GENERAL SERVICES ADMINISTRATION
Federal Supply Service
Authorized Federal Supply Schedule Price List

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

WORLDWIDE FEDERAL SUPPLY SCHEDULE CONTRACT FOR
FSC GROUP Class 70
COMMODITY: Information Technology Supplies
FSC CLASS(ES)/PRODUCT CODE(S): 7010
STANDARD INDUSTRY GROUP: 70
SERVICE: Information Technology Professional Services
SERVICE CODE(S): D302

SIN 54151HACS Highly Adaptable Cybersecurity Services (HACS)
SIN 54151S IT Professional Services

Contract number: GS-35F-525GA
Modification # PA0015 Effective date June 7, 2022
Contract period: July 7, 2022-July 6, 2027

XOR SECURITY LLC
11394 Amber Hills Ct
Fairfax, VA 22033
Tel: 703-650-8853
Fax: 1-888-803-6040
Web Address: www.xorsecurity.com

Contract administration source (if different from preceding entry): Razwan Raja, Managing Member

Business size: 8(a) Certified SDB

Cage Code: 4SUJ4

For more information on ordering from Federal Supply Schedules click on the FSS Schedules button at fss.gsa.gov.
(ii) CUSTOMER INFORMATION:

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

SIN 54151HACS Highly Adaptable Cyber-security Services
SIN 54151S IT Professional Services

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.

SIN 54151HACS Computer Forensic and Intrusion Analyst I $114.39
SIN 54151S Business Systems Process Analyst I $86.49

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. See page 14.

2. Maximum order: $500,000.

3. Minimum order: None

4. Geographic coverage: US and territories

5. Point(s) of production: N/A

6. Prices herein are Net, discount has been taken.

7. Quantity discounts: None

8. Prompt payment terms: Net 30

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

9b. Notification whether Government purchase cards are accepted above the micro-purchase threshold: Yes, up to $25,000.

10. Foreign items: None

11a. Time of delivery: To be determined at the task order.

11b. Expedited Delivery: Contact contractor

11c. Overnight and 2-day delivery: None

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

12. F.O.B. point(s): N/A
13a. Ordering address(es): XOR Security LLC  
11394 Amber Hills Ct.  
Fairfax, VA 22033  
Tel: 703-650-8853  
Fax: 888-803-6040

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: XOR Security LLC  
11394 Amber Hills Ct.  
Fairfax, VA 22033  
Tel: 703-650-8853  
Fax: 888-803-6040

15. Warranty provision.

16. Export packing charges: N/A

17. Terms and conditions of Government purchase card acceptance above the micro-purchase level up to $25,000.

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: Professional Services offered under SINs herein

21. List of service and distribution points : Contact Contractor

22. List of participating dealers : N/A

23. Preventive maintenance : N/A

24a. Special attributes such as environmental attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants): 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. UEI number - NV1MK89XJ2J7

26. Notification regarding registration in System for Award Management (SAM) Database: Current
1. SCOPE
   a. The prices, terms and conditions stated under Special Item Number 54151S Information Technology Professional Services apply exclusively to IT Professional Services within the scope of this Information Technology Schedule.
   
   b. The Contractor shall provide services at the Contractor’s facility and/or at the ordering activity location, as agreed to by the Contractor and the ordering activity.

2. PERFORMANCE INCENTIVES I-FSS-60 Performance Incentives (April 2000)
   a. Performance incentives may be agreed upon between the Contractor and the ordering activity on individual fixed price orders or Blanket Purchase Agreements under this contract.
   b. The ordering activity must establish a maximum performance incentive price for these services and/or total solutions on individual orders or Blanket Purchase Agreements.
   c. Incentives should be designed to relate results achieved by the contractor to specified targets. To the maximum extent practicable, ordering activities shall consider establishing incentives where performance is critical to the ordering activity’s mission and incentives are likely to motivate the contractor. Incentives shall be based on objectively measurable tasks.

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-

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

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

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

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

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

6. INSPECTION OF SERVICES


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

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 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:

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

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

(1) The offeror;

(2) Subcontractors; and/or
(3) Divisions, subsidiaries, or affiliates of the offeror under a common control.

13. **RESUMES**

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

14. **INCIDENTAL SUPPORT COSTS**

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

15. **APPROVAL OF SUBCONTRACTS**

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

16. **DESCRIPTION OF IT PROFESSIONAL SERVICES AND PRICING**

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

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

The following is an example of the manner in which the description of a commercial job title should be presented:

**EXAMPLE:** Commercial Job Title: System Engineer

Minimum/General Experience: Three (3) years of technical experience which applies to systems analysis and design techniques for complex computer systems. Requires competence in all phases of systems analysis techniques, concepts and methods; also requires knowledge of available hardware, system software, input/output devices, structure and management practices.

Functional Responsibility: Guides users in formulating requirements, advises alternative approaches, conducts feasibility studies.

Minimum Education: Bachelor’s Degree in Computer Science
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 800-44 - 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 800-171 - 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 Information Technology Schedule.

b. Services under these SINs are limited to Highly Adaptive Cybersecurity Services only. Software and hardware products are under different Special Item Numbers (e.g. 511210, 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**


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**

a. The Contractor shall provide a description of each type of Highly Adaptive Cybersecurity Service offered under Special Item Numbers 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.

The following is an example of the manner in which the description of a commercial job title should be presented (see SCP FSS 004)

**EXAMPLE**

Commercial Job Title: Computer Network Defense Analysis

Description: Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

Professionals involved in this specialty perform the following tasks:

- Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities
- Provide daily summary reports of network events and activity relevant to Computer Network Defense practices
Monitor external data sources (e.g., Computer Network Defense vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of Computer Network Defense threat condition and determine which security issues may have an impact on the enterprise.

Knowledge, Skills and Abilities: Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws, etc.), statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed.

Minimum Experience: 5 Years

Minimum Education Requirements: a bachelor's of science degree with a concentration in computer science cybersecurity services, management information systems (MIS), engineering or information science is essential.

Highly Desirable: Offensive Security Certified Professional (OSCP) or commercial Cybersecurity advanced certification(s).
## XOR Security Labor Categories Descriptions

<table>
<thead>
<tr>
<th>SIN</th>
<th>SERVICE PROPOSED (e.g. Job Title/Task)</th>
<th>Description</th>
<th>MINIMUM EDUCATION/CERTIFICATION LEVEL</th>
<th>MINIMUM YEARS OF EXPERIENCE</th>
</tr>
</thead>
</table>
| 54151S| Business Systems / Process Analyst I                       | **Shall have experience in formulating and defining systems scope and objectives based on both user needs and a thorough understanding of business systems and industry requirements. Defines and architects business rules for complex programs such as Security Operations Centers, and Mission Support Programs.**  
   a) Devises or modifies procedures to solve complex problems considering computer equipment capacity and limitations, operation time, and form of desired results.  
   b) Provides analysis of business and user needs, documentation of requirements, and translation into proper system requirements specifications and security requirements as mandated by Federal regulations and best practices.  
   c) Provides consultation on complex projects and is considered to be the top level contributor/specialist of most phases of systems analysis, while considering the business implications of the application of technology to the current and future business environment. | Bachelors                            | 0+                           |
| 54151S| Business Systems / Process Analyst II                      | **Shall have three (3) years experience in formulating and defining systems scope and objectives based on both user needs and a thorough understanding of business systems and industry requirements. Defines and architects business rules for complex programs such as Security Operations Centers, and Mission Support Programs.**  
   a) Devises or modifies procedures to solve complex problems considering computer equipment capacity and limitations, operation time, and form of desired results.  
   b) Provides analysis of business and user needs, documentation of requirements, and translation into proper system requirements specifications and security requirements as mandated by Federal regulations and best practices.  
   c) Provides consultation on complex projects and is considered to be the top level contributor/specialist of most phases of systems analysis, while considering the business implications of the application of technology to the current and future business environment.  
   d) Applies information assurance expertise to support the development of Information Assurance artifacts to support Risk Management Framework process. | Bachelors +                          | 3+                           |
<table>
<thead>
<tr>
<th>SIN</th>
<th>SERVICE PROPOSED (e.g. Job Title/Task)</th>
<th>Description</th>
<th>MINIMUM EDUCATION/ CERTIFICATION LEVEL</th>
<th>MINIMUM YEARS OF EXPERIENCE</th>
</tr>
</thead>
</table>
| 54151S| Business Systems / Process Analyst III | Shall have seven (7) experience in formulating and defining systems scope and objectives based on both user needs and a thorough understanding of business systems and industry requirements. Defines and architects business rules for complex programs such as Security Operations Centers, and Mission Support Programs.  
  a) Devises or modifies procedures to solve complex problems considering computer equipment capacity and limitations, operation time, and form of desired results.  
  b) Provides analysis of business and user needs, documentation of requirements, and translation into proper system requirements specifications and security requirements as mandated by Federal regulations and best practices.  
  c) Provides consultation on complex projects and is considered to be the top level contributor/specialist of most phases of systems analysis, while considering the business implications of the application of technology to the current and future business environment.  
  d) Applies information assurance expertise to support the development of Information Assurance artifacts to support Risk Management Framework process.  
  e) Supports Risk Assessments and Audits, as well as Compliance Assessments | Bachelors + | 5+ |
# XOR Security Labor Categories Descriptions

<table>
<thead>
<tr>
<th>SIN</th>
<th>SERVICE PROPOSED (e.g. Job Title/Task)</th>
<th>Description</th>
<th>MINIMUM EDUCATION/CERTIFICATION LEVEL</th>
<th>MINIMUM YEARS OF EXPERIENCE</th>
</tr>
</thead>
</table>
| 54151S | Business Systems / Process Analyst IV | Shall have ten (10) years experience in formulating and defining systems scope and objectives based on both user needs and a thorough understanding of business systems and industry requirements. Defines and architects business rules for complex programs such as Security Operations Centers, and Mission Support Programs.  
  a) Devises or modifies procedures to solve complex problems considering computer equipment capacity and limitations, operation time, and form of desired results.  
  b) Provides analysis of business and user needs, documentation of requirements, and translation into proper system requirements specifications and security requirements as mandated by Federal regulations and best practices.  
  c) Provides consultation on complex projects and is considered to be the top level contributor/specialist of most phases of systems analysis, while considering the business implications of the application of technology to the current and future business environment.  
  d) Applies information assurance expertise to support the development of Information Assurance artifacts to support Risk Management Framework process.  
  e) Supports Risk Assessments and Audits, as well as Compliance Assessments  
  f) Documents Information Assurance and System Engineering artifacts in support of IA and Acquisition life cycle | Bachelors + | 7+ |
| 54151HACS | Computer Forensic & Intrusion Analyst I | Shall have educational or professional experience in incident detection and response and/or cyber intelligence analysis, the candidates shall support Red Team efforts conducting covert focused target penetration testing of US Government installations through focused threat-based methodologies as a simulated adversary to expose and exploit vulnerabilities to improve the Cyber Readiness of infrastructure, Services, and Agencies.  
  a) Provides knowledge in computer and network forensics.  
  b) Conducts vulnerability assessments/penetration tests of information systems. | Bachelors + | 0+ |
| 54151HACS | Computer Forensic & Intrusion Analyst II | Shall have three (3) years of experience in incident detection and response and/or cyber intelligence analysis, the candidates shall support Red Team efforts conducting covert focused target penetration testing of US Government installations through focused threat-based methodologies as a simulated adversary to expose and exploit vulnerabilities to improve the Cyber Readiness of infrastructure, Services, and Agencies.  
  a) Provides knowledge in computer and network forensics.  
  b) Conducts vulnerability assessments/penetration tests of information systems. | Bachelors + | 3+ |
## XOR Security Labor Categories Descriptions

<table>
<thead>
<tr>
<th>SIN</th>
<th>SERVICE PROPOSED (e.g. Job Title/Task)</th>
<th>Description</th>
<th>MINIMUM EDUCATION/CERTIFICATION LEVEL</th>
<th>MINIMUM YEARS OF EXPERIENCE</th>
</tr>
</thead>
</table>
| 54151HACS| Computer Forensic & Intrusion Analyst III                                                                | Shall have seven (7) years of experience in incident detection and response and/or cyber intelligence analysis, the candidates shall support Red Team efforts conducting covert focused target penetration testing of US Government installations through focused threat-based methodologies as a simulated adversary to expose and exploit vulnerabilities to improve the Cyber Readiness of infrastructure, Services, and Agencies.  
  a) Provides knowledge in computer and network forensics  
  b) Conducts vulnerability assessments/penetration tests of information systems.  
  c) Develops, researches and maintains proficiency in tools, techniques, countermeasures, and trend in computer and network vulnerabilities, data hiding, and encryption.  
  d) Identifies, deters, monitors, and investigates computer and network intrusions.  
  e) Provides computer forensic support to high technology investigations in the form of evidence seizure, computer forensic analysis, and data recovery.  
  f) Shall be familiar with: development of attack vectors, system and infrastructure reconnaissance, collection of open-source intelligence, enumeration, and footprinting of target networks and services, and develop exploit payloads and system backdoors. | Bachelors +                                           | 7+                                         |
| 54151HACS| Computer Forensic & Intrusion Analyst IV                                                                | Shall have ten (10) years experience in incident detection and response and/or cyber intelligence analysis, the candidates shall support Red Team efforts conducting covert focused target penetration testing of US Government installations through focused threat-based methodologies as a simulated adversary to expose and exploit vulnerabilities to improve the Cyber Readiness of infrastructure, Services, and Agencies.  
  a) Provides knowledge in computer and network forensics  
  b) Conducts vulnerability assessments/penetration tests of information systems.  
  c) Develops, researches and maintains proficiency in tools, techniques, countermeasures, and trend in computer and network vulnerabilities, data hiding, and encryption.  
  d) Identifies, deters, monitors, and investigates computer and network intrusions.  
  e) Provides computer forensic support to high technology investigations in the form of evidence seizure, computer forensic analysis, and data recovery. | Bachelors +                                           | 10+                                        |
### XOR Security Labor Categories Descriptions

<table>
<thead>
<tr>
<th>SIN</th>
<th>SERVICE PROPOSED (e.g. Job Title/Task)</th>
<th>Description</th>
<th>MINIMUM EDUCATION/CERTIFICATION LEVEL</th>
<th>MINIMUM YEARS OF EXPERIENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>f) Shall be familiar with: development of attack vectors, system and infrastructure reconnaissance, collection of open-source intelligence, enumeration, and footprinting of target networks and services, and develop exploit payloads and system backdoors. g) Candidates shall provide support to the government customer in Red Team penetration testing using tools and techniques to conduct Cyber vulnerability and penetration testing of exercise and test events. h) Candidates shall participate in event planning stages to develop Cyber assessment plans and conduct no-notice penetration tests against network infrastructure and applications.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Data Scientist I</td>
<td>Shall have experience in data engineering, statistics, machine learning, and predictive modeling in support of the development of applications and analytical workflows supporting data analysis, threat modeling, targeting, entity resolution, and big data analytics. (a) Degree in a quantitative field (e.g., Computer Science, Economics, Engineering, Mathematics, Finance, Statistics, or Operations Research). (b) Experience building descriptive, predictive, and prescriptive models with data.</td>
<td>Bachelors +</td>
<td>0+</td>
</tr>
<tr>
<td>54151S</td>
<td>Data Scientist II</td>
<td>Shall have three (3) years experience in data engineering, statistics, machine learning, and predictive modeling in support of the development of applications and analytical workflows supporting data analysis, threat modeling, targeting, entity resolution, and big data analytics. a) Degree in a quantitative field (e.g., Computer Science, Economics, Engineering, Mathematics, Finance, Statistics, or Operations Research). b) At least 3 years experience building descriptive, predictive, and prescriptive models with data. c) Expertise with languages and frameworks such as Spark, Scala, Java, R, Python, and SQL. d) Experience working in a Linux computing environment. e) Experience applying data mining and machine learning techniques in a professional context.</td>
<td>Bachelors +</td>
<td>3+</td>
</tr>
<tr>
<td>54151S</td>
<td>Data Scientist III</td>
<td>Shall have seven (7) years experience in data engineering, statistics, machine learning, and predictive modeling in support of the development of applications and analytical workflows supporting data analysis, threat modeling, targeting, entity resolution, and big data analytics. a) Degree in a quantitative field (e.g., Computer Science, Economics, Engineering, Mathematics, Finance, Statistics, or Operations Research). b) At least 7 years experience building descriptive, predictive, and prescriptive models with data.</td>
<td>Bachelors +</td>
<td>7+</td>
</tr>
</tbody>
</table>
## XOR Security Labor Categories Descriptions

<table>
<thead>
<tr>
<th>SIN</th>
<th>SERVICE PROPOSED (e.g. Job Title/Task)</th>
<th>Description</th>
<th>MINIMUM EDUCATION/CERTIFICATION LEVEL</th>
<th>MINIMUM YEARS OF EXPERIENCE</th>
</tr>
</thead>
</table>
| 54151S   | Data Scientist IV                     | Shall have ten (10) years experience in data engineering, statistics, machine learning, and predictive modeling in support of the development of applications and analytical workflows supporting data analysis, threat modeling, targeting, entity resolution, and big data analytics.  

  a) Degree in a quantitative field (e.g., Computer Science, Economics, Engineering, Mathematics, Finance, Statistics, or Operations Research).
  b) At least 10 years experience building descriptive, predictive, and prescriptive models with data.
  c) Expertise with languages and frameworks such as Spark, Scala, Java, R, Python, and SQL.
  d) Experience working in a Linux computing environment.
  e) Experience applying data mining and machine learning techniques in a professional context.
  f) Strong familiarity with data preparation, processing, classification, and prediction.
  g) Knowledge of data mining and machine learning algorithms, theories, principals and practices.

Desired Skills:
  a) Familiarity with the Apache Hadoop ecosystem.
  b) Familiarity with cloud computing technologies.
  c) Experience working in the big data community and using data to inform business intelligence.
  d) Experience with version control platforms (git, svn, etc.)
  e) Experience with Continuous Integration and Continuous Delivery. | Masters + | 10+ |
| 54151S   | Dev/Ops Engineer I                    | Shall have experience in the design, development, enhancement, and implementation of Continuous Integration Continuous Delivery ecosystems within a Cloud Service Provider ecosystem or onsite cloud infrastructure. Troubleshoots production problems related to software applications.

  a) Researches, tests, builds, and coordinates the conversion and/or continuous integration pipelines and toolchains based on client requirements. | Bachelors + | 0+ |
## XOR Security Labor Categories Descriptions

<table>
<thead>
<tr>
<th>SIN</th>
<th>SERVICE PROPOSED (e.g. Job Title/Task)</th>
<th>Description</th>
<th>MINIMUM EDUCATION/CERTIFICATION LEVEL</th>
<th>MINIMUM YEARS OF EXPERIENCE</th>
</tr>
</thead>
</table>
| 54151S | Dev/Ops Engineer II | Shall have three (3) experience in the design, development, enhancement, and implementation of Continuous Integration Continuous Delivery ecosystems within a Cloud Service Provider ecosystem or onsite cloud infrastructure. Troubleshoots production problems related to software applications.  
  a) Researches, tests, builds, and coordinates the conversion and/or continuous integration pipelines and toolchains based on client requirements.  
  b) Designs and develops new software products or major enhancements to existing software.  
  c) Addresses problems of systems integration, compatibility, and multiple platforms.  
  d) Assesses cloud security architectures and provides recommendations to improve overall infrastructure security and methods to automate security testing of applications moving through the CI/CD pipeline.  
  e) Consults with project teams and end users to identify application requirements.  
  f) Performs feasibility analysis on potential future projects to management. | Bachelors + | 3+ |
| 54151S | Dev/Ops Engineer III | Shall have seven (7) years experience in the design, development, enhancement, and implementation of Continuous Integration Continuous Delivery ecosystems within a Cloud Service Provider ecosystem or onsite cloud infrastructure. Troubleshoots production problems related to software applications.  
  a) Researches, tests, builds, and coordinates the conversion and/or continuous integration pipelines and toolchains based on client requirements.  
  b) Designs and develops new software products or major enhancements to existing software.  
  c) Addresses problems of systems integration, compatibility, and multiple platforms.  
  d) Assesses cloud security architectures and provides recommendations to improve overall infrastructure security and methods to automate security testing of applications moving through the CI/CD pipeline.  
  e) Consults with project teams and end users to identify application requirements.  
  f) Performs feasibility analysis on potential future projects to management. | Bachelors + | 7+ |
## XOR Security Labor Categories Descriptions

<table>
<thead>
<tr>
<th>SIN</th>
<th>SERVICE PROPOSED (e.g. Job Title/Task)</th>
<th>Description</th>
<th>MINIMUM EDUCATION/CERTIFICATION LEVEL</th>
<th>MINIMUM YEARS OF EXPERIENCE</th>
</tr>
</thead>
</table>
| 54151S | Dev/Ops Engineer IV                   | Shall have ten (10) years experience in the design, development, enhancement, and implementation of Continuous Integration Continuous Delivery ecosystems within a Cloud Service Provider ecosystem or onsite cloud infrastructure. Troubleshoots production problems related to software applications.  
   a) Researches, tests, builds, and coordinates the conversion and/or continuous integration pipelines and toolchains based on client requirements.  
   b) Designs and develops new software products or major enhancements to existing software.  
   c) Addresses problems of systems integration, compatibility, and multiple platforms.  
   d) Assesses cloud security architectures and provides recommendations to improve overall infrastructure security and methods to automate security testing of applications moving through the CI/CD pipeline.  
   e) Consults with project teams and end users to identify application requirements.  
   f) Performs feasibility analysis on potential future projects to management.  
   g) Assists in the evaluation and recommendation of application software packages, application integration and testing tools.  
   h) Resolves problems with software and responds to suggestions for improvements and enhancements.  
   i) Acts as team leader on projects.  
   j) Instructs, assigns, directs, and checks the work of other software developers on development team.  
   k) Participates in development of software user manuals.  
   l) Experienced in common programming and scripting languages such as Java, Perl, Ruby and Python. | Masters +                             | 10+                                        |
| 54151S | Software Engineer I                   | Shall have experience in designing, developing and integrating software in support the efforts of cyber threat analysts and computer forensic intrusion analyst in the protection of information systems, ongoing computer network defense operations, and information security projects.  
   a) Applies industry leading methods in the development of new software and applications  
   b) Determines and identifies high level functional and technical requirements based on interactions with the user community and knowledge of the enterprise architecture  
   c) Identifies, assesses, and develops applications to meet functional and technical requirements including services, | Bachelors +                            | 0+                                         |
## XOR Security Labor Categories Descriptions

<table>
<thead>
<tr>
<th>SIN</th>
<th>SERVICE PROPOSED (e.g. Job Title/Task)</th>
<th>Description</th>
<th>MINIMUM EDUCATION/ CERTIFICATION LEVEL</th>
<th>MINIMUM YEARS OF EXPERIENCE</th>
</tr>
</thead>
</table>
| 54151S  | Software Engineer II                   | Shall have three (3) years experience in designing, developing and integrating software in support the efforts of cyber threat analysts and computer forensic intrusion analyst in the protection of information systems, ongoing computer network defense operations, and information security projects.  
  a) Applies industry leading methods in the development of new software and applications  
  b) Determines and identifies high level functional and technical requirements based on interactions with the user community and knowledge of the enterprise architecture  
  c) Identifies, assesses, and develops applications to meet functional and technical requirements including services, software, and security  
  d) Formulates and defines specifications for operating system applications or modifies and maintains existing applications using engineering releases and utilities from the manufacturer  
  e) Creates detailed design specifications for use by software development staff members  
  f) Interacts with project management, information assurance staff and security subject matter experts to plan project schedules and technical direction  
  g) Develops software design documents and technology white papers  
  h) Provides recommendations during the selection of development tools  
  i) Ensures systems are compatible and compliant with the standards for development of secure systems  
  j) Uses the most relevant software engineering paradigms to develop and integrate software and applications to meet stakeholder needs | Bachelors +                                | 3+                                          |
| 54151S  | Software Engineer III                  | Shall have seven (7) years experience in designing, developing and integrating software in support the efforts of cyber threat analysts and computer forensic intrusion analyst in the protection of information systems, ongoing computer network defense operations, and information security projects.  
  a) Applies industry leading methods in the development of new software and applications  
  b) Determines and identifies high level functional and technical requirements based on interactions with the user community and knowledge of the enterprise architecture  
  c) Identifies, assesses, and develops applications to meet functional and technical requirements including services, software, and security  
  d) Formulates and defines specifications for operating system applications or modifies and maintains existing applications using engineering releases and utilities from the manufacturer  
  e) Creates detailed design specifications for use by software development staff members  
  f) Interacts with project management, information assurance staff and security subject matter experts to plan project schedules and technical direction  | Bachelors +                                | 7+                                          |
## XOR Security Labor Categories Descriptions

<table>
<thead>
<tr>
<th>SIN</th>
<th>SERVICE PROPOSED (e.g. Job Title/Task)</th>
<th>Description</th>
<th>MINIMUM EDUCATION/CERTIFICATION LEVEL</th>
<th>MINIMUM YEARS OF EXPERIENCE</th>
</tr>
</thead>
</table>
| 54151S | Software Engineer IV                   | Shall have ten (10) years experience in designing, developing and integrating software in support the efforts of cyber threat analysts and computer forensic intrusion analyst in the protection of information systems, ongoing computer network defense operations, and information security projects.  
  a) Applies industry leading methods in the development of new software and applications  
  b) Determines and identifies high level functional and technical requirements based on interactions with the user community and knowledge of the enterprise architecture  
  c) Identifies, assesses, and develops applications to meet functional and technical requirements including services, software, and security  
  d) Formulates and defines specifications for operating system applications or modifies and maintains existing applications using engineering releases and utilities from the manufacturer  
  e) Creates detailed design specifications for use by software development staff members  
  f) Interacts with project management, information assurance staff and security subject matter experts to plan project schedules and technical direction  
  g) Develops software design documents and technology white papers  
  h) Provides recommendations during the selection of development tools  
  i) Ensures systems are compatible and compliant with the standards for development of secure systems  
  j) Uses the most relevant software engineering paradigms to develop and integrate software and applications to meet stakeholder needs  
  k) Provides top-level technical expertise, including performing in-depth and complex software systems using secure programming and analysis techniques  
  l) Conducts source code static analysis to minimize the delivery of insecure code | Masters + | 10+ |
<table>
<thead>
<tr>
<th>SIN</th>
<th>SERVICE PROPOSED (e.g. Job Title/Task)</th>
<th>Description</th>
<th>MINIMUM EDUCATION/CERTIFICATION LEVEL</th>
<th>MINIMUM YEARS OF EXPERIENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>project schedules and technical direction</td>
<td>Bachelors + 0+</td>
<td>0+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>g) Develops software design documents and technology white papers</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>h) Provides recommendations during the selection of development tools</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>i) Ensures systems are compatible and compliant with the standards for development of secure systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>j) Uses the most relevant software engineering paradigms to develop and integrate software and applications to meet stakeholder needs</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>k) Provides top-level technical expertise, including performing in-depth and complex software systems using secure programming and analysis techniques</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>l) Conducts source code static analysis to minimize the delivery of insecure code</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>m) Manages the technical direction of software engineering efforts as well as the daily interaction of software engineers</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>n) Manages the agile lifecycle of the project</td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Subject Matter Expert I</td>
<td>Shall have direct experience and expertise in a specific domain area.</td>
<td>Bachelors +</td>
<td>3+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a) Serves as subject matter expert, possessing in-depth knowledge of a particular area, such as information security, cloud security, systems engineering, big data, or the various sciences related to enterprise technology.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>b) Provides technical knowledge and analysis of highly specialized applications and operational environments, high-level functional systems analysis, design, integration, security, implementation advice on exceptionally complex problems that need extensive knowledge of the subject matter for effective implementation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>c) Participates as needed in all phases of system and software development with emphasis on the planning, analysis, security, testing, integration, documentation, and presentation phases.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>d) Applies principles, methods and knowledge of the functional area of capability to specific task order requirements, advanced software, systems and security principles and methods to exceptionally difficult and narrowly defined technical problems in engineering and other scientific applications to arrive at automated solutions.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Subject Matter Expert II</td>
<td>Shall have three (3) years direct experience and expertise in a specific domain area.</td>
<td>Bachelors +</td>
<td>3+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a) Serves as subject matter expert, possessing in-depth knowledge of a particular area, such as information security, cloud security, systems engineering, big data, or the various sciences related to enterprise technology.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>b) Provides technical knowledge and analysis of highly specialized applications and operational environments,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIN</td>
<td>SERVICE PROPOSED (e.g. Job Title/Task)</td>
<td>Description</td>
<td>MINIMUM EDUCATION/CERTIFICATION LEVEL</td>
<td>MINIMUM YEARS OF EXPERIENCE</td>
</tr>
<tr>
<td>-------</td>
<td>---------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------</td>
<td>-----------------------------</td>
</tr>
</tbody>
</table>
| 54151S | Subject Matter Expert III             | Shall have seven (7) years direct experience and expertise in a specific domain area.  
  a) Serves as subject matter expert, possessing in-depth knowledge of a particular area, such as information security, cloud security, systems engineering, big data, or the various sciences related to enterprise technology.  
  b) Provides technical knowledge and analysis of highly specialized applications and operational environments, high-level functional systems analysis, design, integration, security, implementation advice on exceptionally complex problems that need extensive knowledge of the subject matter for effective implementation.  
  c) Participates as needed in all phases of system and software development with emphasis on the planning, analysis, security, testing, integration, documentation, and presentation phases.  
  d) Applies principles, methods and knowledge of the functional area of capability to specific task order requirements, advanced software, systems and security principles and methods to exceptionally difficult and narrowly defined technical problems in engineering and other scientific applications to arrive at automated solutions. | Bachelors +                                | 7+                                         |
| 54151S | Subject Matter Expert IV              | Shall have ten (10) years direct experience and expertise in a specific domain area.  
  a) Serves as subject matter expert, possessing in-depth knowledge of a particular area, such as information security, cloud security, systems engineering, big data, or the various sciences related to enterprise technology.  
  b) Provides technical knowledge and analysis of highly specialized applications and operational environments, high-level functional systems analysis, design, integration, security, implementation advice on exceptionally complex problems that need extensive knowledge of the subject matter for effective implementation.  
  c) Participates as needed in all phases of system and software development with emphasis on the planning, analysis, security, testing, integration, documentation, and presentation phases.  
  d) Applies principles, methods and knowledge of the functional area of capability to specific task order requirements, advanced software, systems and security principles and methods to exceptionally difficult and narrowly defined technical problems in engineering and other scientific applications to arrive at automated solutions. | Masters +                                | 10+                                        |
<table>
<thead>
<tr>
<th>SIN</th>
<th>SERVICE PROPOSED (e.g. Job Title/Task)</th>
<th>Description</th>
<th>MINIMUM EDUCATION/CERTIFICATION LEVEL</th>
<th>MINIMUM YEARS OF EXPERIENCE</th>
</tr>
</thead>
</table>
| 54151S | System / Network Administrator I     | Shall responds to and diagnoses problems through discussion with system engineers, tests and security staff.  
(a) Supervises operation of IT and Cloud ecosystems and serves as focal point for system, software and security issues.  
(b) Provides support to system owners on a variety of issues to include cyber security compliance, outages and escalation of user reported events to security operations staff.  
(c) Identifies, researches, and resolves technical and potential security problems.  
(d) Applies principles, methods and knowledge of the functional area of capability to specific task order requirements, advanced software, systems and security principles and methods to exceptionally difficult and narrowly defined technical problems in engineering and other scientific applications to arrive at automated solutions. | bachelors                           | 0+                          |
| 54151S | System / Network Administrator II    | Shall respond to and diagnoses problems through discussion with system engineers, tests and security staff.  
(a) Supervises operation of IT and Cloud ecosystems and serves as focal point for system, software and security issues.  
(b) Provides support to system owners on a variety of issues to include cyber security compliance, outages and escalation of user reported events to security operations staff.  
(c) Identifies, researches, and resolves technical and potential security problems.  
(d) Responds to telephone calls, email and personnel requests for technical support.  
(e) Documents, tracks, and monitors the problem to ensure a timely resolution. | bachelors                           | 3+                          |
| 54151S | System / Network Administrator III   | Shall have seven (7) years experience in responding to, and diagnosing problems through discussion with system engineers, tests and security staff.  
(a) Supervises operation of IT and Cloud ecosystems and serves as focal point for system, software and security issues.  
(b) Provides support to system owners on a variety of issues to include cyber security compliance, outages and escalation of user reported events to security operations staff.  
(c) Identifies, researches, and resolves technical and potential security problems.  
(d) Responds to telephone calls, email and personnel requests for technical support.  
(e) Documents, tracks, and monitors the problem to ensure a timely resolution.  
(f) Interact with network services, software systems | bachelors                           | 7+                          |
<table>
<thead>
<tr>
<th>SIN</th>
<th>SERVICE PROPOSED (e.g. Job Title/Task)</th>
<th>Description</th>
<th>MINIMUM EDUCATION/ CERTIFICATION LEVEL</th>
<th>MINIMUM YEARS OF EXPERIENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S</td>
<td>System / Network Administrator IV</td>
<td>Shall have ten (10) years experience in responding to, and diagnosing problems through discussion with system engineers, testers and security staff. (a) Supervises operation of IT and Cloud ecosystems and serves as focal point for system, software and security issues. (b) Provides support to system owners on a variety of issues to include cyber security compliance, outages and escalation of user reported events to security operations staff. (c) Identifies, researches, and resolves technical and potential security problems. (d) Responds to telephone calls, email and personnel requests for technical support. (e) Documents, tracks, and monitors the problem to ensure a timely resolution. (f) Interact with network services, software systems engineering, and/or applications development to restore service and/or identify and correct core problem. (g) Simulates or recreates user problems to resolve operating difficulties. (h) Recommends systems modifications to reduce user problems and security defects.</td>
<td>bachelors</td>
<td>10+</td>
</tr>
</tbody>
</table>
| 54151S  | Systems Engineer I                    | Shall have experience in designing, developing and integrating systems and software in support the efforts of stakeholders.  
(a) Provides analysis related to the design, development, security and integration of hardware, software, man-machine interfaces and all system level requirements to provide an integrated IT solution.  
(b) Develops integrated system test requirement, strategies, devices and systems.  
(c) Directs overall system level testing and security testing  
(d) Designs and Integrates information security suites, tools, capabilities into delivered solutions to ensure federal and commercial security best practices. | bachelors                             | 0+                           |
| 54151S  | Systems Engineer II                   | Shall have three (3) years experience in designing, developing and integrating systems and software in support the efforts of stakeholders.  
(a) Provides analysis related to the design, development, security and integration of hardware, software, man-machine interfaces and all system level requirements to provide an integrated IT solution.  
(b) Develops integrated system test requirement, | bachelors                             | 3+                           |
<table>
<thead>
<tr>
<th>SIN</th>
<th>SERVICE PROPOSED (e.g. Job Title/Task)</th>
<th>Description</th>
<th>MINIMUM EDUCATION/CERTIFICATION LEVEL</th>
<th>MINIMUM YEARS OF EXPERIENCE</th>
</tr>
</thead>
</table>
| 54151S | Systems Engineer III | Shall have seven (7) years experience in designing, developing and integrating systems and software in support the efforts of stakeholders.  
   a) Provides analysis related to the design, development, security and integration of hardware, software, man-machine interfaces and all system level requirements to provide an integrated IT solution.  
   b) Develops integrated system test requirement, strategies, devices and systems.  
   c) Directs overall system level testing and security testing  
   d) Designs and Integrates information security suites, tools, capabilities into delivered solutions to ensure federal and commercial security best practices.  
   e) Manages software and security engineers in the delivery of new solutions to meet client needs  
   f) Manages risk and opportunity as well as project schedule  
   g) Informs and leads integrated product teams | Bachelors + | 7+ |
| 54151S | Systems Engineer IV | Shall have ten (10) years experience in designing, developing and integrating systems and software in support the efforts of stakeholders.  
   a) Provides analysis related to the design, development, security and integration of hardware, software, man-machine interfaces and all system level requirements to provide an integrated IT solution.  
   b) Develops integrated system test requirement, strategies, devices and systems.  
   c) Directs overall system level testing and security testing  
   d) Designs and Integrates information security suites, tools, capabilities into delivered solutions to ensure federal and commercial security best practices.  
   e) Manages software and security engineers in the delivery of new solutions to meet client needs  
   f) Manages risk and opportunity as well as project schedule  
   g) Informs and leads integrated product teams  
   h) Leads the coordination of development, testing, IA testing and deployment of new and enhanced technologies | Bachelors + | 10+ |
| 54151S | Systems Engineer V | Shall have ten (10) year’s experience in designing, developing and integrating systems and software in support the efforts of stakeholders and three (3) years of experience in specialized technologies with demonstrated proficiency in its design, integration, development, and operations. | Bachelors + | 10+ |
XOR Security Labor Categories Descriptions

<table>
<thead>
<tr>
<th>SIN</th>
<th>SERVICE PROPOSED (e.g. Job Title/Task)</th>
<th>Description</th>
<th>MINIMUM EDUCATION/CERTIFICATION LEVEL</th>
<th>MINIMUM YEARS OF EXPERIENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>a. Provides analysis related to the design, development, security and integration of hardware, software, man-machine interfaces and all system level requirements to provide an integrated IT solution.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. May apply direct and relevant knowledge of specialized systems, technologies, software/applications to support client requirements.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. Develops integrated system test requirement, strategies, devices and systems.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. Directs overall system level testing and security testing.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>e. Designs and Integrates information security suites, tools, capabilities into delivered solutions to ensure federal and commercial security best practices.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>f. Manages software and security engineers in the delivery of new solutions to meet client needs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>g. Manages risk and opportunity as well as project schedule</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>h. Informs and leads integrated product teams</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Leads the coordination of development, testing, IA testing and deployment of new and enhanced technologies</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIN</td>
<td>SERVICE</td>
<td>UNIT OF ISSUE</td>
<td>GSA NET</td>
<td>QUANTITY/VOLUME DISCOUNT</td>
</tr>
<tr>
<td>-------</td>
<td>----------------------------------------</td>
<td>---------------</td>
<td>---------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>54151S</td>
<td>Business Systems / Process Analyst I</td>
<td>Hour</td>
<td>$86.49</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>54151S</td>
<td>Business Systems / Process Analyst II</td>
<td>Hour</td>
<td>$105.11</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>54151S</td>
<td>Business Systems / Process Analyst III</td>
<td>Hour</td>
<td>$124.41</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>54151S</td>
<td>Business Systems / Process Analyst IV</td>
<td>Hour</td>
<td>$136.19</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Computer Forensic &amp; Intrusion Analyst</td>
<td>Hour</td>
<td>$114.39</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Analyst I</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Analyst II</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Analyst III</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Analyst IV</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Data Scientist I</td>
<td>Hour</td>
<td>$96.61</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>54151S</td>
<td>Data Scientist II</td>
<td>Hour</td>
<td>$124.41</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>54151S</td>
<td>Data Scientist III</td>
<td>Hour</td>
<td>$138.46</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>54151S</td>
<td>Data Scientist IV</td>
<td>Hour</td>
<td>$169.04</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>54151S</td>
<td>Dev/Ops Engineer I</td>
<td>Hour</td>
<td>$109.07</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>54151S</td>
<td>Dev/Ops Engineer II</td>
<td>Hour</td>
<td>$124.41</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>54151S</td>
<td>Dev/Ops Engineer III</td>
<td>Hour</td>
<td>$146.83</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>54151S</td>
<td>Dev/Ops Engineer IV</td>
<td>Hour</td>
<td>$163.79</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>54151S</td>
<td>Software Engineer I</td>
<td>Hour</td>
<td>$113.33</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>SIN</td>
<td>SERVICE</td>
<td>UNIT OF ISSUE</td>
<td>GSA NET</td>
<td>QUANTITY/VOLUME DISCOUNT</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------</td>
<td>---------------</td>
<td>----------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>54151S</td>
<td>Software Engineer II</td>
<td>Hour</td>
<td>$133.01</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>54151S</td>
<td>Software Engineer III</td>
<td>Hour</td>
<td>$138.46</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>54151S</td>
<td>Software Engineer IV</td>
<td>Hour</td>
<td>$172.36</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>54151S</td>
<td>Subject Matter Expert I</td>
<td>Hour</td>
<td>$121.88</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>54151S</td>
<td>Subject Matter Expert II</td>
<td>Hour</td>
<td>$133.62</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>54151S</td>
<td>Subject Matter Expert III</td>
<td>Hour</td>
<td>$149.38</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>54151S</td>
<td>Subject Matter Expert IV</td>
<td>Hour</td>
<td>$172.36</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>54151S</td>
<td>System / Network Administrator I</td>
<td>Hour</td>
<td>$88.67</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>54151S</td>
<td>System / Network Administrator II</td>
<td>Hour</td>
<td>$94.59</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>54151S</td>
<td>System / Network Administrator III</td>
<td>Hour</td>
<td>$108.91</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>54151S</td>
<td>System / Network Administrator IV</td>
<td>Hour</td>
<td>$146.47</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>54151S</td>
<td>Systems Engineer I</td>
<td>Hour</td>
<td>$88.67</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>54151S</td>
<td>Systems Engineer II</td>
<td>Hour</td>
<td>$106.57</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>54151S</td>
<td>Systems Engineer III</td>
<td>Hour</td>
<td>$138.46</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>54151S</td>
<td>Systems Engineer IV</td>
<td>Hour</td>
<td>$156.32</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>54151S</td>
<td>Systems Engineer V</td>
<td>Hour</td>
<td>$201.79</td>
<td>1/2% orders over $300,000</td>
</tr>
<tr>
<td>-------</td>
<td>--------------------------------------------</td>
<td>-------------------------------------</td>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>54151S</td>
<td>Business Systems/Process Analyst I</td>
<td>$83.14</td>
<td>$84.80</td>
<td>$86.49</td>
</tr>
<tr>
<td>54151S</td>
<td>Business Systems / Process Analyst II</td>
<td>$101.05</td>
<td>$103.06</td>
<td>$105.12</td>
</tr>
<tr>
<td>54151S</td>
<td>Business Systems / Process Analyst III</td>
<td>$119.59</td>
<td>$121.96</td>
<td>$124.40</td>
</tr>
<tr>
<td>54151S</td>
<td>Business Systems / Process Analyst IV</td>
<td>$130.92</td>
<td>$133.51</td>
<td>$136.18</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Computer Forensic &amp; Intrusion Analyst I</td>
<td>$109.94</td>
<td>$112.15</td>
<td>$114.39</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Computer Forensic &amp; Intrusion Analyst II</td>
<td>$137.69</td>
<td>$140.43</td>
<td>$143.25</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Computer Forensic &amp; Intrusion Analyst III</td>
<td>$158.89</td>
<td>$162.08</td>
<td>$165.31</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Computer Forensic &amp; Intrusion Analyst IV</td>
<td>$161.30</td>
<td>$164.51</td>
<td>$167.82</td>
</tr>
<tr>
<td>54151S</td>
<td>Data Scientist I</td>
<td>$92.89</td>
<td>$94.72</td>
<td>$96.60</td>
</tr>
<tr>
<td>54151S</td>
<td>Data Scientist II</td>
<td>$119.59</td>
<td>$121.96</td>
<td>$124.40</td>
</tr>
<tr>
<td>54151S</td>
<td>Data Scientist III</td>
<td>$133.07</td>
<td>$135.75</td>
<td>$138.46</td>
</tr>
<tr>
<td>54151S</td>
<td>Data Scientist IV</td>
<td>$162.49</td>
<td>$165.73</td>
<td>$169.05</td>
</tr>
<tr>
<td>54151S</td>
<td>Dev/Ops Engineer I</td>
<td>$104.83</td>
<td>$106.92</td>
<td>$109.08</td>
</tr>
<tr>
<td>54151S</td>
<td>Dev/Ops Engineer II</td>
<td>$119.59</td>
<td>$121.96</td>
<td>$124.40</td>
</tr>
<tr>
<td>54151S</td>
<td>Dev/Ops Engineer III</td>
<td>$141.14</td>
<td>$143.94</td>
<td>$146.83</td>
</tr>
<tr>
<td>54151S</td>
<td>Dev/Ops Engineer IV</td>
<td>$157.44</td>
<td>$160.58</td>
<td>$163.79</td>
</tr>
<tr>
<td>54151S</td>
<td>Software Engineer I</td>
<td>$108.94</td>
<td>$111.13</td>
<td>$113.33</td>
</tr>
<tr>
<td>54151S</td>
<td>Software Engineer II</td>
<td>$127.85</td>
<td>$130.40</td>
<td>$133.02</td>
</tr>
<tr>
<td>54151S</td>
<td>Software Engineer III</td>
<td>$133.07</td>
<td>$135.75</td>
<td>$138.46</td>
</tr>
<tr>
<td>54151S</td>
<td>Software Engineer IV</td>
<td>$165.66</td>
<td>$168.99</td>
<td>$172.36</td>
</tr>
<tr>
<td>54151S</td>
<td>Subject Matter Expert I</td>
<td>$117.15</td>
<td>$119.51</td>
<td>$121.88</td>
</tr>
<tr>
<td>54151S</td>
<td>Subject Matter Expert II</td>
<td>$128.43</td>
<td>$131.03</td>
<td>$133.62</td>
</tr>
<tr>
<td>54151S</td>
<td>Subject Matter Expert III</td>
<td>$143.61</td>
<td>$146.46</td>
<td>$149.38</td>
</tr>
<tr>
<td>54151S</td>
<td>Subject Matter Expert IV</td>
<td>$165.66</td>
<td>$168.99</td>
<td>$172.36</td>
</tr>
<tr>
<td>54151S</td>
<td>System / Network Administrator I</td>
<td>$85.23</td>
<td>$86.93</td>
<td>$88.66</td>
</tr>
</tbody>
</table>
## XOR Security Price with 2% escalation - 5 year pricing

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S</td>
<td>System / Network Administrator II</td>
<td>$90.91</td>
<td>$92.73</td>
<td>$94.59</td>
<td>$96.47</td>
<td>$98.40</td>
</tr>
<tr>
<td>54151S</td>
<td>System / Network Administrator III</td>
<td>$104.72</td>
<td>$106.80</td>
<td>$108.92</td>
<td>$111.10</td>
<td>$113.32</td>
</tr>
<tr>
<td>54151S</td>
<td>System / Network Administrator IV</td>
<td>$140.80</td>
<td>$143.62</td>
<td>$146.47</td>
<td>$149.40</td>
<td>$152.39</td>
</tr>
<tr>
<td>54151S</td>
<td>Systems Engineer I</td>
<td>$85.23</td>
<td>$86.93</td>
<td>$88.66</td>
<td>$90.45</td>
<td>$92.25</td>
</tr>
<tr>
<td>54151S</td>
<td>Systems Engineer II</td>
<td>$102.45</td>
<td>$104.49</td>
<td>$106.57</td>
<td>$108.72</td>
<td>$110.88</td>
</tr>
<tr>
<td>54151S</td>
<td>Systems Engineer III</td>
<td>$133.07</td>
<td>$135.75</td>
<td>$138.46</td>
<td>$141.22</td>
<td>$144.07</td>
</tr>
<tr>
<td>54151S</td>
<td>Systems Engineer IV</td>
<td>$150.24</td>
<td>$153.25</td>
<td>$156.31</td>
<td>$159.44</td>
<td>$162.63</td>
</tr>
<tr>
<td>54151S</td>
<td>Systems Engineer V</td>
<td>$201.79</td>
<td>$205.83</td>
<td>$209.94</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>