and may be quoted along with services to provide a total solution.  
c. This SIN provides ordering activities with access to Highly Adaptive Cybersecurity services only.  
d. Highly Adaptive Cybersecurity Services provided under this SIN shall comply  
   with all Cybersecurity certifications and industry standards as applicable pertaining to the type of services as specified by ordering agency.  

e. SCOPE:  

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

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 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.

4. INSPECTION OF SERVICES

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

5. RESPONSIBILITIES OF THE CONTRACTOR

The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character. If the end product of a task order is software, then FAR 52.227-14 (May 2014) Rights in Data – General, may apply.

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

6. RESPONSIBILITIES OF THE ORDERING ACTIVITY

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

7. INDEPENDENT CONTRACTOR

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

8. ORGANIZATIONAL CONFLICTS OF INTEREST
a. Definitions.

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

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

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

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

9. INVOICES

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

10. RESUMES

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

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

12. DESCRIPTION OF HIGHLY ADAPTIVE CYBERSECURITY SERVICES AND PRICING

a. The Contractor shall provide a description of each type of Highly Adaptive Cybersecurity Service offered under Special Item Number 54151HACS for Highly Adaptive Cybersecurity Services and it should be presented in the same manner as the Contractor sells to its commercial and other ordering activity customers. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles (labor categories) for those individuals who will perform the service should be provided.

b. Pricing for all Highly Adaptive Cybersecurity Services shall be in accordance with the Contractor’s customary commercial practices; e.g., hourly rates, minimum general experience and minimum education.
1. SCOPE

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

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

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

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.

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

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

3. ORDER

Agencies may use written orders, EDI 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.

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

4. PERFORMANCE OF SERVICES

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

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

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

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

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

Cancel the stop-work order; or

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

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

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

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

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

6. INSPECTION OF SERVICES


7. RESPONSIBILITIES OF THE CONTRACTOR

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

8. RESPONSIBILITIES OF THE ORDERING ACTIVITY

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

9. INDEPENDENT CONTRACTOR

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

10. ORGANIZATIONAL CONFLICTS OF INTEREST

Definitions.

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

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

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

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

11. INVOICES

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

12. PAYMENTS

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

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

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

The offeror;

Subcontractors; and/or

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

13. RESUMES

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

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

15. APPROVAL OF SUBCONTRACTS

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

16. DESCRIPTION OF IT PROFESSIONAL SERVICES AND PRICING
### Labor Categories

**SIN 54151HACS**

**Title:** Cyber Program Manager V

**Functional Duties/Responsibilities:** Responsible for the initiation, scope planning (including decomposing work effort into work packages), resource assignment, team technical/schedule/cost delivery performance, monitoring and reporting, change management, and project close for a defined Cyber project. Engages external clients and internal resources and management for all items related to the Cyber program. May provide Cyber and/or business insights and guidance to the delivery team to resolve complex challenges. May have responsibility for the oversight of multiple concurrent Cyber projects or programs.

**Minimum Education:** A Master’s degree in Computer Science, Engineering, or Information Technology/Operations Management, or an equivalent technical degree. Bachelor’s degree requires two (2) additional years of minimum experience. Non-technical degrees must be supplemented by various technical Cyber certifications.

**Minimum Experience Requirements:** Technically-degreed individuals must have ten (10) years of overall experience which exhibit increasing levels of responsibility including eight (8) years of Cyber-specific Program Manager experience. Non-technically degreed individuals must have twelve (12) years of Cyber-specific experience.

**Required/Supplemental Certifications:** Advanced technical Cyber certifications in aggregate equivalent to a CISSP, CISM or GSLC or related. Advanced knowledge of PMBOK required, Project Management Professional (PMP) preferred.

---

**Title:** Cyber Project Manager III

**Functional Duties/Responsibilities:** Responsible for the initiation, scope planning (including decomposing work effort into work packages), resource assignment, team technical/schedule/cost delivery performance, monitoring and reporting, change management and project close for a defined Cyber project. Engages external clients and internal resources and management for all items related to the Cyber program. May provide Cyber and business insights and guidance to the delivery team to resolve complex challenges. Project Manager may be responsible for the oversight of multiple concurrent Cyber projects or programs.

**Minimum Education:** A Bachelor’s degree in Computer Science, Engineering, or Information Technology/Operations Management, or an equivalent technical degree. Master’s degree requires two (2) less years of minimum experience. Non-technical degrees must be supplemented by various technical Cyber certifications.

**Minimum Experience Requirements:** Technically-degreed individuals must have six (6) years of overall experiences which exhibit increasing levels of responsibility including four (4) years of Cyber-specific experience. Non-technically degreed individuals must have ten (10) years of Cyber-specific Project Manager experience.

**Required/Supplemental Certifications:** Multiple advanced technical Cyber certifications (e.g. CISSP, CISM, GSLC) required. Working knowledge of PMBOK required, Project Management Professional (PMP) preferred.
Title: Cyber Project Manager II

**Functional Duties/Responsibilities:** Responsible for the initiation, scope planning (including decomposing work effort into work packages), resource assignment, team technical/schedule/cost delivery performance, monitoring and reporting, change management and project close for a defined Cyber project. Engages external clients and internal resources and management for all items related to the Cyber program. May provide Cyber and business insights and guidance to the delivery team to resolve complex challenges. Project Manager may be responsible for the oversight of several concurrent Cyber projects or programs.

**Minimum Education:** A Bachelor’s degree in Computer Science, Engineering, or Information Technology/Operations Management, or an equivalent technical degree. Master’s degree requires two (2) less years of minimum experience. Non-technical degrees must be supplemented by various technical Cyber certifications.

**Minimum Experience Requirements:** Technically-degreed individuals must have four (4) years of overall experiences which exhibit increasing levels of responsibility including two (2) years of Cyber-specific Project Manager experience. Non-technically degreed individuals must have eight (8) years of Cyber-specific experience.

**Required/Supplemental Certifications:** An advanced technical Cyber certification required (e.g. CISSP, CISM, GSLC). Understanding of PMBOK required, Project Management Professional (PMP) desired.

Title: Emergency Cyber Engineer

**Functional Duties/Responsibilities:** Provide expert, on-demand emergency, triage or other immediate services to implement or remediate a broad range of Cyber-related technical issues including Vulnerability and Malware Analysis, System Security Hardening including Security Technical Implementation Guidelines (STIG) Digital Forensics and Incident Response (DFIR), as well as No-Notice Cyber Command Readiness Inspections (CCRI) on a strict timeline basis. Engages customer technical POCs as necessary to trouble-shoot issues and identify/implement resolutions.

**Minimum Education:** A Bachelor’s degree in Computer Science, Engineering, or Information Technology/Operations Management, or an equivalent technical degree. Master’s degree requires two (2) less years of minimum experience. Non-technical degrees must be supplemented by various technical Cyber certifications. An Associate degree must be supplemented by various technical Cyber certifications and two (2) additional years of experience beyond the Minimum Experience Requirements. The absence of a degree must be supplemented by various technical Cyber certifications and four (4) additional years of experience beyond the Minimum Experience Requirements.

**Minimum Experience Requirements:** Individuals must possess five (5) years of hands-on Cyber-specific experience.
Required/Supplemental Certifications: One or more technical certifications such as DOD 8570 IAT Level I or technology-specific platforms (e.g. CISCO, VMWare, Microsoft, etc.) as necessary to perform the specific Cyber emergency task.

---

Title: Exploitation Engineer SME

Functional Duties/Responsibilities: Lead vulnerability scans and penetration testing (e.g. Network, Web Application, Wireless) in support of Red/Blue or interactive Purple Teaming and report remediation recommendations to proactively maintain the security posture of an enterprise or perform as an individual contributor on complex testing projects. Author Rules of Engagement. Additional responsibilities may include social engineering and physical assessments. Engages customer technical POCs as necessary throughout testing and reporting. May require providing guidance and oversight of other exploitation engineers.

Minimum Education: Master’s degree in Computer Science, Engineering, Information Technology or relative technical discipline. Non-technical degrees must be supplemented by various technical Cyber certifications. A Bachelor’s or Associate degree must be supplemented by various technical Cyber certifications and four (4) or two (2) additional years of experience, respectively, beyond the Minimum Experience Requirements. The absence of a degree must be supplemented by various technical Cyber certifications and six (6) additional years of experience beyond the Minimum Experience Requirements.

Minimum Experience Requirements: Twelve (12) years of leading and performing information security-related engineering in areas such as: security operations, vulnerability management, security testing, system patching, log analysis, intrusion detection and security device technologies administration and incident analysis. Expert knowledge of Penetration Testing Execution Standard (PTES) and Open Web Application Security Project (OWASP) Frameworks and toolsets such as BurpSuite, NESSUS/ACAS, Kali Linux required. Custom scripting experience required. Advanced knowledge of one or more of the following compliance frameworks (RMF, PCI, HIPAA, IRS, CJIS).

Required/Supplemental Certifications: Multiple advanced Cyber certifications such as Certified Ethical Hacker (CEH), Licensed Penetration Tester (LPT), Offensive Security Certified Professional (OSCP), Offensive Certified Security Expert (OSCE), Offensive Certified Wireless Professional (OSWP), and other related credentials.

---

Title: Exploitation Engineer V

Functional Duties/Responsibilities: Lead vulnerability scans and penetration testing (e.g. Network, Web Application, Wireless) in support of Red/Blue or interactive Purple Teaming and report remediation recommendations to proactively maintain the security posture of an enterprise or perform as an individual contributor on complex testing projects. Author Rules of Engagement. Additional responsibilities may include social engineering and physical assessments. Engages customer technical POCs as necessary throughout testing and reporting. May require providing guidance and oversight of other exploitation engineers.

Minimum Education: Master’s degree in Computer Science, Engineering, Information Technology or relative technical discipline. Non-technical degrees must be supplemented by various technical Cyber certifications. A Bachelor’s or Associate degree must be supplemented by various technical Cyber certifications and four (4) or two (2) additional years of experience, respectively, beyond the Minimum Experience Requirements. The absence of a
degree must be supplemented by various technical Cyber certifications and six (6) additional years of experience beyond the Minimum Experience Requirements.

**Minimum Experience Requirements:** Ten (10) years of leading and performing information security-related engineering in areas such as: security operations, vulnerability management, security testing, system patching, log analysis, intrusion detection and security device technologies administration and incident analysis. Expert knowledge of Penetration Testing Execution Standard (PTES) and Open Web Application Security Project (OWASP) Frameworks and toolsets such as BurpSuite, NESSUS/ACAS, Kali Linux required. Custom scripting experience required.

**Required/Supplemental Certifications:** Multiple advanced Cyber certifications such as Certified Ethical Hacker (CEH), Licensed Penetration Tester (LPT), Offensive Security Certified Professional (OSCP), Offensive Certified Security Expert (OSCE), Offensive Certified Wireless Professional (OSWP), GIAC Security Essentials (GSEC), GIAC-Certified Intrusion Analyst (GCIA), GIAC-Certified Incident Handler (GCIH), Certified Information Systems Security Professional (CISSP), Security + and other related credentials.

---

**Title:** Exploitation Engineer IV

**Functional Duties/Responsibilities:** Lead vulnerability scans and penetration testing (e.g. Network, Web Application, Wireless) in support of Red/Blue or interactive Purple Teaming and report remediation recommendations to proactively maintain the security posture of an enterprise or perform as an individual contributor on complex testing projects. Author Rules of Engagement. Additional responsibilities may include social engineering and physical assessments. Engages customer technical POCs as necessary throughout testing and reporting. May require providing guidance and oversight of other exploitation engineers.

**Minimum Education:** Bachelor’s degree in Computer Science, Engineering, Information Technology or relative technical discipline. Non-technical degrees must be supplemented by various technical Cyber certifications. An Associate degree must be supplemented by various technical Cyber certifications and two (2) additional years of experience beyond the Minimum Experience Requirements. The absence of a degree must be supplemented by various technical Cyber certifications and four (4) additional years of experience beyond the Minimum Experience Requirements.

**Minimum Experience Requirements:** Eight (8) years of leading and performing information security-related engineering in areas such as: security operations, vulnerability management, security testing, system patching, log analysis, intrusion detection and security device technologies administration and incident analysis. Advanced knowledge of Penetration Testing Execution Standard (PTES) and Open Web Application Security Project (OWASP) Frameworks and toolsets such as BurpSuite, NESSUS/ACAS, Kali Linux required. Custom scripting experience required.

**Required/Supplemental Certifications:** Multiple Cyber certifications such as Certified Ethical Hacker (CEH), GIAC Security Essentials (GSEC), GIAC-Certified Intrusion Analyst (GCIA), GIAC Certified Incident Handler (GCIH), Certified Information Systems Security Professional (CISSP), Security + and other related credentials. Licensed Penetration Tester (LPT) or Offensive Security Certified Professional (OSCP) desired.

---

**Title:** Exploitation Engineer III
Functional Duties/Responsibilities: Perform or lead vulnerability scans and penetration testing (e.g. Network, Web Application, Wireless) in support of Red/Blue or interactive Purple Teaming and report remediation recommendations to proactively maintain the security posture of an enterprise. Additional responsibilities may include social engineering and physical assessments. Engages customer technical POCs as necessary throughout testing and reporting. May require providing guidance and oversight of other exploitation engineers.

Minimum Education: Bachelor’s degree in Computer Science, Engineering, Information Technology or relative technical discipline. Non-technical degrees must be supplemented by various technical Cyber certifications. An Associate degree must be supplemented by various technical Cyber certifications and two (2) additional years of experience beyond the Minimum Experience Requirements. The absence of a degree must be supplemented by various technical Cyber certifications and four (4) additional years of experience beyond the Minimum Experience Requirements.

Minimum Experience Requirements: Six (6) years of leading and performing information security-related engineering in areas such as: security operations, vulnerability management, security testing, system patching, log analysis, intrusion detection and security device technologies administration and incident analysis. Knowledge of Penetration Testing Execution Standard (PTES) and Open Web Application Security Project (OWASP) Frameworks and toolsets such as BurpSuite, NESSUS/ACAS, Kali Linux required. Custom scripting experience a plus.

Required/Supplemental Certifications: Multiple Cyber certifications such as Certified Ethical Hacker (CEH), GIAC Security Essentials (GSEC), GIAC-Certified Intrusion Analyst (GCIA), GIAC Certified Incident Handler (GCIH), Certified Information Systems Security Professional (CISSP), Security + and other related credentials.

Title: Exploitation Engineer II

Functional Duties/Responsibilities: Individually performs vulnerability scans and penetration testing (e.g. Network, Web Application, Wireless) or in support of a Red/Blue or interactive Purple Teaming activity and report remediation recommendations to proactively maintain the security posture of an enterprise. Additional responsibilities may include social engineering and physical assessments. May engage customer technical POCs as necessary throughout testing and reporting. May require providing guidance and oversight of other exploitation engineers.

Minimum Education: Bachelor’s degree in Computer Science, Engineering, Information Technology or relative technical discipline. Non-technical degrees must be supplemented by various technical Cyber certifications. An Associate degree must be supplemented by various technical Cyber certifications and two (2) additional years of experience beyond the Minimum Experience Requirements. The absence of a degree must be supplemented by various technical Cyber certifications and four (4) additional years of experience beyond the Minimum Experience Requirements.

Minimum Experience Requirements: Four (4) years leading or performing information security-related engineering in areas such as: security operations, vulnerability management, security testing, system patching, log analysis, intrusion detection and security device technologies administration and incident analysis. Understanding of Penetration Testing Execution Standard (PTES) and Open Web Application Security Project (OWASP) Frameworks and toolsets such as BurpSuite, NESSUS/ACAS, Kali Linux required. Custom scripting experience a plus.
Required/Supplemental Certifications: A Cyber certification such as Certified Ethical Hacker (CEH), GIAC Security Essentials (GSEC), GIAC-Certified Intrusion Analyst (GCIA), GIAC Certified Incident Handler (GCIH), Certified Information Systems Security Professional (CISSP), Security + and other related credentials.

Title: Incident Responder IV

Functional Duties/Responsibilities: Lead teams or proactively and/or reactively individually receive unique and/or complex anomalous security incidents from security engineers and/or SOC analysts and follow appropriate handling and response procedures to analyze data, review system and device audit logs for unauthorized intrusions or activities, identify root causes sustained by artifacts, devise potential triage solutions and report recommendations to stakeholders to re-establish the security posture of a technology or enterprise. Lead complex trend analysis initiatives across the enterprise. Recommend Process Improvements and lead implementations. Engages customer technical POCs as necessary throughout Incident Response. May require providing guidance and oversight of other Incident Responders.

Minimum Education: Bachelor’s degree in technical or non-technical discipline. Non-technical degrees must be supplemented by various technical Cyber certifications. An Associate degree must be supplemented by various technical Cyber certifications and two (2) additional years of experience beyond the Minimum Experience Requirements to be considered compliant. The absence of a degree must be supplemented by various technical Cyber certifications and three (3) additional years of experience beyond the Minimum Experience Requirements to be considered compliant.

Minimum Experience Requirements: Four (4) years leading and performing information security-related services in areas such as: security operations, system patching, log analysis, intrusion detection and security device technologies administration and incident analysis. Advanced knowledge of toolsets such as a SIEM, ACAS, HBSS or other SOC environment technologies required.

Required/Supplemental Certifications: Advanced Cyber certifications such as GIAC-Certified Incident Handler (GCIH), Security +, Network +, A+ and other related credentials.

Title: Incident Responder III

Functional Duties/Responsibilities: Lead teams or proactively and/or reactively individually receive anomalous security incidents from security engineers and/or SOC analysts and follow appropriate handling and response procedures to analyze data, review system and device audit logs for unauthorized intrusions or activities, identify root causes sustained by artifacts, devise potential triage solutions and report recommendations to stakeholders to re-establish the security posture of a technology or enterprise. Perform trend analysis initiatives across the enterprise. Recommend Process Improvements and lead implementations. Engages customer technical POCs as necessary throughout Incident Response. May require providing guidance and oversight of other Incident Responders.

Minimum Education: Bachelor’s degree in technical or non-technical discipline. Non-technical degrees must be supplemented by various technical Cyber certifications. An Associate degree must be supplemented by various
technical Cyber certifications and one (1) additional year of experience beyond the Minimum Experience Requirements. The absence of a degree must be supplemented by various technical Cyber certifications and two (2) additional years of experience beyond the Minimum Experience Requirements.

**Minimum Experience Requirements:** Three (3) years of performing information security-related services in areas such as: security operations, system patching, log analysis, intrusion detection and security device technologies administration and incident analysis. Knowledge of toolsets such as a SIEM, ACAS, HBSS or other SOC environment technologies required.

**Required/Supplemental Certifications:** Multiple Cyber certifications such as GIAC-Certified Incident Handler (GCIH), Security +, Network +, A+ and other related credentials.

---------------------------------------------------------------------------------------------------------------------

**Title:** SOC Analyst III

**Functional Duties/Responsibilities:** Lead teams of analysts to proactively monitor network/bandwidth traffic and/or performance and audit logs which prevents network attacks and/or reactively identify network intrusions and/or anomalous security incidents across the enterprise. Perform malware vulnerability scanning and network monitoring. Provide initial analysis, documentation artifacts and escalate incidents to Incident Responders for detailed analysis remediation recommendations. May conduct Cyber Hunt Teams. Perform advanced analysis of warning intelligence data. May individually perform these tasks as well as provide supplemental information and analysis for complex issues as required by Incident Responders to implement remediation actions which re-establish the security posture of a technology or enterprise. Lead advanced rule generation and/or trend analysis and correlation initiatives across the enterprise. Support the creation of operational policies and identify documentation and/or technology Process Improvements and support implementations. Engages customer technical POCs as necessary throughout SOC operations. Provide guidance and oversight of multiple individual SOC Analysts.

**Minimum Education:** Bachelor’s degree in technical or non-technical discipline. Non-technical degrees must be supplemented by various technical Cyber certifications. An Associate degree must be supplemented by various technical Cyber certifications and one (1) additional years of experience beyond the Minimum Experience. The absence of a degree must be supplemented by various technical Cyber certifications and two (2) additional years of experience beyond the Minimum Experience Requirements.

**Minimum Experience Requirements:** Three (3) years of leading and performing information security-related services in areas such as: security operations, system patching, log analysis, intrusion detection and security device technologies administration and incident analysis. Knowledge of toolsets such as a SIEM, ACAS, HBSS or other SOC environment technologies required.

**Required/Supplemental Certifications:** Advanced Cyber certifications such as GIAC-Certified Incident Handler (GCIH), Security +, Network +, A+ and other related credentials.

---------------------------------------------------------------------------------------------------------------------

**Title:** SOC Analyst II
**Functional Duties/Responsibilities:** Proactively monitor network/bandwidth traffic and/or performance and audit logs which prevents network attacks and/or reactively identify network intrusions and/or anomalous security incidents across the enterprise and/or support Level 1 Analysts doing similar. Perform and/or support malware vulnerability scanning and network monitoring. Provide initial analysis, documentation artifacts and escalate incidents to Incident Responders for detailed analysis remediation recommendations. May support Cyber Hunt Teams. Perform advanced analysis of warning intelligence data. May individually perform these tasks as well as provide supplemental information and analysis for complex issues as required by Incident Responders to implement remediation actions which re-establish the security posture of a technology or enterprise. Lead fundamental rule generation and/or trend analysis and correlation initiatives across the enterprise. Implement existing and champion newly created operational policies and identify documentation and/or technology Process Improvement initiatives. Engages customer technical POCs as necessary throughout SOC operations. Provide guidance and oversight of several individual SOC Analysts.

**Minimum Education:** Associate degree in technical or non-technical discipline. Non-technical degrees must be supplemented by various technical Cyber certifications. The absence of a degree must be supplemented by various technical Cyber certifications and one (1) additional years of experience beyond the Minimum Experience Requirements.

**Minimum Experience Requirements:** Two (2) years performing information security-related services in areas such as: security operations, system patching, log analysis, intrusion detection and security device technologies administration and incident analysis. Knowledge of toolsets such as a SIEM, ACAS, HBSS or other SOC environment technologies required.

**Required/Supplemental Certifications:** Advanced Cyber certifications such as GIAC-Certified Incident Handler (GCIH), Security +, Network +, A+ and other related credentials.

---

**Title:** SOC Analyst I

**Functional Duties/Responsibilities:** Proactively monitor network/bandwidth traffic and/or performance and audit logs which prevents network attacks and/or reactively identify network intrusions and/or anomalous security incidents across the enterprise. Perform malware vulnerability scanning and network monitoring. Provide initial analysis, documentation artifacts and escalate incidents to Incident Responders for detailed analysis remediation recommendations. Perform fundamental analysis of warning intelligence data. Provide supplemental information and analysis for basic issues as required by Incident Responders to implement remediation actions which re-establish the security posture of a technology or enterprise. Implement rule generation and/or perform basic trend analysis and correlation initiatives across the enterprise. Implement existing and newly created operational policies and support implementation of technology Process Improvement initiatives. Engages directly with the Program/Project Manager or higher level SOC Analyst as necessary throughout SOC operations.

**Minimum Education:** Associate degree in technical or non-technical discipline. Non-technical degrees must be supplemented by various technical Cyber certifications. The absence of a degree must be supplemented by various technical Cyber certifications and one (1) additional years of experience beyond the Minimum Experience Requirements compliant.

**Minimum Experience Requirements:** N/A
Required/Supplemental Certifications: N/A

Title: Information Assurance Engineer SME

Functional Duties/Responsibilities: Develop IA strategies. Perform and resolve the most complex and unique projects and problems across all phases of compliance analysis in information systems security at an expert level to achieve strategic outcomes. Break down and evaluate information systems compliance policies, program and regulation development. Expected to be a thought-leader in applying current compliance standards, current trends, and future states and how to effectively assess technical and non-technical controls and aspects across a wide variety of information system technologies. Engages customer technical POCs as necessary throughout IA activities. May provide supervisory guidance to lower level Information Assurance Engineers.

Minimum Education: Master’s degree in Computer Science, Engineering, or Information Technology, or relevant discipline. A Bachelor’s degree must be supplemented by the required Cyber certification and two (2) additional years of experience beyond the Minimum Experience Requirements. An Associate degree must be supplemented by the required Cyber certification and four (4) additional years of experience beyond the Minimum Experience Requirements. The absence of a degree must be supplemented by the required Cyber certification and six (6) additional years of experience.

Minimum Experience Requirements: Eleven (11) years leading and performing information assurance engineering and expert understanding of practical areas relating to and applying current compliance standards to advanced technological systems, concepts and analysis. Example experience includes previously performing as an Information System Officer or Certifying Authority Representative.

Required/Supplemental Certifications: An IAT Level III DoD 8570 compliant certification is also required if in lieu the degree listed above

Title: Information Assurance Engineer V

Functional Duties/Responsibilities: Develop IA strategies. Perform the most complex projects and resolve problems across all phases of compliance analysis in information systems security to achieve strategic outcomes. Break down and evaluate information systems compliance policies, program and regulation development. Expected to be an expert in applying current compliance standards, possess advanced knowledge of current trends, knowledgeable of future states and how to effectively assess technical and non-technical controls and aspects across a wide variety of information system technologies. Engages customer technical POCs as necessary throughout IA activities. May provide supervisory guidance to lower level Information Assurance Engineers.

Minimum Education: Master’s degree in Computer Science, Engineering, or Information Technology, or relevant discipline. A Bachelor’s degree must be supplemented. By the required Cyber certification and two (2) additional years of experience beyond the Minimum Experience Requirements. An Associate degree must be supplemented by the required Cyber certification and four (4) additional years of experience beyond the Minimum Experience Requirements.
Requirements. The absence of a degree must be supplemented by the required Cyber certification and six (6) additional years of experience and beyond the Minimal Experience Requirements.

**Minimum Experience Requirements:** Nine (9) years leading and performing information assurance engineering and expert understanding of practical areas relating to and applying current compliance standards to advanced technological systems, concepts and analysis. Example experience includes previously performing as an Information System Officer or Certifying Authority Representative.

**Required/Supplemental Certifications:** An IAT Level III DoD 8570 compliant certification is also required if in lieu the degree listed above.

---

**Title:** Information Assurance Engineer IV

**Functional Duties/Responsibilities:** Develop IA strategies. Perform complex projects and resolve problems across all phases of compliance analysis in information systems security to achieve strategic outcomes. Break down and evaluate information systems compliance policies, program and regulation development. Expected to be fully articulate in and applying current compliance standards, knowledgeable of current trends, cognizant of future states and how to effectively assess technical and non-technical controls and aspects across a wide variety of information system technologies. Engages customer technical POCs as necessary throughout IA activities. May provide supervisory guidance to lower level Information Assurance Engineers.

**Minimum Education:** Bachelor’s degree in Computer Science, Engineering, or Information Technology, or relevant discipline. An Associate degree must be supplemented by the required Cyber certification and two (2) additional years of experience beyond the Minimum Experience Requirements. The absence of a degree must be supplemented by the required Cyber certification and four (4) additional years of experience and beyond the Minimal Experience Requirements.

**Minimum Experience Requirements:** Seven (7) years of experience leading and performing information assurance engineering and an advanced understanding of practical areas relating to and applying current compliance standards to advanced technological systems, concepts and analysis. Example experience includes previously performing as an Information System Officer or Certifying Authority Representative.

**Required/Supplemental Certifications:** An IAT Level II DoD 8570 compliant certification is also required if in lieu the degree listed above.

---

**Title:** Information Assurance Engineer II

**Functional Duties/Responsibilities:** May develop IA strategies. Perform projects and resolve standard problems across all phases of compliance analysis in information systems security to achieve strategic outcomes. Break down and evaluate information systems compliance policies, program and regulation development. Expected to be conversant in and applying current compliance standards and how to effectively assess technical and non-technical controls and aspects across a wide variety of information system technologies. Engages customer technical POCs as necessary throughout IA activities. May provide supervisory guidance to lower level Information Assurance Engineers.
Minimum Education: Associate degree. The absence of a degree must be supplemented by the required Cyber certification and two (2) additional year of experience beyond the Minimal Experience Requirements.

Minimum Experience Requirements: Three (3) years of experience performing information assurance services and a firm understanding of practical areas relating to and applying current compliance standards to advanced technological systems, concepts and analysis. Example experience includes previously performing as an Information System Manager or Certifying Authority Representative.

Required/Supplemental Certifications: An IAT Level I DoD 8570 compliant certification is also required if in lieu the degree listed above.

Title: Information Assurance Engineer I

Functional Duties/Responsibilities: Perform fundamental projects and resolve basic problems across all phases of compliance analysis in information systems security domain. Break down and evaluate basic information systems compliance policies, program and regulation development. Expected to understand and apply current compliance standards. Interacts directly with the Program/Project Manager and or Lead IA Engineer.

Minimum Education: Associate degree. The absence of a degree must be supplemented by the required Cyber certification and one (1) additional year of experience beyond the Minimal Experience Requirements.

Minimum Experience Requirements: One (1) year of experience performing information assurance services and a firm understanding of practical areas relating to and applying current compliance standards to advanced technological systems, concepts and analysis.

Required/Supplemental Certifications: An IAT Level I DoD 8570 compliant certification is required.

SIN 54151S

Title: Project Manager V

Functional Duties/Responsibilities: Responsible for the initiation, scope planning (including decomposing work effort into work packages), resource assignment, team technical/schedule/cost delivery performance, monitoring and reporting, change management, and project close for a defined project. Engages external clients and internal resources and management of all items related to the program. May provide technical and business insights and guidance to the delivery team to resolve complex challenges. May have responsibility for the oversight of multiple concurrent projects or programs.

Minimum Education: A Bachelor’s degree in Engineering, Information Technology, Business Administration or equivalent. Master’s degree requires two (2) less years of minimum experience.

Minimum Experience Requirements: Twelve (12) years of overall professional experience which exhibit increasing levels of responsibility including eight (8) years of Project Management-specific experience.
**Required/Supplemental Certifications:** Technical certifications such as ITIL, Certified Scrum Master (CSM) or equivalent is required for applicable projects. Advanced knowledge of PMBOK required, Project Management Professional (PMP) preferred.

---

**Title:** Project Manager IV

**Functional Duties/Responsibilities:** Responsible for the initiation, scope planning (including decomposing work effort into work packages), resource assignment, the team’s technical/schedule/cost delivery performance, monitoring and reporting, change management and project close for a defined project. Engages external clients and internal resources and management of all items related to the program. May provide technical and business insights and guidance to the delivery team to resolve complex challenges. Project Manager will be responsible for the oversight of multiple concurrent projects or programs.

**Minimum Education:** A Bachelor’s degree in Engineering, Information Technology, Business Administration or equivalent. Master’s degree requires two (2) less years of minimum experience.

**Minimum Experience Requirements:** Must have ten (10) years of professional experience which exhibit increasing levels of responsibility including six (6) years of Project Management-specific experience.

**Required/Supplemental Certifications:** Technical certifications such as ITIL, Certified Scrum Master or equivalent is required for applicable projects. Knowledge of PMBOK required, Project Management Professional (PMP) preferred.

---

**Title:** Project Manager III

**Functional Duties/Responsibilities:** Responsible for the initiation, scope planning (including decomposing work effort into work packages), resource assignment, the team’s technical/schedule/cost delivery performance, monitoring and reporting, change management and project close for a defined project. Engages external clients and internal resources and management of all items related to the program. May provide technical and business insights and guidance to the delivery team to resolve complex challenges. Project Manager may be responsible for the oversight of multiple concurrent projects or programs.

**Minimum Education:** A Bachelor’s degree in Engineering, Information Technology, Business Administration or equivalent. Master’s degree requires two (2) less years of minimum experience.

**Minimum Experience Requirements:** Must have eight (8) years of professional experience which exhibit increasing levels of responsibility including four (4) years of Project Management-specific experience.

**Required/Supplemental Certifications:** Technical certifications such as ITIL, Certified Scrum Master (CSM) or equivalent is required for applicable projects. Working knowledge of PMBOK required, Project Management Professional (PMP) preferred.
Title: Project Manager I

Functional Duties/Responsibilities: Responsible for the initiation, scope planning (including decomposing work effort into work packages), resource assignment, the team’s technical/schedule/cost delivery performance, monitoring and reporting, change management and project close for a defined project. Engages external clients and internal resources and management of all items related to the program. May provide technical and business insights and guidance to the delivery team to resolve complex challenges.

Minimum Education: A Bachelor’s degree in Engineering, Information Technology, Business Administration or equivalent.

Minimum Experience Requirements: Must have four (4) years of professional experience which exhibit increasing levels of responsibility including two (2) years of Scrum Team, Team Lead or Deputy Project Management-specific experience.

Required/Supplemental Certifications: Technical certifications such as ITIL, Certified Scrum Master (CSM) or equivalent is required for applicable projects. Understanding of PMBOK required, Project Management Professional (PMP) preferred.

Title: Emergency Engineer SME

Functional Duties/Responsibilities: Provide expert, on-demand emergency, triage or other immediate engineering services to address a broad range of technology issues security, virtualization, PKI, cloud, data, system administration, information assurance, inspection support, etc. on a strict timeline basis. Engages customer technical POCs as necessary to trouble-shoot issues and identify/implement resolutions.

Minimum Education: A Bachelor’s degree in Computer Science, Engineering, or Information Technology/Operations Management, or an equivalent technical degree. Master’s degree requires two (2) less years of minimum experience. Non-technical degrees must be supplemented by various technical Cyber certifications. An Associate degree must be supplemented by various technical Cyber certifications and two (2) additional years of experience beyond the Minimum Experience Requirements. The absence of a degree must be supplemented by various technical Cyber certifications and four (4) additional years of experience beyond the Minimum Experience Requirements.

Minimum Experience Requirements: Individuals must possess five (5) years of hands-on engineering experience across a wide array of technologies.

Required/Supplemental Certifications: One or more technical certifications such as ITIL, DOD 8570 IAT Level I or technology-specific platforms (e.g. CISCO, VMWare, Microsoft, etc.) as necessary to perform the specific emergency task.

Title: IT Architecture Engineer SME
**Functional Duties/Responsibilities:** Lead and/or define and/or maintain complex or unique Information System architecture strategy, technology, software and security system or unique component design baselines and related best-practices and documentation. Troubleshoot complex or unique problems. Engage vendors and vendor management and direct and/or perform research of complex or unique emerging technologies/best practices and apply findings to enable business solutions. Direct and/or perform unique Analysis of Alternatives and Make/Buy decisions. Engages customer technical POCs as necessary throughout architecture design and implementation activities. May provide supervisory guidance to lower level Engineers.

**Minimum Education:** Bachelor’s degree in Engineering, Information Technology, MIS or related technical field. Master’s degree requires two (2) less years of Minimum Experience. Associate degree requires two (2) more years of Minimum Experience. Non-degreed individuals require four (4) more years of Minimum experience.

**Minimum Experience Requirements:** Twelve (12) years leading and performing relevant IT engineering, including exposure to business planning, systems requirements analysis, network system and security design and application development including detailed knowledge of applicable toolsets, risk management frameworks, architecture frameworks (e.g. DODAF), processes and engineering techniques.

**Required/Supplemental Certifications:** Multiple advanced technical certifications such as ITIL, DOD 8570 IAT Level II or technology-specific platforms (e.g. CISCO, VMWare, Microsoft, etc.) or development languages as necessary to perform the specific architecture tasks.

---

**Title:** IT Architecture Engineer IV

**Functional Duties/Responsibilities:** Lead or define and/or maintain Information System architecture strategy, technology, software and security system or component design baselines and related best-practices and documentation. Engage vendors and research complex emerging technologies/best practices and apply findings to enable business solutions. Lead complex Analysis of Alternatives and Make/Buy decisions. Engages customer technical POCs as necessary throughout architecture design and implementation activities. May provide supervisory guidance to lower level Engineers.

**Minimum Education:** Bachelor’s degree in Engineering, Information Technology, MIS or related technical field. Master’s degree requires two (2) less years of Minimum Experience. Associate degree requires two (2) more years of Minimum Experience. Non-degreed individuals require four (4) more years of Minimum experience.

**Minimum Experience Requirements:** Eight (8) years leading and performing relevant IT engineering, including exposure to business planning, systems requirements analysis, network system and security design and application development including detailed knowledge of applicable toolsets, risk management frameworks, architecture frameworks (e.g. DODAF), processes and engineering techniques.

**Required/Supplemental Certifications:** Multiple advanced technical certifications such as ITIL, DOD 8570 IAT Level II or technology-specific platforms (e.g. CISCO, VMWare, Microsoft, etc.) or development languages as necessary to perform the specific architecture tasks.
Title: IT Architecture Engineer II

Functional Duties/Responsibilities: Define and/or Support and maintain Information System architecture strategy, technology, software and security system or component design baselines and related best-practices and documentation or define and maintain subcomponent design baselines. Support vendor engagements and research fundamental emerging technologies/best practices and apply findings to enable business solutions. Conduct moderate-level Analysis of Alternatives and Make/Buy decisions or support as appropriate. May engages customer technical POCs as necessary throughout architecture design and implementation activities. May provide supervisory guidance to lower level Engineers.

Minimum Education: Bachelor’s degree in Engineering, Information Technology, MIS or related technical field. Master’s degree requires two (2) less years of Minimum Experience. Associate degree requires two (2) more years of Minimum Experience. Non-degreed individuals require four (4) more years of Minimum Required experience.

Minimum Experience Requirements: Four (4) years performing relevant IT experience, including exposure to business planning, systems requirements analysis, network system and security design and application development including detailed knowledge of applicable toolsets, risk management frameworks, architecture frameworks (e.g. DODAF), processes and engineering techniques.

Required/Supplemental Certifications: Technical certifications such as ITIL, DOD 8570 IAT Level I or technology-specific platforms (e.g. CISCO, VMWare, Microsoft, etc.) or development languages as necessary to perform the specific architecture tasks.

----------------------------------------------------------------------------------

Title: IT Engineer III

Functional Duties/Responsibilities: Design and operationalize and/or maintain Information System technology, software and security system or component design baselines and related best-practices and documentation. Troubleshoot systems as required. Engage vendors and/or research advanced emerging technologies/best practices and apply findings to enable business solutions. Conduct or support Analysis of Alternatives and Make/Buy decisions. Engages customer technical POCs as necessary throughout architecture design and implementation activities. May provide supervisory guidance to lower level Engineers.

Minimum Education: Bachelor’s degree in Engineering, Information Technology, MIS or related technical field. Master’s degree requires two (2) less years of Minimum Experience. Associate degree requires two (2) more years of Minimum Experience. Non-degreed individuals require four (4) more years of Minimum experience.

Minimum Experience Requirements: Four (4) years leading or performing relevant IT engineering, including exposure to systems requirements analysis, network system and security design, system administration and application development including detailed knowledge of applicable toolsets, processes and engineering techniques.

Required/Supplemental Certifications: Multiple or advanced technical certifications such as ITIL, DOD 8570 IAT Level II or technology-specific platforms (e.g. CISCO, VMWare, Microsoft, etc.) or development languages as necessary to perform the specific architecture tasks.
Title: IT Engineer II

Functional Duties/Responsibilities: Design and/or Support and/or operationalize and/or maintain Information System technology, software and security system or (sub)component design baselines and related best-practices and documentation. Troubleshoot systems as required. Support vendors and/or research fundamental emerging technologies/best practices and apply findings to enable business solutions. Conduct moderate-level Analysis of Alternatives and Make/Buy decisions or support as appropriate. May engages customer technical POCs as necessary throughout architecture design and implementation activities. May provide supervisory guidance to lower level Engineers.

Minimum Education: Bachelor’s degree in Engineering, Information Technology, MIS or related technical field. Master’s degree requires two (2) less years of Minimum Experience. Associate degree requires two (2) more years of Minimum Experience. Non-degreed individuals require four (4) more years of Minimum experience.

Minimum Experience Requirements: Two (2) years performing relevant IT engineering, including exposure to systems requirements analysis, network system and security design, system administration and application development including detailed knowledge of applicable toolsets, processes and engineering techniques.

Required/Supplemental Certifications: Technical certifications such as ITIL, DOD 8570 IAT Level I or technology-specific platforms (e.g. CISCO, VMWare, Microsoft, etc.) or development languages as necessary to perform the specific architecture tasks.

Title: IT Engineer I

Functional Duties/Responsibilities: Design and/or Support and/or operationalize and/or maintain Information System technology, software and security system or (sub)component design baselines and related best-practices and documentation. Perform basic troubleshooting of systems as required. Support vendors and/or research technologies/best practices and apply findings to enable business solutions. Support Analysis of Alternatives and Make/Buy decisions as appropriate. Interacts directly with the Program/Project Manager and or Lead Engineer.

Minimum Education: Bachelor’s degree in Engineering, Information Technology, MIS or related technical field. Master’s degree requires two (2) less years of Minimum Experience. Associate degree requires two (2) more years of Minimum Experience. Non-degreed individuals require four (4) more years of Minimum experience.

Minimum Experience Requirements: N/A

Required/Supplemental Certifications: N/A

Title: IT Requirements Analyst V
**Functional Duties/Responsibilities:** Lead customer stakeholders, architects and engineers in the decomposition and documentation of highly-complex and/or unique technical requirements of a business solutions into operational – level requirements suitable for design and maintenance of an advanced or complex Information System technology, software and security system. Ensure adherence to System/Software Design Lifecycle (SDLC) best-practices. Provide authoritative contributions to Analysis of Alternatives and Make/Buy decisions. Support design review processes. Lead the translation of business requirements and designs into technical manuals or training materials. Engages customer and team technical POCs as necessary throughout requirements activities. May provide supervisory guidance to lower level Analysts.

**Minimum Education:** Bachelor’s degree. Master’s degree requires two (2) less years of Minimum Experience. Associate degree requires two (2) more years of Minimum Experience. Non-degreed individuals require four (4) more years of Minimum experience.

**Minimum Experience Requirements:** Eight (8) years of relevant IT experience, including expert knowledge of systems requirements analysis, business analysis, technical writing and/or detailed knowledge of applicable toolsets, processes and engineering techniques.

**Required/Supplemental Certifications:** A professional IT certification such as ITIL, Certified Scrum Master, etc.

Title: IT Requirements Analyst III

**Functional Duties/Responsibilities:** Lead customer stakeholders, architects and engineers in the decomposition and documentation of high-level and/or complex technical requirements of a business solutions into operational – level requirements suitable for design and maintenance of an advanced or complex Information System technology, software and security system or subcomponent. Ensure adherence to System/Software Design Lifecycle (SDLC) best-practices. Support Analysis of Alternatives and Make/Buy decisions. Support design review processes. Translate business requirements and designs into technical manuals or training materials. Engages customer and team technical POCs as necessary throughout requirements activities. May provide supervisory guidance to lower level Analysts.

**Minimum Education:** Bachelor’s degree. Master’s degree requires two (2) less years of Minimum Experience. Associate degree requires two (2) more years of Minimum Experience. Non-degreed individuals require four (4) more years of Minimum experience.

**Minimum Experience Requirements:** Four (4) years of relevant IT experience, including knowledge of systems requirements analysis, business analysis, technical writing and/or detailed knowledge of applicable toolsets, processes and engineering techniques.

**Required/Supplemental Certifications:** N/A

Title: IT Requirements Analyst I
**Functional Duties/Responsibilities:** Interface with or support customer stakeholders, architects and engineers in the decomposition and documentation of high-level technical requirements of a business solution into operational – level requirements suitable for design and maintenance of an Information System technology, software and security system or subcomponent. Help ensure adherence to System/Software Design Lifecycle (SDLC) best-practices. Support Analysis of Alternatives and Make/Buy decisions. Support design review processes. Translate or support the translation of business requirements and designs into technical manuals or training materials. Interacts directly with the Program/Project Manager and or Lead Engineer.

**Minimum Education:** Associate degree. Non-degreed individuals require two (2) more years of Minimum experience.

**Minimum Experience Requirements:** N/A

**Required/Supplemental Certifications:** N/A

---

**Title:** System Security Engineer SME

**Functional Duties/Responsibilities:** Perform the security design, configuration, hardening, testing and monitoring of unique or highly complex Information System technologies independently or lead the larger design team. Performs secure engineering and vulnerability testing on information systems to include but not limited to: Physical and Virtual Operating Systems, Web Applications, Databases, and Networking Devices. Provides specialized troubleshooting across a wide range of technologies and performs penetration testing across technologies. Applies expert knowledge of current compliance standards and associated technical controls across these technologies. Engages customer technical POCs as necessary throughout security architecture design and implementation activities. May provide supervisory guidance to lower level Engineers.

**Minimum Education:** Bachelor’s degree in Computer Science, Engineering or Information Technology or related technical field. Master’s degree requires two (2) less years of Minimum Experience. Associate degree requires two (2) more years of Minimum Experience. Non-degreed individuals require four (4) more years of Minimum experience.

**Minimum Experience Requirements:** Must have twelve (12) years of information security-related experience leading and performing security operations, vulnerability management, security testing, system patching, log analysis, intrusion detection and security device technologies administration. Expert knowledge of RMF, Windows/Linux Operating Systems, STIGS, ACAS, HBSS and/or related technologies.

**Required/Supplemental Certifications:** DoD 8570 IAT III compliant certifications required and technology-specific platforms (e.g. CISCO, VMWare, Microsoft, etc.) certifications as appropriate to perform the taskings. Advanced technical certifications such as Offensive Security Certifications, Licensed Penetration Tester or CISCO Network Security certifications or equivalent required.

---

**Title:** System Security Engineer V

**Functional Duties/Responsibilities:** Perform the security design, configuration, hardening, testing and monitoring of a wide variety of complex Information System technologies independently or lead the larger design team.
Performs secure engineering and vulnerability testing on information systems to include but not limited to: Physical and Virtual Operating Systems, Web Applications, Databases, and Networking Devices. Provides higher level troubleshooting across a wide range of technologies and performs penetration testing across technologies. Applies expert knowledge of current compliance standards and associated technical controls across these technologies. Engages customer technical POCs as necessary throughout security architecture design and implementation activities. May provide supervisory guidance to lower level Engineers.

**Minimum Education:** Bachelor’s degree in Computer Science, Engineering or Information Technology or related technical field. Master’s degree requires two (2) less years of Minimum Experience. Associate degree requires two (2) more years of Minimum Experience. Non-degreed individuals require four (4) more years of Minimum experience.

**Minimum Experience Requirements:** Must have ten (10) years of information security-related experience leading and performing security operations, vulnerability management, security testing, system patching, log analysis, intrusion detection and security device technologies administration. Advanced knowledge of RMF, Windows/Linux Operating Systems, STIGS, ACAS, HBSS and/or related technologies.

**Required/Supplemental Certifications:** DoD 8570 IAT III compliant certifications required and technology-specific platforms (e.g. CISCO, VMWare, Microsoft, etc.) certifications as appropriate to perform the taskings. An advanced technical certification such as Offensive Security Certifications, Licensed Penetration Tester or CISCO Network Security certifications or equivalent required.

Title: System Security Engineer IV

**Functional Duties/Responsibilities:** Perform the security design, configuration, hardening, testing and monitoring of a wide variety of complex Information System technologies independently or lead the larger design team. Performs secure engineering and vulnerability testing on information systems to include but not limited to: Physical and Virtual Operating Systems, Web Applications, Databases, and Networking Devices. Provides higher level troubleshooting across a wide range of technologies and may perform penetration testing. Applies advanced knowledge of current compliance standards and associated technical controls across these technologies. Engages customer technical POCs as necessary throughout security architecture design and implementation activities. May provide supervisory guidance to lower level Engineers.

**Minimum Education:** Bachelor’s degree in Computer Science, Engineering or Information Technology or related technical field. Master’s degree requires two (2) less years of Minimum Experience. Associate degree requires two (2) more years of Minimum Experience. Non-degreed individuals require four (4) more years of Minimum experience.

**Minimum Experience Requirements:** Must have eight (8) years of information security-related experience leading and performing security operations, vulnerability management, security testing, system patching, log analysis, intrusion detection and/or security device technologies administration. Knowledge of RMF, Windows/Linux Operating Systems, STIGS, ACAS, HBSS and/or related technologies.

**Required/Supplemental Certifications:** DoD 8570 IAT III compliant certifications required and technology-specific platforms (e.g. CISCO, VMWare, Microsoft, etc.) certifications as appropriate to perform the taskings. An advanced
technical certification such as Offensive Security Certifications, Licensed Penetration Tester or CISCO Network Security certifications required.

Title: System Security Engineer III

**Functional Duties/Responsibilities:** Lead the security design, configuration, hardening, testing and monitoring of a wide variety of moderately complex Information System technologies independently or as part of a larger design team. Performs secure engineering and vulnerability testing on information systems to include but not limited to: Physical and Virtual Operating Systems, Web Applications, Databases, and Networking Devices. Applies knowledge of current compliance standards and associated technical controls across these technologies. Engages customer technical POCs as necessary throughout security architecture design and implementation activities. May provide supervisory guidance to lower level Engineers.

**Minimum Education:** Bachelor’s degree in Computer Science, Engineering or Information Technology or related technical field. Master’s degree requires two (2) less years of Minimum Experience. Associate degree requires two (2) more years of Minimum Experience. Non-degreed individuals require four (4) more years of Minimum experience.

**Minimum Experience Requirements:** Must have six (6) years of information security-related experience leading or performing security operations, vulnerability management, security testing, system patching, log analysis, intrusion detection and/or security device technologies administration. Knowledge of RMF, Windows/Linux Operating Systems, STIGS, ACAS, HBSS and/or related technologies.

**Required/Supplemental Certifications:** DoD 8570 IAT II compliant certifications required and technology-specific platforms (e.g. CISCO, VMWare, Microsoft, etc.) certifications as appropriate to perform the taskings.

Title: System Security Engineer II

**Functional Duties/Responsibilities:** Lead or perform the security design, configuration, hardening, testing and monitoring of a wide variety of advanced Information System technologies independently or as part of a larger design team. Performs secure engineering and vulnerability testing on information systems to include but not limited to: Physical and Virtual Operating Systems, Web Applications, Databases, and Networking Devices. Applies knowledge of current compliance standards and associated technical controls across these technologies. Engages customer technical POCs as necessary throughout security architecture design and implementation activities. May provide supervisory guidance to lower level Engineers.

**Minimum Education:** Bachelor’s degree in Computer Science, Engineering or Information Technology or related technical field. Master’s degree requires two (2) less years of Minimum Experience. Associate degree requires two (2) more years of Minimum Experience. Non-degreed individuals require four (4) more years of Minimum experience.

**Minimum Experience Requirements:** Must have four (4) years of information security-related experience in areas such as security operations, vulnerability management, security testing, system patching, log analysis, intrusion
detection and security device technologies administration. Knowledge of RMF, Windows/Linux Operating Systems, STIGS, ACAS, HBSS and/or related technologies.

**Required/Supplemental Certifications:** DoD 8570 IAT I compliant certification. Technology-specific platforms (e.g. CISCO, VMWare, Microsoft, etc.) certifications as appropriate to perform the taskings.

---

**Title:** Information Assurance Analyst SME

**Functional Duties/Responsibilities:** Develop IA strategies and provide expert consultation on IA related matters. Lead and/or review and/or develop and publish security plans, policies, procedures and associated guidance documents necessary to implement a compliant IT security program across the lifecycle of a wide variety of unique technologies to achieve the strategic outcomes. Maintain an inventory of all Information Systems documentation. Provide comprehensive analysis and validate implementation of Information System controls on complex technologies. Submit compliance packages to the adjudicating organization and lead and/or support audits as appropriate. Engages customer technical POCs as necessary throughout IA activities. May provide supervisory guidance to lower level Information Assurance Analysts.

**Minimum Education:** Master’s degree in Engineering, MIS, Business Administration or equivalent. A Bachelor’s or Associate degree must be supplemented by technical certifications four (4) or two (2) additional years of experience, respectively, beyond the Minimum Experience Requirements. The absence of a degree must be supplemented by multiple technical certification and four (4) additional years of experience and beyond the Minimal Experience Requirements.

**Minimum Experience Requirements:** Ten (10) years of experience leading and or performing information assurance responsibilities and a detailed understanding of practical areas relating to and applying current compliance standards to unique technological systems, concepts and analysis. Previously performed as an Information System Manager or Certifying Authority Representative.

**Required/Supplemental Certifications:** CISSP or CISM.

---

**Title:** Information Assurance Analyst V

**Functional Duties/Responsibilities:** Develop IA strategies and provide expert consultation on IA related matters. Lead and/or review and/or develop and publish security plans, policies, procedures and associated guidance documents necessary to implement a compliant IT security program across the lifecycle of a wide variety of unique or complex technologies to achieve the strategic outcomes. Maintain an inventory of all Information Systems documentation. Provide comprehensive analysis and validate implementation of Information System controls on complex technologies. Submit compliance packages to the adjudicating organization and lead and/or support audits as appropriate. Engages customer technical POCs as necessary throughout IA activities. May provide supervisory guidance to lower level Information Assurance Analysts.

**Minimum Education:** Master’s degree in Engineering, MIS, Business Administration or equivalent. A Bachelor’s or Associate degree must be supplemented by technical certifications four (4) or two (2) additional years of experience,
respectively, beyond the Minimum Experience Requirements. The absence of a degree must be supplemented by multiple technical certification and four (4) additional years of experience and beyond the Minimal Experience Requirements.

**Minimum Experience Requirements**: Eight (8) years of experience leading and or performing information assurance responsibilities and a detailed understanding of practical areas relating to and applying current compliance standards to unique or complex technological systems, concepts and analysis. Previously performed as an Information System Manager or Certifying Authority Representative.

**Required/Supplemental Certifications**: CISSP or CISM.

---

**Title**: Information Assurance Analyst IV

**Functional Duties/Responsibilities**: Develop IA strategies and provide consultation on complex IA related matters. Lead and/or review and/or develop and publish security plans, policies, procedures and associated guidance documents necessary to implement a compliant IT security program across the lifecycle of a wide variety of complex technologies to achieve the strategic outcomes. Maintain an inventory of all Information Systems documentation. Provide comprehensive analysis and validate implementation of Information System controls on complex technologies. Submit compliance packages to the adjudicating organization and lead and/or support audits as appropriate. Engages customer technical POCs as necessary throughout IA activities. May provide supervisory guidance to lower level Information Assurance Analysts.

**Minimum Education**: Bachelor’s degree in Engineering, MIS, Business Administration or equivalent. An Associate degree must be supplemented by technical certifications and two (2) additional years of experience beyond the Minimum Experience Requirements. The absence of a degree must be supplemented by multiple technical certification and four (4) additional years of experience and beyond the Minimal Experience Requirements.

**Minimum Experience Requirements**: Six (6) years of experience leading and or performing information assurance responsibilities and a detailed understanding of practical areas relating to and applying current compliance standards to complex technological systems, concepts and analysis. Previously performed as an Information System Manager or Certifying Authority Representative.

**Required/Supplemental Certifications**: CISSP or CISM.

---

**Title**: Information Assurance Analyst III

**Functional Duties/Responsibilities**: Develop IA strategies. Lead and/or review and/or develop and publish security plans, policies, procedures and associated guidance documents necessary to implement a compliant IT security program across the lifecycle of a wide variety of advanced technologies to achieve strategic outcomes. Maintain an inventory of all Information Systems documentation. Provide comprehensive analysis and validate implementation of Information System controls on advanced technologies. Submit compliance packages to the adjudicating organization and lead and/or support audits as appropriate. Engages customer technical POCs as necessary throughout IA activities. May provide supervisory guidance to lower level Information Assurance Analysts.
Minimum Education: Bachelor’s degree in Engineering, MIS, Business Administration or equivalent. An Associate degree must be supplemented by technical certifications and two (2) additional years of experience beyond the Minimum Experience Requirements. The absence of a degree must be supplemented by multiple technical certification and four (4) additional years of experience and beyond the Minimal Experience Requirements.

Minimum Experience Requirements: Four (4) years of experience leading and or performing information assurance responsibilities and a detailed understanding of practical areas relating to and applying current compliance standards to advanced technological systems, concepts and analysis. Example experience includes previously performing as an Information System Manager or Certifying Authority Representative.

Required/Supplemental Certifications: CISSP or multiple technical certifications such as CISM or Security +.

Title: Information Assurance Analyst I

Functional Duties/Responsibilities: Review and/or develop and publish security plans, policies, procedures and associated guidance documents necessary to implement a compliant IT security program across the lifecycle of a wide variety of technologies. Maintain an inventory of all Information Systems documentation. Provide analysis and validate implementation of Information System controls on technologies. Submit compliance packages to the adjudicating organization and lead and/or support audits as appropriate. Interacts directly with the Program/Project Manager and or Lead IA Engineer.

Minimum Education: Associate degree. A Bachelor’s or Master’s degree requires two (2) less years of Minimum Experience. The absence of a degree must be supplemented by multiple technical certification and four (4) additional years of experience and beyond the Minimal Experience Requirements.

Minimum Experience Requirements: One (1) year of experience performing information assurance or IT responsibilities and a basic understanding of practical areas relating to and applying current compliance standards to technological systems, concepts and analysis.

Required/Supplemental Certifications: Security + or equivalent

Title: System Administrator SME

Functional Duties/Responsibilities: Lead and/or perform installation, configuration, operationalization, system(s) management/monitoring, data backup/restoration/ transformation and maintenance (e.g. patching/upgrades) of unique IT infrastructure including hardware, firmware, security and software technologies to perform within designated availability levels and enable mission and/or business solutions. Create associated process documentation. Schedule and perform complex or time sensitive Install, Move, Add, Change accounts and technology devices as necessary. Diagnose unique IT system issues and outages and provide associated communications and After-Action Reports. Identify and direct recommended technology or process enhancements including script automation. Engages customer technical POCs as necessary throughout the system administration activities. May provide supervisory guidance to lower level Administrators.
Minimum Education: Master’s degree in Engineering, Information Technology, MIS or related technical field. A Bachelor’s degree requires two (2) more years of Minimum Experience. Associate degree requires four (4) more years of Minimum Experience. Non-degreed individuals require six (6) more years of Minimum experience.

Minimum Experience Requirements: Ten (10) years leading or performing relevant system or network administration duties demonstrating expertise across a broad range of technologies to include physical and virtual networks (e.g. LAN/WAN/Wireless), operating systems and platforms (e.g. Microsoft, Linux, MAC), databases and security devices.

Required/Supplemental Certifications: ITIL and Technology-specific platforms (e.g. CISCO, VMWare, Microsoft, etc.) as necessary to perform the specific system administration tasks.

Title: System Administrator III

Functional Duties/Responsibilities: Lead and/or perform installation, configuration, operationalization, system(s) management/monitoring, data backup/restoration/ transformation and maintenance (e.g. patching/upgrades) of advanced IT infrastructure including hardware, firmware, security and software technologies to perform within designated availability levels and enable mission and/or business solutions. Create and update associated process documentation. Schedule and perform Install, Move, Add, Change accounts and technology devices as necessary. Diagnose IT system issues and outages and provide associated communications and After-Action Reports. Identify and recommend technology or process enhancements which may include script automation. Engages customer technical POCs as necessary throughout system administration activities. May provide supervisory guidance to lower level Administrators.

Minimum Education: Bachelor’s degree in Engineering, Information Technology, MIS or related technical field. Master’s degree requires two (2) less years of Minimum Experience. Associate degree requires two (2) more years of Minimum Experience. Non-degreed individuals require four (4) more years of Minimum experience.

Minimum Experience Requirements: Four (4) years leading or performing relevant system or network administration duties demonstrating advanced proficiency across a broad range of technologies to include physical and virtual networks (e.g. LAN/WAN/Wireless), operating systems and platforms (e.g. Microsoft, Linux, MAC), databases and security devices.

Required/Supplemental Certifications: Technology-specific platforms (e.g. CISCO, VMWare, Microsoft, etc.) as necessary to perform the specific system administration tasks.

Title: System Administrator I

Functional Duties/Responsibilities: Perform installation, configuration, operationalization, system(s) management/monitoring, data backup/restoration/ transformation and maintenance (e.g. patching/upgrades) of IT infrastructure including hardware, firmware, security and software technologies to perform within designated availability levels and enable mission and/or business solutions. Update associated process documentation. Schedule and perform Install, Move, Add, Change accounts and technology devices as necessary. Diagnose and/or...
help resolve IT system issues and outages and provide associated communications and After-Action Reports. Interacts directly with the Program/Project Manager and or Lead Administrator.

**Minimum Education:** Associate degree technical field. Non-degreed individuals require four (4) more years of Minimum experience.

**Minimum Experience Requirements:** Working knowledge of demonstrating comprehension of IT systems across technologies to include physical (e.g. LAN/WAN/Wireless), operating systems and platforms (e.g. Microsoft, Linux, MAC), databases and security devices.

**Required/Supplemental Certifications:** N/A.

---

**Title:** SW Engineer V

**Functional Duties/Responsibilities:** Lead and/or perform the custom design, coding, integration, quality testing, debugging, acceptance testing and Operations/Maintenance/Enhancements of efficient complex software to achieve a mission or business solution in accordance with customer-specified requirements and languages. May also be required to integrate, adapt/customize and optimize Commercial-Off-The-Shelf (COTS) software packages independently or as part of a larger software solution. Ensure developed software is free of common or known security vulnerabilities. Maximize efficiencies in open-source, virtualization, code-reuse and automated testing. Communicate expertly in various software development collaboration tools including automated deployments. Develop algorithms. Create and update associated software documentation and user manuals consistent within various Software Development Lifecycles (SDLC). Diagnose software issues and outages and provide associated communications and After-Action Reports. Identify and recommend software or processing enhancements. Engages customer technical Product Managers and other developers as necessary throughout the software development activities. May provide supervisory guidance to lower level Developers.

**Minimum Education:** Bachelor’s degree in Computer Science, Engineering, Information Technology or related technical field. Master’s degree requires two (2) less years of Minimum Experience. Associate degree requires two (2) more years of Minimum Experience. Non-degreed individuals require four (4) more years of Minimum experience.

**Minimum Experience Requirements:** Eight (8) years leading or performing advanced software development demonstrating mastery across a broad range of SDLCs, Agile/Waterfall methodologies, software languages, frameworks/platforms, systems, databases and related specialized technologies, processes and/or collaboration tools (e.g. SLACK, JIRA, Confluence, CI/CD, DevOps, DevSecOps, etc.) consistent with project requirements.

**Required/Supplemental Certifications:** Microsoft, AWS or another technology-specific certification as necessary to perform the specific development tasks.

---

**Title:** SW Engineer III

**Functional Duties/Responsibilities:** Lead and/or perform the custom design, coding, integration, quality testing, debugging, acceptance testing and Operations/Maintenance/Enhancements of efficient advanced software to
achieve a mission or business solution in accordance with customer-specified requirements and languages. May also be required to integrate, adapt/customize and optimize Commercial-Off-The-Shelf (COTS) software packages independently or as part of a larger software solution. Ensure developed software is free of common or known security vulnerabilities. Maximize efficiencies in open-source, virtualization code-reuse and automated testing. Communicate proficiently in various software development collaboration tools. May require algorithm development. Create and update associated software documentation and user manuals consistent within various Software Development Lifecycles (SDLC). Diagnose software issues and outages and provide associated communications and After-Action Reports. Identify and recommend software or processing enhancements. Engages customer technical Product Managers and other developers as necessary throughout the software development activities. May provide supervisory guidance to lower level Developers.

**Minimum Education:** Bachelor’s degree in Computer Science, Engineering, Information Technology or related technical field. Master’s degree requires two (2) less years of Minimum Experience. Associate degree requires two (2) more years of Minimum Experience. Non-degreed individuals require four (4) more years of Minimum experience.

**Minimum Experience Requirements:** Four (4) years leading or performing advanced software development demonstrating advanced proficiency across a broad range of SDLCs, Agile/Waterfall methodologies, software languages, frameworks/platforms, systems, databases and related specialized technologies, processes and/or collaboration tools (e.g. SLACK, JIRA, Confluence, CI/CD, DevOps, DevSecOps, etc.) consistent with project requirements.

**Required/Supplemental Certifications:** Microsoft, AWS or another technology-specific certification as necessary to perform the specific development tasks.

---

**Title:** Cloud Engineer V

**Functional Duties/Responsibilities:** Lead and/or perform the custom architecture, design, planning, implementation, orchestration/automation, troubleshooting, quality testing, data ingest, acceptance testing, management and Operations/Maintenance/Enhancements to deploy complex virtualization/cloud computing capabilities to achieve a mission or business solution in accordance with customer-specified requirements and platform environments. May also be required to integrate, adapt/customize and optimize Commercial-Off-The-Shelf (COTS) technologies into the larger software solution. Also builds, designs and leverages Web Services and/or APIs. Ensure the cloud solution is free of common or known security vulnerabilities. Communicate expertly in various technology collaboration tools. Report system performance through visualization dashboards. Create and update associated technical documentation and user manuals consistent with prevailing governance framework. Diagnose unique or complex performance issues and outages and provide associated communications and After-Action Reports. Identify and recommend process enhancements. Engage cloud providers. Engages customer technical Product Managers and other engineers as necessary throughout the engineering activities. May provide supervisory guidance to lower level Engineers.

**Minimum Education:** Master’s degree in Computer Science, Engineering, Information Technology or related technical field. Bachelor’s degree requires two (2) more years of Minimum Experience. Associate degree requires four (4) more years of Minimum Experience. Non-degreed individuals require six (6) more years of Minimum experience and advanced cloud certifications.
Minimum Experience Requirements: Eight (8) years leading or performing advanced cloud computing engineering in AWS, Azure or related virtual platforms with associated programming, scripting, databases and open source technologies skills consistent with project requirements.

Required/Supplemental Certifications: AWS, Microsoft or another equivalent technology-specific certification (e.g. AWS Developer, Solutions Architect, VMWare, etc.) as necessary to perform the specific development tasks.

Title: Cloud Engineer III

Functional Duties/Responsibilities: Lead and/or perform the custom architecture, design, planning, implementation, orchestration/automation, troubleshooting, quality testing, data ingest, acceptance testing, management and Operations/Maintenance/Enhancements to deploy advanced virtualization/cloud computing capabilities to achieve a mission or business solution in accordance with customer-specified requirements and platform environments. May also be required to integrate, adapt/customize and optimize Commercial-Off-The-Shelf (COTS) technologies into the larger software solution. Also builds, designs and leverages Web Services and/or APIs. Ensure the cloud solution is free of common or known security vulnerabilities. Communicate proficiently in various technology collaboration tools. Report system performance through visualization dashboards. Create and update associated technical documentation and user manuals consistent with prevailing governance framework. Diagnose advanced performance issues and outages and provide associated communications and After-Action Reports. Identify and recommend process enhancements. Engage cloud providers. Engages customer technical Product Managers and other engineers as necessary throughout the engineering activities. May provide supervisory guidance to lower level Engineers.

Minimum Education: Bachelor’s degree in Computer Science, Engineering, Information Technology or related technical field. Master’s degree requires two (2) less years of Minimum Experience. Associate degree requires two (2) more years of Minimum Experience. Non-degreed individuals require four (4) more years of Minimum experience and advanced cloud certifications.

Minimum Experience Requirements: Four (4) years leading or performing advanced cloud computing engineering in AWS, Azure or related cloud platforms with associated programming, scripting, databases and open source technologies skills consistent with project requirements.

Required/Supplemental Certifications: AWS, Microsoft or another equivalent technology-specific certification (e.g. AWS Cloud Practitioner, Developer, VMWare, etc.) as necessary to perform the specific development tasks.

Title: Cloud Engineer II

Functional Duties/Responsibilities: Lead and/or perform the custom design, planning, implementation, orchestration/automation, troubleshooting, quality testing, data ingest, acceptance testing, management and Operations/Maintenance/Enhancements to deploy virtualization/cloud computing capabilities to achieve a mission or business solution in accordance with customer-specified requirements and platform environments. May also be required to integrate, adapt/customize and optimize Commercial-Off-The-Shelf (COTS) technologies into the larger software solution.
software solution. Also leverages Web Services and/or APIs. Ensure the cloud solution is free of common or known security vulnerabilities. Communicate proficiently in various technology collaboration tools. Report system performance through visualization dashboards. Create and update associated technical documentation and user manuals consistent with prevailing governance framework. Diagnose performance issues and outages and provide associated communications and After-Action Reports. Identify and recommend process enhancements. Engage cloud providers. Engages customer technical Product Managers and other engineers as necessary throughout the engineering activities. May provide supervisory guidance to lower level Engineers.

**Minimum Education:** Bachelor’s degree in Computer Science, Engineering, Information Technology or related technical field. Master’s degree requires two (2) less years of Minimum Experience. Associate degree requires two (2) more years of Minimum Experience. Non-degreed individuals require four (4) more years of Minimum experience.

**Minimum Experience Requirements:** Two (2) years leading or performing cloud computing engineering in AWS, Azure or related cloud platforms and associated programming, scripting, databases and open source technologies skills, consistent with project requirements.

**Required/Supplemental Certifications:** AWS, Microsoft or another equivalent technology-specific certification (e.g. AWS Cloud Practitioner VMWare, etc.) as necessary to perform the specific development tasks.

---

**Title:** Data Scientist Engineer IV

**Functional Duties/Responsibilities:** Lead and/or leverage the use of data gathering/mining for both large structured and unstructured data sets, analytical/statistical modeling and visualization toolsets to synthesize disparate data into useable information to help mission or business stakeholders identify data-driven to highly-complex solutions and make knowledge-based decisions. Create advanced data architectures, leverage data conditioning and apply both commercially available toolsets and custom scripting to reorganize and modeling the data to achieve these outcomes. Develop algorithms for predictive analytics. Utilize Machine Learning as part of the analytical processes. Continually enhance hypothesis and data models to refine both accuracy and precision of ongoing strategic, operational and tactical analysis. Create and update associated technical documentation and reports. Engages customer technical POCs and other engineers as necessary throughout the engineering activities. May provide supervisory guidance to lower level Engineers.

**Minimum Education:** Master’s degree in Computer Science, Engineering, Information Technology or related technical field. Bachelor’s degree requires two (2) more years of Minimum Experience. Associate degree requires four (4) more years of Minimum Experience. Non-degreed individuals require six (6) more years of Minimum Experience.

**Minimum Experience Requirements:** Six (6) years leading or performing data science engineering leveraging associated programming, scripting, databases, open source technologies and statistical tools consistent with project requirements.

**Required/Supplemental Certifications:** Certifications in recognized data-science and analytics toolsets, programming languages or a data science-unique certification as required to perform the specific data science taskings.
Title: Data Scientist Engineer II

Functional Duties/Responsibilities: Lead and/or leverage the use of data gathering/mining for both large structured and unstructured data sets, analytical/statistical modeling and visualization toolsets to synthesize disparate data into useable information to help mission or business stakeholders identify data-driven solutions and make knowledge-based decisions. Create data architectures, leverage data conditioning and apply both commercially available toolsets and custom scripting to reorganize and modeling the data to achieve these outcomes. Develop algorithms for predictive analytics. May utilize Machine Learning as part of the analytical processes. Continually enhance hypothesis and data models to refine both accuracy and precision of on-going strategic, operational and tactical analysis. Create and update associated technical documentation and reports. Engages customer technical POCs and other engineers as necessary throughout the engineering activities. May provide supervisory guidance to lower level Engineers.

Minimum Education: Master’s degree in Computer Science, Engineering, Information Technology or related technical field. Bachelor’s degree requires two (2) more years of Minimum Experience. Associate degree requires four (4) more years of Minimum Experience. Non-degreed individuals require six (6) more years of Minimum Experience.

Minimum Experience Requirements: Four (4) years leading or performing data science engineering leveraging associated programming, scripting, databases, open source technologies and statistical tools consistent with project requirements.

Required/Supplemental Certifications: Certifications in recognized data-science and analytics toolsets, programming languages or a data science-unique certification as required to perform the specific data science taskings.

Title: Data Requirements Analyst III

Functional Duties/Responsibilities: Lead customer stakeholders and data engineers in the decomposition and documentation of high-level and/or complex data requirements of a strategic objective into operational – level requirements suitable for the design of data gathering, modeling, algorithm development, statistical analysis and validation testing to create data-driven solutions. May support the development of data architectures and perform general data conditioning. Support the continual enhancement of data engineers’ hypothesis and data models to refine both accuracy and precision of on-going strategic, operational and tactical analysis. Translate data requirements into associated technical documentation, reports and training artifacts. Engages customer technical POCs and other data engineers as necessary throughout the requirements activities. May provide supervisory guidance to lower level Analysts.

Minimum Education: Bachelor’s degree in Computer Science, Engineering, IT, MIS or equivalent. Master’s degree requires two (2) less years of Minimum Experience. Associate degree requires two (2) more years of Minimum Experience. Non-degreed individuals require four (4) more years of Minimum experience.
Minimum Experience Requirements: Four (4) years of relevant data requirements experience, including knowledge of systems requirements analysis, business analysis, technical writing and/or detailed knowledge of applicable data science toolsets, processes and engineering techniques.

Required/Supplemental Certifications: N/A

Title: Data Requirements Analyst II

Functional Duties/Responsibilities: Lead customer stakeholders and data engineers in the decomposition and documentation of high-level data requirements of a strategic or operational objective into actionable requirements suitable for the design of data gathering, modeling, algorithm development, statistical analysis and validation testing to create data-driven solutions. May support the development of data architectures and perform general data conditioning. Support the continual enhancement of data engineers’ hypothesis and data models to refine both accuracy and precision of on-going strategic, operational and tactical analysis. Translate data requirements into associated technical documentation, reports and training artifacts. Engages customer technical POCs and other data engineers as necessary throughout the requirements activities. May provide supervisory guidance to lower level Analysts.

Minimum Education: Bachelor’s degree in Computer Science, Engineering, IT, MIS or equivalent. Associate degree requires two (2) more years of Minimum Experience. Non-degreed individuals require four (4) more years of Minimum experience.

Minimum Experience Requirements: Two (2) years of relevant data requirements experience, including knowledge of systems requirements analysis, business analysis, technical writing and/or working knowledge of applicable data science toolsets, processes and engineering techniques.

Required/Supplemental Certifications: N/A

<table>
<thead>
<tr>
<th>Labor Category</th>
<th>year 1</th>
<th>year 2</th>
<th>year 3</th>
<th>year 4</th>
<th>year 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Program Manager V</td>
<td>$187.27</td>
<td>$191.95</td>
<td>$196.75</td>
<td>$201.67</td>
<td>$206.71</td>
</tr>
<tr>
<td>Cyber Project Manager III</td>
<td>$140.33</td>
<td>$143.83</td>
<td>$147.43</td>
<td>$151.11</td>
<td>$154.89</td>
</tr>
<tr>
<td>Cyber Project Manager II</td>
<td>$121.95</td>
<td>$125.00</td>
<td>$128.13</td>
<td>$131.33</td>
<td>$134.61</td>
</tr>
<tr>
<td>Emergency Cyber Engineer</td>
<td>$327.96</td>
<td>$336.16</td>
<td>$344.56</td>
<td>$353.18</td>
<td>$362.01</td>
</tr>
<tr>
<td>Exploitation Engineer SME</td>
<td>$183.35</td>
<td>$187.94</td>
<td>$192.63</td>
<td>$197.45</td>
<td>$202.39</td>
</tr>
<tr>
<td>Exploitation Engineer V</td>
<td>$165.29</td>
<td>$169.42</td>
<td>$173.66</td>
<td>$178.00</td>
<td>$182.45</td>
</tr>
<tr>
<td>Exploitation Engineer IV</td>
<td>$156.72</td>
<td>$160.63</td>
<td>$164.65</td>
<td>$168.77</td>
<td>$172.99</td>
</tr>
<tr>
<td>Exploitation Engineer III</td>
<td>$142.59</td>
<td>$146.16</td>
<td>$149.81</td>
<td>$153.56</td>
<td>$157.39</td>
</tr>
<tr>
<td>Exploitation Engineer II</td>
<td>$121.68</td>
<td>$124.72</td>
<td>$127.84</td>
<td>$131.04</td>
<td>$134.31</td>
</tr>
<tr>
<td>Incident Responder IV</td>
<td>$140.69</td>
<td>$144.20</td>
<td>$147.81</td>
<td>$151.50</td>
<td>$155.29</td>
</tr>
<tr>
<td>Incident Responder III</td>
<td>$112.46</td>
<td>$115.27</td>
<td>$118.15</td>
<td>$121.10</td>
<td>$124.13</td>
</tr>
</tbody>
</table>

54151HACS
<table>
<thead>
<tr>
<th>Labor Category</th>
<th>year 1</th>
<th>year 2</th>
<th>year 3</th>
<th>year 4</th>
<th>year 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOC Analyst II</td>
<td>$105.09</td>
<td>$107.72</td>
<td>$110.41</td>
<td>$113.17</td>
<td>$116.00</td>
</tr>
<tr>
<td>SOC Analyst I</td>
<td>$97.18</td>
<td>$99.61</td>
<td>$102.10</td>
<td>$104.65</td>
<td>$107.27</td>
</tr>
<tr>
<td>Information Assurance Engineer SME</td>
<td>$179.95</td>
<td>$184.45</td>
<td>$189.06</td>
<td>$193.79</td>
<td>$198.63</td>
</tr>
<tr>
<td>Information Assurance Engineer V</td>
<td>$165.29</td>
<td>$169.42</td>
<td>$173.66</td>
<td>$178.00</td>
<td>$182.45</td>
</tr>
<tr>
<td>Information Assurance Engineer IV</td>
<td>$141.46</td>
<td>$145.00</td>
<td>$148.62</td>
<td>$152.34</td>
<td>$156.15</td>
</tr>
<tr>
<td>Information Assurance Engineer II</td>
<td>$117.28</td>
<td>$120.21</td>
<td>$123.22</td>
<td>$126.30</td>
<td>$129.45</td>
</tr>
<tr>
<td>Information Assurance Engineer I</td>
<td>$89.02</td>
<td>$91.24</td>
<td>$93.52</td>
<td>$95.86</td>
<td>$98.26</td>
</tr>
<tr>
<td>Program Manager V</td>
<td>$182.36</td>
<td>$186.92</td>
<td>$191.60</td>
<td>$196.39</td>
<td>$201.30</td>
</tr>
<tr>
<td>Project Manager IV</td>
<td>$140.33</td>
<td>$143.83</td>
<td>$147.43</td>
<td>$151.11</td>
<td>$154.89</td>
</tr>
<tr>
<td>Project Manager III</td>
<td>$120.69</td>
<td>$123.71</td>
<td>$126.80</td>
<td>$129.97</td>
<td>$133.22</td>
</tr>
<tr>
<td>Project Manager I</td>
<td>$92.63</td>
<td>$94.95</td>
<td>$97.32</td>
<td>$99.75</td>
<td>$102.25</td>
</tr>
<tr>
<td>Emergency Engineer SME</td>
<td>$327.96</td>
<td>$336.16</td>
<td>$344.56</td>
<td>$353.18</td>
<td>$362.01</td>
</tr>
<tr>
<td>IT Architect Engineer SME</td>
<td>$182.72</td>
<td>$187.29</td>
<td>$191.97</td>
<td>$196.77</td>
<td>$201.69</td>
</tr>
<tr>
<td>IT Architect Engineer IV</td>
<td>$166.15</td>
<td>$170.30</td>
<td>$174.56</td>
<td>$178.92</td>
<td>$183.39</td>
</tr>
<tr>
<td>IT Architect Engineer II</td>
<td>$141.46</td>
<td>$145.00</td>
<td>$148.62</td>
<td>$152.34</td>
<td>$156.15</td>
</tr>
<tr>
<td>IT Engineer III</td>
<td>$137.39</td>
<td>$140.83</td>
<td>$144.35</td>
<td>$147.96</td>
<td>$151.66</td>
</tr>
<tr>
<td>IT Engineer II</td>
<td>$120.59</td>
<td>$123.61</td>
<td>$126.70</td>
<td>$129.87</td>
<td>$133.11</td>
</tr>
<tr>
<td>IT Engineer I</td>
<td>$101.00</td>
<td>$103.53</td>
<td>$106.11</td>
<td>$108.77</td>
<td>$111.49</td>
</tr>
<tr>
<td>IT Requirements Analyst V</td>
<td>$138.10</td>
<td>$141.55</td>
<td>$145.09</td>
<td>$148.72</td>
<td>$152.44</td>
</tr>
<tr>
<td>IT Requirements Analyst III</td>
<td>$115.21</td>
<td>$118.09</td>
<td>$121.04</td>
<td>$124.07</td>
<td>$127.17</td>
</tr>
<tr>
<td>IT Requirements Analyst I</td>
<td>$93.54</td>
<td>$95.88</td>
<td>$98.28</td>
<td>$100.74</td>
<td>$103.25</td>
</tr>
<tr>
<td>System Security Engineer SME</td>
<td>$182.40</td>
<td>$186.96</td>
<td>$191.63</td>
<td>$196.42</td>
<td>$201.33</td>
</tr>
<tr>
<td>System Security Engineer V</td>
<td>$167.00</td>
<td>$171.18</td>
<td>$175.46</td>
<td>$179.84</td>
<td>$184.34</td>
</tr>
<tr>
<td>System Security Engineer IV</td>
<td>$156.31</td>
<td>$160.22</td>
<td>$164.23</td>
<td>$168.33</td>
<td>$172.54</td>
</tr>
<tr>
<td>System Security Engineer III</td>
<td>$140.33</td>
<td>$143.83</td>
<td>$147.43</td>
<td>$151.11</td>
<td>$154.89</td>
</tr>
<tr>
<td>System Security Engineer II</td>
<td>$121.68</td>
<td>$124.72</td>
<td>$127.84</td>
<td>$131.04</td>
<td>$134.31</td>
</tr>
<tr>
<td>Information Assurance Analyst SME</td>
<td>$156.31</td>
<td>$160.22</td>
<td>$164.23</td>
<td>$168.33</td>
<td>$172.54</td>
</tr>
<tr>
<td>Information Assurance Analyst V</td>
<td>$139.68</td>
<td>$143.17</td>
<td>$146.75</td>
<td>$150.42</td>
<td>$154.18</td>
</tr>
<tr>
<td>Information Assurance Analyst IV</td>
<td>$123.57</td>
<td>$126.66</td>
<td>$129.83</td>
<td>$133.08</td>
<td>$136.40</td>
</tr>
<tr>
<td>Information Assurance Analyst III</td>
<td>$115.21</td>
<td>$118.09</td>
<td>$121.04</td>
<td>$124.07</td>
<td>$127.17</td>
</tr>
<tr>
<td>Information Assurance Analyst I</td>
<td>$89.02</td>
<td>$91.24</td>
<td>$93.52</td>
<td>$95.86</td>
<td>$98.26</td>
</tr>
<tr>
<td>System Administrator SME</td>
<td>$141.13</td>
<td>$144.65</td>
<td>$148.27</td>
<td>$151.98</td>
<td>$155.78</td>
</tr>
<tr>
<td>System Administrator III</td>
<td>$103.13</td>
<td>$105.71</td>
<td>$108.35</td>
<td>$111.06</td>
<td>$113.83</td>
</tr>
<tr>
<td>System Administrator I</td>
<td>$89.02</td>
<td>$91.24</td>
<td>$93.52</td>
<td>$95.86</td>
<td>$98.26</td>
</tr>
<tr>
<td>SW Engineer V</td>
<td>$147.47</td>
<td>$151.16</td>
<td>$154.93</td>
<td>$158.81</td>
<td>$162.78</td>
</tr>
<tr>
<td>SW Engineer III</td>
<td>$121.84</td>
<td>$124.88</td>
<td>$128.00</td>
<td>$131.20</td>
<td>$134.48</td>
</tr>
<tr>
<td>Cloud Engineer V</td>
<td>$185.69</td>
<td>$190.34</td>
<td>$195.09</td>
<td>$199.97</td>
<td>$204.97</td>
</tr>
<tr>
<td>Cloud Engineer III</td>
<td>$142.93</td>
<td>$146.51</td>
<td>$150.17</td>
<td>$153.92</td>
<td>$157.77</td>
</tr>
<tr>
<td>Cloud Engineer II</td>
<td>$120.53</td>
<td>$123.55</td>
<td>$126.64</td>
<td>$129.80</td>
<td>$133.05</td>
</tr>
<tr>
<td>Data Scientist IV</td>
<td>$157.93</td>
<td>$161.87</td>
<td>$165.92</td>
<td>$170.07</td>
<td>$174.32</td>
</tr>
<tr>
<td>Labor Category</td>
<td>year 1</td>
<td>year 2</td>
<td>year 3</td>
<td>year 4</td>
<td>year 5</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
</tr>
<tr>
<td>Data Scientist II</td>
<td>$121.78</td>
<td>$124.82</td>
<td>$127.94</td>
<td>$131.14</td>
<td>$134.42</td>
</tr>
<tr>
<td>Data Req Analyst III</td>
<td>$120.59</td>
<td>$123.61</td>
<td>$126.70</td>
<td>$129.87</td>
<td>$133.11</td>
</tr>
<tr>
<td>Data Req Analyst II</td>
<td>$100.91</td>
<td>$103.44</td>
<td>$106.02</td>
<td>$108.67</td>
<td>$111.39</td>
</tr>
</tbody>
</table>