GENERAL SERVICES ADMINISTRATION
FEDERAL SUPPLY SERVICE
AUTHORIZED FEDERAL SUPPLY SCHEDULE PRICE LIST

MULTIPLE AWARD SCHEDULE (MAS)

ENTRUST GOVERNMENT SOLUTIONS

935 GRAVIER STREET, SUITE 1840
NEW ORLEANS, LA 70112
PHONE: 504-308-1464
FAX: 504-814-8440
EMAIL: GSASchedule70@entrustsolutions.com
WEB: www.entrustsolutions.com

CONTRACT NUMBER: 47QTCA20D00FK

PERIOD COVERED BY CONTRACT:
September 25, 2020 through September 24, 2025

BUSINESS SIZE: SMALL, Veteran-Owned Small Business

CUSTOMER CONTACT:
Christian Mobley, President
504-323-7084, chris.mobley@entrustsolutions.com

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

TABLE OF CONTENTS

INFORMATION FOR ORDERING ACTIVITIES 1
1. Contract Information 1
2. Maximum Order 1
3. Minimum Order 1
4. Geographic Coverage 1
5. Point of Production 1
6. Discount 1
7. Volume Discounts 1
8. Prompt Payment Terms 1
9. Government Purchase Cards 1
10. Foreign Items 1
11. a. Time of Delivery 2
11. b. Expedited Time of Delivery 2
12. FOB Shipping Terms 2
13. Ordering Address 2
14. Payment Address 2
15. Warranty Provision 2
16. Export Packaging Charges 2
17. Terms & Conditions for Government Purchase Cards 2
18. Terms & Conditions of Rental, Maintenance & Repair 2
19. Installation 2
20. Repair Parts 2
20. A. Other Services 2
21. Service & Distribution Points 3
22. Participating Dealers 3
23. Preventive Maintenance 3
24. Special Attributes such as Environmental Attributes 3
25. DUNS Number 3
26. CAGE 3

TERMS AND CONDITIONS APPLICABLE TO HIGHLY ADAPTIVE CYBERSECURITY SERVICES: SPECIAL ITEM NUMBER 54151HACS 4
1. Scope 5
2. Order 5
3. Performance of Services 5
4. Inspection of Services 6
5. Responsibilities of the Contractor 6
6. Responsibilities of the Ordering Activity 6
7. Independent Contractor 6
8. Organizational Conflicts of Interest 6
9. Invoices 7
10. Resumes 7
11. Approval of Subcontracts 7
12. Description of Highly Adaptive Cybersecurity Services and Pricing 7
TERMS AND CONDITIONS APPLICABLE TO INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES: SPECIAL ITEM NUMBER 54151S 8
1. Scope 8
2. Performance Incentives 8
3. Order 8
4. Performance of Services 8
5. Stop-Work Order (FAR 52.242-15) (Aug 1989) 9
6. Inspection of Services 10
7. Responsibilities of the Contractor 10
8. Responsibilities of the Ordering Activity 10
9. Independent Contractor 10
10. Organizational Conflicts of Interest 10
11. Invoices 11
12. Payments 11
13. Resumes 11
14. Incidental Support Costs 11
15. Approval of Subcontracts 12
LABOR CATEGORIES 13
1. SIN 54151HACS 13

Cyber Security Principal 13
Cyber Security Senior Manager 14
Cyber Security Manager II 14
Cyber Security Manager I 15
Cyber Security Senior Staff 17
Cyber Security Technology Staff 17
Cyber Security Associate Staff 18
Cyber Security Support Staff 19
2. SIN 54151S 20
IT Principal 20
IT Senior Manager 21
IT Manager II 22
IT Manager I 23
IT Senior Staff 24
IT Technology Staff 24
IT Associate Staff 25
IT Support Staff 26
IT Degree / Experience Equivalency 27
LABOR PRICING: 54151HACS SIN 28
LABOR PRICING: 54151S SIN 29

INFORMATION FOR ORDERING ACTIVITIES

1. Contract Information

Business Size: Small
Contract Number: 47QTCA20D00FK
Contract Period: September 25, 2020 through September 24, 2025
Schedule Number: 70 Information Technology
Special Item Number:
54151S: IT Professional Services
54151HACS: Highly Adaptive Cybersecurity Services

2. Maximum Order

$500,000

3. Minimum Order

$100

4. Geographic Coverage

Worldwide

5. Point of Production

Same as Contractor

6. Discount

Government net prices (discounts already deducted)

7. Volume Discounts

1% off Orders over $350K

8. Prompt Payment Terms

1% if Payment made within 10 days, Net 30 Days

9. Government Purchase Cards

The Government Purchase Card will be accepted for payment on orders below the micro-purchase threshold.

10. Foreign Items

None

11. a. Time of Delivery

Negotiated at Time of Order

11. b. Expedited Time of Delivery

Negotiated at Time of Order

12. FOB Shipping Terms

Destination

13. Ordering Address

Entrust Government Solutions
935 Gravier Street, Suite 1840
New Orleans, LA 70112

14. Payment Address

Entrust Government Solutions
935 Gravier Street, Suite 1840
New Orleans, LA 70112

15. Warranty Provision

Contractor's standard commercial warranty.

16. Export Packaging Charges

N/A

17. Terms & Conditions for Government Purchase Cards

None

18. Terms & Conditions of Rental, Maintenance & Repair

N/A

19. Installation

N/A

20. Repair Parts

N/A

20. A. Other Services

N/A

21. Service & Distribution Points

N/A

22. Participating Dealers

N/A

23. Preventive Maintenance

N/A

24. Special Attributes such as Environmental Attributes

N/A

25. DUNS Number

08-069-6986

26. CAGE

7WZ02

TERMS AND CONDITIONS APPLICABLE TO HIGHLY ADAPTIVE CYBERSECURITY SERVICES: SPECIAL ITEM NUMBER 54151HACS

Vendor suitability for offering services through the Highly Adaptive Cybersecurity Services (HACS) SINs 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-06-19 - Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments
- OMB Memorandum M -07-16 - Safeguarding Against and Responding to the Breach of Personally Identifiable Information
- OMB Memorandum M-16-03 - Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements
- OMB Memorandum M-16-04 – Cybersecurity Implementation Plan (CSIP) for Federal Civilian Government
- The Cybersecurity National Action Plan (CNAP)
- NIST SP 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems
- NIST SP 800-27A - Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
- NIST SP 800-30 - Guide for Conducting Risk Assessments
- NIST SP 800-35 - Guide to Information Technology Security Services
- NIST SP 800-37 - Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- NIST SP 800-39 - Managing Information Security Risk: Organization, Mission, and Information System View
- NIST SP 800-44 - Guidelines on Securing Public Web Servers
- NIST SP 800-48 - Guide to Securing Legacy IEEE 802.11 Wireless Networks
- NIST SP 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-61 - Computer Security Incident Handling Guide
- NIST SP 800-64 - Security Considerations in the System Development Life Cycle
- NIST SP 800-82 - Guide to Industrial Control Systems (ICS)Security
- NIST SP 800-86 - Guide to Integrating Forensic Techniques into Incident Response
- NIST SP 800-115 - Technical Guide to Information Security Testing and Assessment
- NIST SP 800-128 - Guide for Security-Focused Configuration Management of Information Systems
- NIST SP 800-137 - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- NIST SP 800-153 - Guidelines for Securing Wireless Local Area Networks (WLANs)

- NIST SP 800-171 - 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 Numbers 54151HACS High Adaptive Cybersecurity Services apply exclusively to High Adaptive Cybersecurity Services within the scope of this Multiple Award Schedule.
b. Services under these SINs are limited to Highly Adaptive Cybersecurity Services only. Software and hardware products are under different Special Item Numbers on Multiple Award Schedule (e.g. 511210 and 33411) and may be quoted along with services to provide a total solution.
c. These SINs provide ordering activities with access to Highly Adaptive Cybersecurity services only.
d. Highly Adaptive Cybersecurity Services provided under these SINs shall comply with all Cybersecurity certifications and industry standards as applicable pertaining to the type of services as specified by ordering agency.
e. The Contractor shall provide services at the Contractor's facility and/or at the ordering activity location, as agreed to by the Contractor and the ordering activity.

2. Order

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

3. Performance of Services

a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity. All Contracts will be fully funded.
b. The Contractor agrees to render services 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 (MAY 2015) (ALTERNATE II – JUL 2009) (FAR DEVIATION – JUL 2015) (TAILORED) for Firm-Fixed Price and Time-and-Materials and Labor-Hour Contracts orders placed under this contract.

5. Responsibilities of the Contractor

The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character. If the end product of a task order is software, then FAR 52.227-14 (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's 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's 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

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.

TERMS AND CONDITIONS APPLICABLE TO INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES: SPECIAL ITEM NUMBER 54151S

1. Scope

a. The prices, terms and conditions stated under Special Item Number 54151S Information Technology Professional Services apply exclusively to IT Services within the scope of this Multiple Award Schedule.
b. The Contractor shall provide services at the Contractor's facility and/or at the ordering activity location, as agreed to by the Contractor and the ordering activity.

2. Performance Incentives

a. Performance incentives may be agreed upon between the Contractor and the ordering activity on individual fixed price orders or Blanket Purchase Agreements under this contract in accordance with this clause.
b. The ordering activity must establish a maximum performance incentive price for these services and/or total solutions on individual orders or Blanket Purchase Agreements.
c. Incentives should be designed to relate results achieved by the contractor to specified targets. To the maximum extent practicable, ordering activities shall consider establishing incentives where performance is critical to the ordering activity's mission and incentives are likely to motivate the contractor. Incentives shall be based on objectively measurable tasks.

3. Order

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

4. Performance of Services

a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity.
b. The Contractor agrees to render services only during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.

c. The ordering activity should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner.
d. Any Contractor travel required in the performance of IT 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)

a. The Contracting Officer may, at any time, by written order to the Contractor, require the Contractor to stop all, or any part, of the work called for by this contract for a period of 90 days after the order is delivered to the Contractor, and for any further period to which the parties may agree. The order shall be specifically identified as a stop-work order issued under this clause. Upon receipt of the order, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the order during the period of work stoppage. Within a period of 90 days after a stop-work is delivered to the Contractor, or within any extension of that period to which the parties shall have agreed, the Contracting Officer shall either-
   i. Cancel the stop-work order; or
   ii. Terminate the work covered by the order as provided in the Default, or the Termination for Convenience of the Government, clause of this contract.
b. If a stop-work order issued under this clause is canceled or the period of the order or any extension thereof expires, the Contractor shall resume work. The Contracting Officer shall make an equitable adjustment in the delivery schedule or contract price, or both, and the contract shall be modified, in writing, accordingly, if-
   i. 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
   ii. The Contractor asserts its right to the adjustment within 30 days after the end of the period of work stoppage; provided, that, if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon the claim submitted at any time before final payment under this contract.
c. If a stop-work order is not canceled and the work covered by the order is terminated for the convenience of the Government, the Contracting Officer shall allow reasonable costs resulting from the stop-work order in arriving at the termination settlement.
d. If a stop-work order is not canceled and the work covered by the order is terminated for default, the Contracting Officer shall allow, by equitable adjustment or otherwise, reasonable costs resulting from the stop-work order.

6. Inspection of Services

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

7. Responsibilities of the Contractor

The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character. If the end product of a task order is software, then FAR 52.227-14 (Deviation – May 2003) Rights in Data – General, may apply.

8. Responsibilities of the Ordering Activity

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

9. Independent Contractor

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

10. Organizational Conflicts of Interest

a. Definitions. "Contractor" means the person, firm, unincorporated association, joint venture, partnership, or corporation that is a party to this contract. "Contractor and its affiliates" and "Contractor or its affiliates" refers to the Contractor, its chief executives, directors, officers, subsidiaries, affiliates, subcontractors at any tier, and consultants and any joint venture involving the Contractor, any entity into or with which the Contractor subsequently merges or affiliates, or any other successor or assignee of the Contractor. An "Organizational conflict of interest" exists when the nature of the work to be performed under a proposed ordering activity contract, without some restriction on ordering activities by the Contractor and its affiliates, may either (i) result in an unfair competitive advantage to the Contractor or its affiliates or (ii) impair the Contractor's or its affiliates' objectivity in performing contract work.

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

contract. Examples of situations, which may require restrictions, are provided at FAR 9.508.

11. Invoices

The Contractor, upon completion of the work ordered, shall submit invoices for IT 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:

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

13. Resumes

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

14. Incidental Support Costs

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

15. Approval of Subcontracts

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

LABOR CATEGORIES

1. SIN 54151HACS

Cyber Security Principal

Functional Responsibility: The Cyber Security Principal is an executive leader supporting cyber security, program management or related technology initiatives. Responsibilities and experience typically include executive/program sponsor level relationships, management and direction on customer engagements, experience in project definition and IT systems and technology analysis, and integration of complex technical solutions across organizational and geographic boundaries. The Principal is proficient in project estimation and resource planning efforts and in resolving project issues, such as technical compatibility, client expectations, and cross-organizational challenges. A Principal helps to ensure overall soundness of analytical approach and is able to suggest alternatives. A Principal manages resources and is the liaison and main point of contact with client representatives. Other experience includes coordinating multiple projects and teams and assisting clients in achieving desired program results. Serves as the customer's engagement partner for specific project areas and assumes responsibility for client communications related to communicating technical concerns. Maintains responsibility for formulating work standards, creating strategic project objectives, and managing client issues and feedback. Assumes accountability of allocating resources, supervising resources, and enforcing quality control practices for each project. Responsible for project reviews and overall contract progress and performance. Ability to acquire U.S. Security Clearance preferred but not required.

Specialized Experience: The Cyber Security Principal has experience leading development or management of complex, technical security solutions and/or services while serving in an executive leadership or technical role, such as the Chief Information Security Officer (CISO). Acts as main interface for client-side executives. Advises on enterprise-wide Cyber Security needs, improvements, optimization, or maintenance. May be a Subject Matter Expert (SME) in security operations, vulnerability management, information security and/or incident handling. Role also recommends innovative solutions and promotes emerging Cyber Security research.

Experience: Minimum of twelve (12) years of experience.

Education: Holds a four-year (4) degree from an accredited college or university and may possess advanced degrees and/or IT industry certifications.

* These are minimum requirements, staff that exceed these education and experience requirements may be aligned to the labor categories at Entrust’s discretion.

Cyber Security Senior Manager

Functional Responsibility: The Cyber Security Senior Manager is typically a program manager or cyber security technical expert on projects supporting cyber security, program management, enterprise systems or related technology initiatives. Possesses engagement experience in program scope and approach. Has the ability to drive cyber strategy and planning changes at the executive levels, provides oversight of key information technology enablers, and management of project resources. Maintains responsibility for managing the program team and daily operations of project development or serves in a role as a highly experienced technical expert. Assesses program feasibility with designed solution. Advises partners, principals, and/or executive directors of major developments throughout execution. Reviews work products and oversees the development of IT deliverables, documentation, and reporting. Other responsibilities include communication with client and project managers, management of multiple projects across various commercial and other clients, management of program activities, and serving as a key point of contact with client executives. Assumes responsibility for program delivery and oversight of key technical enablers on projects. Maintains responsibility for technical solutions, resource allocation and delegation and helping to ensure quality standards are achieved throughout program execution. Ability to acquire U.S. Security Clearance preferred but not required.

Specialized Experience: The Cyber Security Senior Manager is a highly experienced, Cyber Security practitioner with specialized training and experience. This role may serve as a program manager or technical expert on customer engagement, providing guidance, business process models, or project approaches to follow, or may offer methods, tools, and techniques that improve client cyber defenses. A CS Senior Manager may lead Cyber Security programs or serve as a Subject Matter Expert (SME) on security operations, vulnerability management, information security or related security domains. The CS Senior Manager typically has specialized credentials such as CISSP, PMP, CISA, CISM or other Cyber Security industry credentials that document their experience and knowledge.

Experience: Minimum of eight (8) years of experience.

Education: Holds a four-year (4) degree from an accredited college or university and may possess advanced degrees and/or IT industry certifications.

* These are minimum requirements, staff that exceed these education and experience requirements may be aligned to the labor categories at Entrust's discretion.

Cyber Security Manager II

Functional Responsibility: The Cyber Security Manager II is typically a senior security project manager, senior security engineer or senior credentialed security

professional on projects supporting cyber security, information technology, enterprise systems or related technology initiatives. Possesses project experience in program scope and approach. Focuses on integration and technical solution delivery. Has the ability to drive cyber strategy and planning changes at the executive levels, provides oversight of key information technology enablers, and management of project resources. Maintains responsibility for managing the project team and daily operations of project development or serves in a role as a highly experienced technical expert. Advises partners, principals, and/or executive directors of all major developments throughout execution. Reviews work products and oversees the development of IT deliverables, documentation, and reporting. Other responsibilities include communication with client and project managers, management of multiple projects across various commercial and public sector clients, management of program activities, and serving as a key point of contact with client executives. Assumes responsibility for program delivery and oversight of key technical enablers on projects and identifies needs for new tools. Assumes responsibility for project delivery and oversight of key technical enablers on projects. Maintains responsibility for technical solutions, resource delegation and helping to ensure quality standards are achieved throughout program execution. Ability to acquire U.S. Security Clearance preferred but not required.

Specialized Experience: The Cyber Security Manager II is a highly experienced, Cyber Security practitioner with specialized training and experience. A CS Manager II may serve as a senior security engineer within a program and provide project and/or technical leadership. A CS Manager II may lead Cyber Security programs or serve as a Subject Matter Expert (SME) on security operations, NIST Risk Management Framework (RMF), vulnerability management, information security or related security domains. The CS Security Manager II typically has specialized credentials such as Navy Qualified Validator Level III (NQV), CISSP, CISM, PMP, CISA, or other Cyber Security industry credentials that document their experience and knowledge.

Experience: Minimum of six (6) years of experience.

Education: Holds a four-year (4) degree from an accredited college or university and may possess advanced degrees and/or IT industry certifications.

* These are minimum requirements, staff that exceed these education and experience requirements may be aligned to the labor categories at Entrust's discretion.

Cyber Security Manager I

Functional Responsibility: The Cyber Security Manager I typically provides project technical leadership and direction on projects including, but not limited to security architecture; cyber security; systems integration; information security; vulnerability operations; data analytics and visualization; and application development and maintenance; Possesses competencies in multiple IT technologies, business processes, or combination of both. Extensive knowledge of and experience in one of

the following: network security, security architecture, security operations, vulnerability management, application security, information security. A Cyber Security Manager devises or modifies procedures to solve complex problems, provides guidance and experience on technical solution implementation, engages resources and/or serves as a team leader, performs analyses of project or client issues, interprets implications of design, and helps to ensure that technical design or service meets business needs. Ability to recommend right techniques/tools for team improvement. Experience with leading and managing team meetings, and a deep understanding of the specific engagement underway. Other experience may include implementing business process reengineering, orchestrating change management principles, and conducting performance measurements. Serves in the role of project team leader over assigned support areas, often filling the position of project team lead and instructing, directing, and monitoring the work of other IT staff, or serves in a role of an experienced technical expert. Conducts analysis of work plan completeness, prepares status reports, and supports quality control practices. Performs analyses of issues, assesses appropriate alternatives, and recommends solutions. Communicates client expectations to project team and escalates appropriate issues to senior-level project staff. Provides structure for IT working groups and teams to maintain focus and productivity. Works closely with group members to enhance team building, communication, interpersonal relations, meetings, and decision making. Maintains technical knowledge within industry. Ability to acquire U.S. Security Clearance preferred but not required.

Specialized Experience: The Cyber Security Manager has prior experience leading Cyber Security project work-streams that implement solutions. A Cyber Security Manager may be a Subject Matter Expert (SME) on a given tool, technology or method being used in a project. A CS Manager may lead a team of security analysts, vulnerability operations analysts, penetration testers or information systems security engineers. A Cyber Security Manager conducts technical planning, supervises staff, reviews, and completes work products, determines objectives, and executes plans. A Cyber Security Manager often has security credentials such as CISSP, CISM, NQV Level II, or another security industry credential. They assess effectiveness of security defenses, facilitate the NIST Risk Management Framework (RFM) to accredit systems, and/or improve those defenses for our clients.

Experience: Minimum of four (4) years of experience.

Education: Holds a four-year (4) degree from an accredited college or university and may possess advanced degrees and/or IT industry certifications.

* These are minimum requirements, staff that exceed these education and experience requirements may be aligned to the labor categories at Entrust’s discretion.

Cyber Security Senior Staff

Functional Responsibility: Cyber Security Senior Staff supports one of the following areas: cyber security, program management, enterprise systems or related technologies. A Cyber Security Senior Staff generally possesses a fundamental understanding of IT implementation and operations management best practices. Leads and supports tasks, including deliverable development, on IT engagements related, but not limited to: technology strategy, architecture and service management; IT security; systems integration; data analytics and visualization; application development and maintenance; help desk operations; and infrastructure/network design and management. Familiarity with client issues, assists with design issues, leads client teams, provides analysis of project data, and assists with the development of appropriate deliverables. Proficient in the use of Entrust tools and supports the overall objectives and goals of the program. Provides senior-level analytical and program support and is focused on providing high performance work. Serves as a senior-level analytical resource within the project team. Applies business modeling, process modeling, and business design techniques. Formulates diagnoses through financial or statistical modeling, assesses appropriate alternatives, and offers conclusions to senior-level project staff. This position performs analyses and makes diagnoses, as well as defines symptoms and problems, and develops conclusions. The ability to acquire U.S. Security Clearance preferred but not required.

Specialized Experience: Cyber Security Senior Staff have prior experience on projects with similar tools, techniques, and methods. Cyber Security Senior Staff may handle the installation of data analytics and visualization tools; A Cyber Security Senior Staff completes more analytical tasks related to security business processes, agency accreditation processes, information security processes and compliance audits. A Cyber Security Senior Staff may have Cyber Security credentials such as CISM, CRISC or CISA, or may possess another security industry credential.

Experience: Minimum of four (4) years of experience.

Education: Holds a four-year (4) degree from an accredited college or university and may possess advanced degrees and/or IT industry certifications.

* These are minimum requirements, staff that exceed these education and experience requirements may be aligned to the labor categories at Entrust's discretion.

Cyber Security Technology Staff

Functional Responsibility: Cyber Security Technology Staff provides technical support to a project in one of the following: security architecture; cyber security; systems integration; information security; vulnerability operations; data analytics and visualization; and application development and maintenance; Ability to support activities in network security, security architecture, security operations, vulnerability

management, application security or information security. Assists with the design and completion of planned tasks, analyzes relevant data and information, and institutes and supports business solutions. Provides technical project support. Completes assigned tasks within the project scope and budget, while meeting deliverable requirements. Serves as a contributing technical resource on the project team. Assumes responsibility for conducting relevant technical research, distilling data, and utilizing research in completing tasks. Actively engages Entrust tools and methodologies to meet project objectives and complete technical activities. Maintains responsibility for quality assurance practices and the completion and accuracy of system documentation. The ability to acquire U.S. Security Clearance preferred but not required.

Specialized Experience: Cyber Security Technology Staff have prior experience working on a Cyber Security project. CS Technology Staff are expected to perform vulnerability assessments, determine approach, and apply vulnerability remediation and mitigation in multiple environments. CS Technology Staff typically have computer science skills, and may assist in vulnerability management operations, writing scripts to automate remediation of vulnerability, applying STIGs, and interpreting security assessment results. May have testing skills and will be part of a penetration testing teams or testing of security automation tools. CS Technology Staff prepare deliverables, which are reviewed by a senior-level project staff, typically works under the guidance of a CS Manager as part of a Cyber Security project team. A CS Technology Staff may have Cyber Security credentials such as CEH, CompTIA Security+, Operating System or other relevant certifications.

Experience: Minimum of two (2) years of experience.

Education: Holds a four-year (4) degree from an accredited college or university and may possess advanced degrees and/or IT industry certifications.

* These are minimum requirements, staff that exceed these education and experience requirements may be aligned to the labor categories at Entrust's discretion.

Cyber Security Associate Staff

Functional Responsibility: Cyber Security Associate Staff provides technical and/or analytical support to a project in one of the following: information technology, cyber security, program management or related technologies. Ability to support activities in network security, security architecture, security operations, vulnerability management, application security or information security. Assists with the design and completion of planned tasks, analyzes relevant data and information, and institutes and supports business solutions. Provides technical and/or analytical project support. Completes assigned tasks within the project scope and budget, while meeting deliverable requirements. Conducts relevant research, distilling data, and utilizing research in completing tasks. Actively engages Entrust tools and methodologies to meet project objectives and complete technical and project deliverables. Maintains responsibility for

quality assurance practices and the completion and accuracy of system documentation. The ability to acquire U.S. Security Clearance preferred but not required.

Specialized Experience: Cyber Security Associate Staff may have prior experience working on a Cyber Security project. CS Associate Staff are expected to perform vulnerability assessments and apply vulnerability remediation tasks on systems, documentation of remediation processes and research of remediation and mitigation techniques. CS Associate Staff typically have computer science skills, and may assist in vulnerability management development operations, writing scripts to automate remediation of vulnerabilities, applying STIGs, and interpreting security assessment results. May have testing skills and will be part of a penetration testing team or testing of security automation tools. CS Associate Staff prepare deliverables, which are reviewed by a senior-level project staff, typically works under the guidance of a CS Manager as part of a Cyber Security project team.

Experience: Minimum of three (3) years of experience.

Education: Holds a two-year associate degree from an accredited college and/or IT industry certification.

* These are minimum requirements, staff that exceed these education and experience requirements may be aligned to the labor categories at Entrust's discretion.

Cyber Security Support Staff

Functional Responsibility: Cyber Security Support Staff provides support to project and technical teams in one or more of the following: conducting research and analysis, technical documentation and developing project deliverables. Has ability to support activities in information technology, security architecture and service management; IT security; systems integration; data analytics and visualization; application development and maintenance; help desk operations; and infrastructure/network design and management. Assists with the completion of planned tasks, analyzes relevant data and information, and institutes and supports business solutions. Completes assigned engagement tasks within the project scope and budget, while meeting deliverable requirements. Conducts relevant research, distilling data, and creating reports. Actively engages Entrust tools and methodologies to meet project objectives and complete technical and project deliverables. Maintains responsibility for quality assurance practices and the completion and accuracy of system documentation. The ability to acquire U.S. Security Clearance preferred but not required.

Specialized Experience: Cyber Security Support Staff may have prior experience working on a Cyber Security project. CS Support Staff are expected to perform vulnerability assessments and apply vulnerability remediation tasks on systems, documentation of remediation processes and research of remediation and mitigation techniques. May have testing skills and will be part of testing of security automation

tools. CS Support Staff prepare deliverables, which are reviewed by a senior-level project staff, typically works under the guidance of a CS Manager as part of a Cyber Security project team.

Experience: Minimum of one (1) year of experience.

Education: Holds a two-year associate degree from an accredited college and/or IT industry certification.

* These are minimum requirements, staff that exceed these education and experience requirements may be aligned to the labor categories at Entrust's discretion.

2. SIN 54151S

IT Principal

Functional Responsibility: The IT Principal is an executive leader supporting Information Technology, program management or related technology initiatives. Responsibilities and experience typically include executive/program sponsor level relationships, management and direction on customer engagements, experience in project definition and IT systems and technology analysis, and integration of complex technical solutions across organizational and geographic boundaries. The Principal is proficient in project estimation and resource planning efforts and in resolving project issues, such as technical compatibility, client expectations, and cross-organizational challenges. A Principal helps to ensure overall soundness of analytical approach and is able to suggest alternatives. A Principal manages resources and is the liaison and main point of contact with client representatives. Other experience includes coordinating multiple projects and teams and assisting clients in achieving desired program results. Serves as the customer's engagement partner for specific project areas and assumes responsibility for client communications related to communicating technical concerns. Maintains responsibility for formulating work standards, creating strategic project objectives, and managing client issues and feedback. Assumes accountability of allocating resources, supervising resources, and enforcing quality control practices for each project. Responsible for project reviews and overall contract progress and performance. Ability to acquire U.S. Security Clearance preferred but not required.

Specialized Experience: The IT Principal has experience leading development or management of complex, technical IT solutions and/or services while serving in an executive leadership or technical role, such as the Chief Information Officer (CISO) or Chief Technology Officer (CTO). The IT Principal acts as main interface for client-side executives and advises on enterprise-wide IT needs, improvements, optimization, or maintenance. May be a Subject Matter Expert (SME) in IT operations, solutions architecture, cloud or other. Role also recommends innovative solutions and promotes emerging IT research.

Experience: Minimum of twelve (12) years of experience.

Education: Holds a four-year (4) degree from an accredited college or university and may possess advanced degrees and/or IT industry certifications.

* These are minimum requirements, staff that exceed these education and experience requirements may be aligned to the labor categories at Entrust's discretion.

IT Senior Manager

Functional Responsibility: The IT Senior Manager is typically a program manager or IT technical expert on projects supporting information technology, program management, enterprise systems or related technology initiatives. Possesses engagement experience in program scope and approach. Has the ability to drive IT strategy and planning changes at the executive levels, provides oversight of key information technology enablers, and management of project resources. Maintains responsibility for managing the program team and daily operations of project development or serves in a role as a highly experienced technical expert. Assesses program feasibility with designed solution. Advises partners, principals, and/or executive directors of major developments throughout execution. Reviews work products and oversees the development of IT deliverables, documentation, and reporting. Other responsibilities include communication with client and project managers, management of multiple projects across various commercial and other clients, management of program activities, and serving as a key point of contact with client executives. Assumes responsibility for program delivery and oversight of key technical enablers on projects. Maintains responsibility for technical solutions, resource allocation and delegation and helping to ensure quality standards are achieved throughout program execution. Ability to acquire U.S. Security Clearance preferred but not required.

Specialized Experience: The IT Senior Manager is a highly experienced, IT practitioner with specialized training and experience. This role may serve as a program manager or technical expert on customer engagement, providing guidance, business process models, or project approaches to follow, or may offer methods, tools, and techniques to meet client objectives. An IT Senior Manager may lead IT programs or serve as a Subject Matter Expert (SME) on complex systems integration projects. The IT Senior Manager typically has specialized credentials such as PMP, CISSP or other IT industry credentials that document their experience and knowledge.

Experience: Minimum of eight (8) years of experience.

Education: Holds a four-year (4) degree from an accredited college or university and may possess advanced degrees and/or IT industry certifications.

* These are minimum requirements, staff that exceed these education and experience requirements may be aligned to the labor categories at Entrust's discretion.

IT Manager II

Functional Responsibility: The IT Manager II is typically a senior IT project manager, senior systems engineer, network engineer or senior credentialed IT professional on projects supporting one of the following areas: Information technology, enterprise systems, cyber security, or related technologies. Possesses project experience in program scope and approach. Focuses on integration and technical solution delivery. Has the ability to drive IT strategy and planning changes at the executive levels, provides oversight of key information technology enablers, and management of project resources. Maintains responsibility for managing the project team and daily operations of project development or serves in a role as a highly experienced technical expert. Advises partners, principals, and/or executive directors of all major developments throughout execution. Reviews work products and oversees the development of IT deliverables, documentation, and reporting. Other responsibilities include communication with client and project managers, management of multiple projects across various commercial and public sector clients, management of program activities, and serving as a key point of contact with client executives. Assumes responsibility for program delivery and oversight of key technical enablers on projects and identifies needs for new tools. Assumes responsibility for project delivery and oversight of key technical enablers on projects. Maintains responsibility for technical solutions, resource delegation and helping to ensure quality standards are achieved throughout program execution. Ability to acquire U.S. Security Clearance preferred but not required.

Specialized Experience: The IT Manager II is a highly experienced, IT practitioner with specialized training and experience. The IT Manager II may serve as a senior system engineer within a program and provide project and/or technical leadership. The IT Manager II may lead IT programs or serve as a Subject Matter Expert (SME) on system integration, systems engineer or operations projects. The IT Security Manager II typically has specialized credentials such as PMP, CISSP other IT industry credentials that document their experience and knowledge.

Experience: Minimum of six (6) years of experience.

Education: Holds a four-year (4) degree from an accredited college or university and may possess advanced degrees and/or IT industry certifications.

* These are minimum requirements, staff that exceed these education and experience requirements may be aligned to the labor categories at Entrust's discretion.

IT Manager I

Functional Responsibility: The IT Manager I typically provide project technical leadership and direction on projects including, but not limited to enterprise and solutions architecture; systems integration; software integration; cyber security; data analytics and visualization; and IT service management. Possesses competencies in multiple IT technologies, business processes, or combination of both. Extensive knowledge of and experience in one of the following: enterprise architecture, security architecture, IT service management, cyber security, systems engineering and/or ITIL. An IT Manager devises or modifies procedures to solve complex problems, provides guidance and experience on technical solution implementation, engages resources and/or serves as a team leader, performs analyses of project or client issues, interprets implications of design, and helps to ensure that technical design or service meets business needs. Ability to recommend right techniques/tools for team improvement. Experience with leading and managing team meetings, and a deep understanding of the specific engagement underway. Other experience includes implementing business process reengineering, orchestrating change management principles, and conducting performance measurements. Serves in the role of project team leader over assigned support areas, often filling the position of project team lead and instructing, directing, and monitoring the work of other IT staff, or serves in a role of an experienced technical expert. Conducts analysis of work plan completeness, prepares status reports, and supports quality control practices. Performs analyses of issues, assesses appropriate alternatives, and recommends solutions. Communicates client expectations to project team and escalates appropriate issues to senior-level project staff. Provides structure for IT working groups and teams to maintain focus and productivity. Works closely with group members to enhance team building, communication, interpersonal relations, meetings, and decision making. Maintains technical knowledge within industry. Ability to acquire U.S. Security Clearance preferred but not required.

Specialized Experience: The IT Manager has prior experience leading IT project work-streams that implement solutions. The IT Manager may be a Subject Matter Expert (SME) on a given tool, technology or method being used in a project. The IT Manager may lead a team of systems analysts, systems engineers, software engineers and/or network engineers in design, development and testing of IT solutions and services. The IT Manager conducts technical planning, supervises staff, reviews, and completes work products, determines objectives, and executes plans. The IT Manager often has credentials such as CompTIA Security+, CCNP, CISSP, MCSE or another industry credential.

Experience: Minimum of four (4) years of experience.

Education: Holds a four-year (4) degree from an accredited college or university and may possess advanced degrees and/or IT industry certifications.

* These are minimum requirements, staff that exceed these education and experience requirements may be aligned to the labor categories at Entrust's discretion.

IT Senior Staff

Functional Responsibility: IT Senior Staff supports one of the following areas: Information technology, program management, enterprise systems or related technologies. IT Senior Staff generally possesses a fundamental understanding of IT implementation and operations management best practices. Leads and supports tasks, including deliverable development, on IT engagements related, but not limited to: technology strategy, architecture and service management; IT security; systems integration; data analytics and visualization; application development and maintenance; help desk operations; and infrastructure/network design and management. Familiarity with client issues, assists with design issues, leads client teams, provides analysis of project data, and assists with the development of appropriate deliverables. Proficient in the use of Entrust tools and supports the overall objectives and goals of the program. Provides senior-level analytical and program support and is focused on providing high performance work. Serves as a senior-level analytical resource within the project team. Applies business modeling, process modeling, and business design techniques. Formulates diagnoses through financial or statistical modeling, assesses appropriate alternatives, and offers conclusions to senior-level project staff. This position performs analyses and makes diagnoses, as well as defines symptoms and problems, and develops conclusions. The ability to acquire U.S. Security Clearance preferred but not required.

Specialized Experience: IT Senior Staff have prior experience on projects with similar tools, techniques, and methods. IT Senior Staff may handle the installation of data analytics and visualization tools; IT Senior Staff complete more analytical tasks related to business objectives and enterprise IT requirements, IT business processes, ITIL, and security and compliance initiatives. IT Senior Staff may have credentials such as CISA, ITILv3 or may possess other industry credential.

Experience: Minimum of four (4) years of experience.

Education: Holds a four-year (4) degree from an accredited college or university and may possess advanced degrees and/or IT industry certifications.

* These are minimum requirements, staff that exceed these education and experience requirements may be aligned to the labor categories at Entrust's discretion.

IT Technology Staff

Functional Responsibility: IT Technology Staff provide technical support to a project in one of the following: Enterprise and solutions architecture; systems integration; software integration; cyber security; data analytics and visualization; and IT service

management. Assists with the design and completion of planned tasks, analyzes relevant data and information, and institutes and supports business solutions. Provides technical project support. Completes assigned tasks within the project scope and budget, while meeting deliverable requirements. Serves as a contributing technical resource on the project team. Assumes responsibility for conducting relevant technical research, distilling data, and utilizing research in completing tasks. Actively engages Entrust tools and methodologies to meet project objectives and complete technical activities. Maintains responsibility for quality assurance practices and the completion and accuracy of system documentation. The ability to acquire U.S. Security Clearance preferred but not required.

Specialized Experience: IT Technology Staff have prior experience working on information technology projects. IT Technology Staff are expected to perform design, configuration, testing, and implementation tasks, recommend technical approaches within project team, and perform root cause analysis to solve technical problems. IT Technology Staff are contributing members in developing and delivering technical solutions and IT services. IT Technology Staff typically have computer science skills, and may assist in development of scripts, software tools or other components of an integrated system. Project deliverables are reviewed by senior-level project staff, typically works under the guidance of an IT Manager as part of an IT project team. IT Technology Staff may have credentials such as CompTIA Security+, CCNA, ITILv3 or may possess other industry credential.

Experience: Minimum of two (2) years of experience.

Education: Holds a four-year (4) degree from an accredited college or university and may possess advanced degrees and/or IT industry certifications.

* These are minimum requirements, staff that exceed these education and experience requirements may be aligned to the labor categories at Entrust's discretion.

IT Associate Staff

Functional Responsibility: IT Associate Staff provide technical and/or analytical support to a project in one of the following: information technology, IT, program management or related technologies. Ability to support activities in enterprise and solutions architecture; systems integration; software integration; cyber security; data analytics and visualization; and IT service management. Assists with the design and completion of planned tasks, analyzes relevant data and information, and institutes and supports business solutions. Provides technical and/or analytical project support. Completes assigned tasks within the project scope and budget, while meeting deliverable requirements. Conducts relevant research, distilling data, and utilizing research in completing tasks. Actively engages Entrust tools and methodologies to meet project objectives and complete technical and project deliverables. Maintains responsibility for quality assurance practices and the completion and accuracy of

system documentation. The ability to acquire U.S. Security Clearance preferred but not required.

Specialized Experience: IT Associate Staff may have prior experience working on IT projects. IT Support Staff are expected to perform systems support and analysis, test validation, IT process development, change management activities and other ITIL related process support. IT Associate Staff typically have computer science skills, and may assist in help desk operations, network operations center operations and other IT facility operations. IT Associate Staff prepare deliverables, which are reviewed by senior-level project staff, typically works under the guidance of an IT Manager as part of an IT project team.

Experience: Minimum of three (3) years of experience.

Education: Holds a two-year associate degree from an accredited college and/or IT industry certification.

* These are minimum requirements, staff that exceed these education and experience requirements may be aligned to the labor categories at Entrust's discretion.

IT Support Staff

Functional Responsibility: IT Support Staff provide support to project and technical teams in one or more of the following: conducting research and analysis, technical documentation and developing project deliverables. Has ability to support activities in support of information technology projects. Assists with the completion of planned tasks, analyzes relevant data and information, and institutes and supports business solutions. Completes assigned engagement tasks within the project scope and budget, while meeting deliverable requirements. Conducts relevant research, distilling data, and creating reports. Actively engages Entrust tools and methodologies to meet project objectives and complete technical and project deliverables. Maintains responsibility for quality assurance practices and the completion and accuracy of system documentation. The ability to acquire U.S. Security Clearance preferred but not required.

Specialized Experience: IT Support Staff may have prior experience working on an IT project. IT Support Staff are expected to perform systems administration, documentation and research required for assigned project tasks. May have broad range of skills that can be used in variety of domains within an IT project to included but not limited to systems administration, vulnerability management, technical writing, testing, installation, and others. IT Support Staff prepare deliverables, which are reviewed by senior-level project staff, typically works under the guidance of an IT Manager as part of an IT project team.

Experience: Minimum of one (1) year of experience.

Education: Holds a two-year associate degree from an accredited college and/or IT industry certification.

* These are minimum requirements, staff that exceed these education and experience requirements may be aligned to the labor categories at Entrust's discretion.

IT Degree / Experience Equivalency

The labor category descriptions describe the functional responsibilities and education and experience requirements for each labor category. These requirements are a guide to the types of experience and educational background of typical personnel in each labor category. Education and experience may be substituted for each other. Each year of relevant experience may be substituted for 1 year of education, and vice versa. In addition, certifications, professional licenses, and vocational technical training may be substituted for experience or education with the written approval of the ordering activity.

Degree	Experience Equivalence*	Other Experience
Associates	1 year of relevant experience.	Vocational or technical training in work-related field.
Bachelor's	Associates degree + 2 years of relevant experience or 4 years of relevant experience.	Professional certification.
Master's	Bachelor's degree + 2 years of relevant experience, or Associates degree + 4 years of relevant experience.	Professional license.
Doctorate	Master's degree + 2 years of relevant experience, or Bachelor's degree + 4 years of relevant experience.	

**** Successful completion of each year of higher education that has not yet resulted in a degree may be counted 1-for-1 for a year of experience.***

Staff must meet the minimum qualifications of the labor categories as defined or qualify via the experience equivalence outlined above. Entrust may, at our discretion, map staff that exceed the minimum associated with each labor category. Labor category qualifications set the minimum requirement necessary to qualify to perform services. The labor category qualifications do not set an education or experience ceiling.

Further, both parties recognize that, on occasion, there may be a need to waive the requirements in order to use the best individual for the task. Therefore, waivers to the education/experience requirements may be granted by either the task order contracting officer or contracting officer technical representative. If such a waiver is included in our proposal, award of said proposal shall be deemed a grant of the waiver.

LABOR PRICING: 54151HACS SIN

SIN	Labor Category	Contract Year 1	Contract Year 2	Contract Year 3	Contract Year 4	Contract Year 5
54151HACS	Cyber Security Principal	$ 200.34	$ 205.35	$ 210.48	$ 215.74	$ 221.14
54151HACS	Cyber Security Senior Manager	$ 174.37	$ 178.73	$ 183.20	$ 187.78	$ 192.47
54151HACS	Cyber Security Manager II	$ 150.26	$ 154.01	$ 157.86	$ 161.81	$ 165.85
54151HACS	Cyber Security Manager I	$ 129.85	$ 133.10	$ 136.42	$ 139.83	$ 143.33
54151HACS	Cyber Security Senior Staff	$ 113.16	$ 115.98	$ 118.88	$ 121.86	$ 124.90
54151HACS	Cyber Security Technology Staff	$ 97.39	$ 99.82	$ 102.32	$ 104.88	$ 107.50
54151HACS	Cyber Security Associate Staff	$ 84.40	$ 86.51	$ 88.68	$ 90.89	$ 93.16
54151HACS	Cyber Security Support Staff	$ 73.27	$ 75.10	$ 76.98	$ 78.91	$ 80.88

LABOR PRICING: 54151S SIN

SIN	Labor Category	Contract Year 1	Contract Year 2	Contract Year 3	Contract Year 4	Contract Year 5
54151S	IT Principal	$ 200.34	$ 205.35	$ 210.48	$ 215.74	$ 221.14
54151S	IT Senior Manager	$ 174.37	$ 178.73	$ 183.20	$ 187.78	$ 192.47
54151S	IT Manager II	$ 150.26	$ 154.01	$ 157.86	$ 161.81	$ 165.85
54151S	IT Manager I	$ 129.85	$ 133.10	$ 136.42	$ 139.83	$ 143.33
54151S	IT Senior Staff	$ 113.16	$ 115.98	$ 118.88	$ 121.86	$ 124.90
54151S	IT Technology Staff	$ 97.39	$ 99.82	$ 102.32	$ 104.88	$ 107.50
54151S	IT Associate Staff	$ 84.40	$ 86.51	$ 88.68	$ 90.89	$ 93.16
54151S	IT Support Staff	$ 73.27	$ 75.10	$ 76.98	$ 78.91	$ 80.88