TWM Associates, Inc. (TWM) is providing the technical solutions for your Information Technology needs. TWM has a history of providing high quality cyber security engineering, system engineering, system analysis, system design, network support, process improvement, integration support, FISMA support, IT Audit support, and other specially requested services.

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 for GSA Advantage is http://www.gsaadvantage.gov

SCHEDULE TITLE: Federal Supply Catalog (FSC) Group Information Technology Category F, Subcategory F03-IT Services, Special Item Numbers (SINs) 54151S and 54151HACS Information Technology Professional Services and Highly Adaptive Cybersecurity Services (HACS). Standard Industry Group Multiple Award Schedule (MAS)

Contract Number: GS-35F-315CA

Contract Period: 05/05/2015 through 5/4/2025

For more information on ordering from Federal Supply Schedules go to the GSA Schedules page at GSA.gov.

CONTRACTOR: TWM Associates, Inc.
13408 Black Walnut Lane
Spotsylvania, VA 22551
Phone Number: (703) 280-3102
Email: lisa.johnson@twmInc.com
www.twmInc.com
CAGE Code: 0R3A0

CONTRACTOR’S ADMINISTRATION SOURCE:

Lisa A. Johnson
TWM Associates, Inc.
13408 Black Walnut Lane
Spotsylvania, VA 22551
Phone Number: (703) 280-3102
Email: lisa.johnson@twmInc.com

BUSINESS SIZE: Small Woman Owned.

CUSTOMER INFORMATION:

1a. TABLE OF AWARDED SPECIAL ITEM NUMBERS (SINs)

SIN 54151S - Information Technology (IT) Professional Services

July 13, 2022
SIN 54151HACS – Highly Adaptive Cybersecurity Services (Penetration Testing, Incident Response, and Risk Vulnerability Assessment)

1b. **LOWEST PRICED LABOR CATEGORY AND PRICE FOR EACH SIN:** Administration Support $45.68.

1c. **HOURLY RATES:**

<table>
<thead>
<tr>
<th>Information Technology Professional Services</th>
<th>GSA Net Rates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Manager 54151S</td>
<td>$ 205.58</td>
</tr>
<tr>
<td>SME IV 54151S</td>
<td>$ 205.58</td>
</tr>
<tr>
<td>SME IIII 54151S</td>
<td>$ 182.73</td>
</tr>
<tr>
<td>SME II 54151S</td>
<td>$ 159.90</td>
</tr>
<tr>
<td>SME I 54151S</td>
<td>$ 137.05</td>
</tr>
<tr>
<td>Task Manager 54151S</td>
<td>$ 137.05</td>
</tr>
<tr>
<td>Principal 54151S</td>
<td>$ 125.62</td>
</tr>
<tr>
<td>Senior Analyst 54151S</td>
<td>$ 108.49</td>
</tr>
<tr>
<td>Analyst 54151S</td>
<td>$ 97.09</td>
</tr>
<tr>
<td>Junior Analyst 54151S</td>
<td>$ 79.94</td>
</tr>
<tr>
<td>Staff Analyst 54151S</td>
<td>$ 68.53</td>
</tr>
<tr>
<td>Support 54151S</td>
<td>$ 57.11</td>
</tr>
<tr>
<td>Administrative Support 54151S</td>
<td>$ 45.68</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Labor Categories for SIN 54151HACS Penetration Testing</th>
<th>GSA Net Rates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Penetration Tester and Technician SME IV PenTest</td>
<td>$ 205.58</td>
</tr>
<tr>
<td>Penetration Tester and Technician SME IIII PenTest</td>
<td>$ 182.73</td>
</tr>
<tr>
<td>Penetration Tester and Technician SME II PenTest</td>
<td>$ 159.90</td>
</tr>
<tr>
<td>Penetration Tester and Technician SME I PenTest</td>
<td>$ 137.05</td>
</tr>
<tr>
<td>Penetration Tester and Technician Task Manager PenTest</td>
<td>$ 134.47</td>
</tr>
<tr>
<td>Penetration Tester and Technician Principal PenTest</td>
<td>$ 121.55</td>
</tr>
<tr>
<td>Penetration Tester and Technician Senior Analyst PenTest</td>
<td>$ 107.58</td>
</tr>
<tr>
<td>Penetration Tester and Technician Analyst PenTest</td>
<td>$ 96.81</td>
</tr>
<tr>
<td>Penetration Tester and Technician Junior Analyst PenTest</td>
<td>$ 75.29</td>
</tr>
<tr>
<td>Penetration Tester and Technician Staff Analyst PenTest</td>
<td>$ 68.53</td>
</tr>
<tr>
<td>Penetration Tester and Technician Support PenTest</td>
<td>$ 57.11</td>
</tr>
<tr>
<td>Penetration Tester and Technician Technical Writer PenTest</td>
<td>$ 45.68</td>
</tr>
<tr>
<td>Labor Categories for SIN 54151HACS</td>
<td>GSA Net Rates</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td><strong>Incident Response</strong></td>
<td></td>
</tr>
<tr>
<td>Incident Response SME IV IR</td>
<td>$ 205.58</td>
</tr>
<tr>
<td>Incident Response SME III IR</td>
<td>$ 182.73</td>
</tr>
<tr>
<td>Incident Response SME II IR</td>
<td>$ 159.90</td>
</tr>
<tr>
<td>Incident Response SME I IR</td>
<td>$ 137.05</td>
</tr>
<tr>
<td>Incident Response Task Manager IR</td>
<td>$ 134.47</td>
</tr>
<tr>
<td>Incident Response Principal IR</td>
<td>$ 121.55</td>
</tr>
<tr>
<td>Incident Response Senior Analyst IR</td>
<td>$ 107.58</td>
</tr>
<tr>
<td>Incident Response Analyst IR</td>
<td>$ 96.81</td>
</tr>
<tr>
<td>Incident Response Junior Analyst IR</td>
<td>$ 75.29</td>
</tr>
<tr>
<td>Incident Response Staff Analyst IR</td>
<td>$ 68.53</td>
</tr>
<tr>
<td>Incident Response Support IR</td>
<td>$ 57.11</td>
</tr>
<tr>
<td>Incident Response Technical Writer IR</td>
<td>$ 45.68</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Labor Categories for SIN 54151HACS</th>
<th>GSA Net Rates</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Vulnerability Assessment (RVA)</strong></td>
<td></td>
</tr>
<tr>
<td>Risk Vulnerability Assessment (RVA SME IV) RVA</td>
<td>$ 205.58</td>
</tr>
<tr>
<td>Risk Vulnerability Assessment (RVA SME III) RVA</td>
<td>$ 182.73</td>
</tr>
<tr>
<td>Risk Vulnerability Assessment (RVA SME II) RVA</td>
<td>$ 159.90</td>
</tr>
<tr>
<td>Risk Vulnerability Assessment (RVA SME I) RVA</td>
<td>$ 137.05</td>
</tr>
<tr>
<td>Risk Vulnerability Assessment (RVA Task Manager) RVA</td>
<td>$ 134.47</td>
</tr>
<tr>
<td>Risk Vulnerability Assessment (RVA Principal) RVA</td>
<td>$ 121.55</td>
</tr>
<tr>
<td>Risk Vulnerability Assessment (RVA Senior Analyst) RVA</td>
<td>$ 107.58</td>
</tr>
<tr>
<td>Risk Vulnerability Assessment (RVA Analyst) RVA</td>
<td>$ 96.81</td>
</tr>
<tr>
<td>Risk Vulnerability Assessment (RVA Junior Analyst) RVA</td>
<td>$ 75.29</td>
</tr>
<tr>
<td>Risk Vulnerability Assessment (RVA Staff Analyst) RVA</td>
<td>$ 68.53</td>
</tr>
<tr>
<td>Risk Vulnerability Assessment (RVA Support) RVA</td>
<td>$ 57.11</td>
</tr>
<tr>
<td>Risk Vulnerability Assessment (RVA Technical Writer) RVA</td>
<td>$ 45.68</td>
</tr>
</tbody>
</table>

Discounts Offered:
- **Prompt Payment**: 1% if net 10 days.
- **Volume Discount**: 2% for dollar volume > $500,000 in one calendar year.

Concessions Offered:
- **Value added services**: Access to the use of proprietary evaluation tools and dedicated resources.
- **TWM Associates, Inc.** Number: 82-701-1248
  TWM Associates, Inc. is currently registered in the Central Contractor Registration (CCR) now SAM system.
- Credit cards are accepted for payments.

*Based on GSA MAS Contract GS-35F-315CA Mod A847.*

Last Updated: 07-13-2022
2. **MAXIMUM ORDER:** $500,000 per SIN 54151S, 54151HACS, and per order

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

3. **MINIMUM ORDER:** $100

4. **GEOGRAPHIC COVERAGE:** Domestic and worldwide

5. **POINT(S) OF PRODUCTION:** NA

6. **DISCOUNTS FROM LIST PRICES:** GSA NET Prices are shown on the attached GSA Pricelist. Negotiated discount has been applied and the IFF has been added.

   For calculation of the GSA Schedule price see Page 1A.

7. **QUANTITY DISCOUNT(S):** 2% for orders over $500,000 within one (1) calendar year.

8. **PROMPT PAYMENT TERMS:** 1% Net 10 days/Net 30. NOTE: Prompt payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions.

9. **FOREIGN ITEMS:** NA

10a. **TIME OF DELIVERY:** As negotiated with the ordering activity

10b. **EXPEDITED DELIVERY:** Items available for expedited delivery are noted in this price list.

10c. **OVERNIGHT AND 2-DAY DELIVERY:** Overnight and 2-day delivery are available. Contact the Contractor for rates.

10d. **URGENT REQUIREMENTS:** Agencies can contact the Contractor’s representative to effect a faster delivery. Customers are encouraged to contact the contractor for the purpose of requesting accelerated delivery.

11. **FOB POINT:** Destination

123a. **ORDERING ADDRESS:** Same as contractor

12b. **ORDERING PROCEDURES:** For supplies and services, the ordering procedures, information on Blanket Purchase Agreements (BPAs) are found in Federal Acquisition Regulation 8.405-3.

13. **PAYMENT ADDRESS:**

   Payment Information: **Electronic**
   Wells Fargo Bank
   10501 Main Street
   Fairfax, VA 22030
   Account Title: TWM Associates, Inc.
14. **WARRANTY PROVISION:** NA

15. **EXPORT PACKING CHARGES:** NA

16. **TERMS AND CONDITIONS OF RENTAL, MAINTENANCE, AND REPAIR (IF APPLICABLE):** N/A

17. **TERMS AND CONDITIONS OF INSTALLATION (IF APPLICABLE):** N/A

18.a. **TERMS AND CONDITIONS OF REPAIR PARTS INDICATING DATE OF PARTS PRICE LISTS AND ANY DISCOUNTS FROM LIST PRICES (IF AVAILABLE):** N/A

18.b. **TERMS AND CONDITIONS FOR ANY OTHER SERVICES (IF APPLICABLE):** N/A

19. **LIST OF SERVICE AND DISTRIBUTION POINTS (IF APPLICABLE):** N/A

20. **LIST OF PARTICIPATING DEALERS (IF APPLICABLE):** N/A

21. **PREVENTIVE MAINTENANCE (IF APPLICABLE):** N/A

22.a. **SPECIAL ATTRIBUTES SUCH AS ENVIRONMENTAL ATTRIBUTES (e.g. recycled content, energy efficiency, and/or reduced pollutants):** N/A

22b. **Section 508 Compliance for Electronic and Information Technology (EIT):** N/A

23. **Unique Entity Identifier (UEI):** XELWCZZ9NUE7

24. **NOTIFICATION REGARDING REGISTRATION IN SYSTEM for AWARD MANAGEMENT (SAM) DATABASE:** Contractor has an Active Registration in the SAM database.
DESCRIPTION OF IT SERVICES AND PRICING

Description of each type of IT Service offered under Special Item Number 54151S:

FPDS Code D306 IT Systems Analysis Services

1. Financial application reviews for adequate internal controls and security configurations.
2. System review and/or audits for internal controls, security configurations, FISMA, HIPPA, and other compliance related activities.
3. Cost/benefit analysis for development decisions on financial and non-financial applications.
4. Benchmarking of types of software used in other agencies and organizations.
5. Benchmarking of COTS packages against desired functionality in applications.
6. Creation of functional requirements based on reviews of existing business processes.
7. Architectural modifications to existing systems after analysis of what’s in place and where the organization wants to go.
8. Evaluation and integration of new technologies into existing architectures or new architectures.

FPDS Code D307 IT Automated Information Systems Design and Integration Services

1. Network architecture design and connectivity development.
2. New technology evaluation and integration recommendations on new or existing network configurations.
3. Development and maintenance of certification and accreditation findings reporting systems.
4. Security training and self-assessments through web page developed tools.
5. Development and maintenance of database reporting systems.

FPDS Code D310 IT Backup and Cyber Security Services

1. Develop security policies.
2. Develop Memorandum Of Assignments and Memorandum Of Understandings.
3. Develop Penetration and Analysis procedures and execute those developed procedures.
4. Support of FISMA, HIPAA, and other compliance related activities.
5. Support for Office of Inspector General (OIG) audit and review activities.
6. Application control reviews.
7. Security Controls Assessments (SCA), System Test & Evaluations (ST&Es).
8. Physical security reviews.
9. Audit or reviews in accordance with Yellow Book standards.
10. Audit or review in accordance with FISMA, OMB, FISMA, FISCAM, Yellow Book, NIST 800-53, NIST, and other designated requirements.
11. Develop contingency plans.
12. Develop security plans.
13. Develop SSAAs., SSPs, Assessment Control plans
15. Develop Security Controls Analysis, ST&E, and related plans and procedures.
16. Develop test reports.
17. Develop audit reports.
18. Develop transition plans.
20. Vulnerability analysis.
22. Develop self-assessment security programs.
23. Execute general controls reviews for security administration, logical access controls, physical access controls, network security structures, operating systems controls, and other related configurations.
24. Develop technical evaluation procedures for operating systems (i.e., zOS, UNIX, Windows, Linux, etc.), networks, routers, security and database applications (i.e., RACF, Oracle, Sybase, Top Secret, ACF2, etc.)
25. NATO specific security services.
26. EPA specific security services.
27. Execute SCAs, ST&Es, and other security assessments.
28. Evaluate and re-write security policies.

**FPDS Code D316 IT Network Management Services**

1. Router configurations.
2. Network management software configuration.
3. Switch configurations.
4. Assessment and Authorization, Certification and Accreditation specific network router commands and security criteria for operation.
5. Firewall configuration.
6. Preparation of and documentation of network configuration guides.
7. Administration of architectures and network components.

**FPDS Code D399 Other IT Services, Not Elsewhere Classified**

1. Investigative support services and evidential information gathering through the computer.
2. Configuration of computers, networks, firewalls, and routers in anticipation of evidential information gathering for investigative support matters.
3. Other related IT and Cyber services not specifically delineated above.
DESCRIPTION OF JOB TITLES (LABOR CATEGORIES):

Job Title: Program Manager

Minimum/General Experience: Thirteen (13) years of management experience which applies to the management of programs in the Government sector. Requires competence in all phases of Contract Management, coordination with Contracting Officer’s Representatives, and some technical knowledge. Must demonstrate experience in all phases of the assignment of resources, supervision of assigned resources, and handling of project administrative matters.

Functional Responsibility: Responsible for overall contract performance for contracts exceeding $500,000. The Program Manager is responsible for the management of the project in terms of personnel resources and Contracting Officer coordination. The Program Manager will ensure the assigned work is completed based on the deliverable schedules and contributes technical support on tasks as necessary.

Minimum Education: Masters Degree in Computer Science or Management Information Systems. Also acceptable is a technical Bachelor’s Degree (Computer Science, Engineering, or Management Information Systems) with fifteen (15) years of program management experience, a CPA or CISA with fifteen (15) years’ experience, or a non-technical Bachelor’s Degree with seventeen (17) years of program management experience, or no degree with nineteen (19) years of experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

Systems Analysis Services

Job Title: Systems Analysis Task Manager

Minimum/General Experience: Thirteen (13) 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, infrastructure and management practices.

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

Minimum Education: Bachelor’s Degree in Computer Science or Management Information Systems. Also acceptable is a technical Bachelor’s Degree (Computer Science, Engineering, or Management Information Systems) with thirteen (13) years of technical experience, a CPA or CISA with thirteen (13) years’ experience, or a non-technical degree with fifteen (15) years of technical experience or no degree with seventeen (17) years of experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.
Job Title: Systems Analysis Principal

Minimum/General Experience: Eleven (11) years of technical experience which applies to systems analysis and design techniques for complex computer systems. Requires competence in most phases of systems analysis techniques, concepts and methods; also requires knowledge of available hardware, system software, input/output devices, infrastructure and management practices.

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

Minimum Education: Bachelor’s Degree in Computer Science or Management Information Systems. Also acceptable is a technical Masters Degree with nine (9) years of experience or an Engineering Degree or other Technical Degree with eleven (11) years of technical experience, a CPA or CISA with eleven (11) years’ experience, or a non-technical Bachelor’s degree with thirteen (13) years of technical experience or no degree with fifteen (15) years of experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

Job Title: Systems Analysis Senior Analyst

Minimum/General Experience: Eight (8) years of technical experience, which applies to systems analysis and design techniques for complex computer systems. Requires competence in many phases of systems analysis techniques, concepts and methods; also requires strong knowledge of available hardware, system software, input/output devices, infrastructure and management practices.

Functional Responsibility: Works with users in formulating requirements, researches and advises alternative approaches, gathers information for and conducts feasibility studies.

Minimum Education: Bachelor’s Degree in Computer Science or Management Information Systems. Also acceptable is an Masters Degree with six (6) years of technical experience or Engineering Degree or other Technical Degree with eight (8) years of technical experience, a CPA or CISA with eight (8) years’ experience, or a non-technical degree with ten (10) years of technical experience or no degree with twelve (12) years of technical experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

Job Title: Systems Analysis Analyst

Minimum/General Experience: Six (6) years of technical experience which applies to systems analysis and design techniques for complex computer systems. Requires competence in many phases of systems analysis techniques, concepts and methods; also requires some knowledge of available hardware, system software, input/output devices, infrastructure and management practices.

Functional Responsibility: Works with users in identifying and formulating requirements, advises alternative approaches, conducts feasibility studies.
**Minimum Education:** Bachelor’s Degree in Computer Science or Management Information Systems. Also acceptable is an Masters Degree with four (4) years technical experience or an Engineering Degree or other Technical Degree with six (6) years of technical experience, a CPA or CISA with six (6) years’ experience, or a non-technical degree with eight (8) years of technical experience or no degree with ten (10) years of technical experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** Systems Analysis Junior Analyst

**Minimum/General Experience:** Four (4) years of technical experience which applies to systems analysis and design techniques for complex computer systems. Requires competence in some phases of systems analysis techniques, concepts and methods; also requires some knowledge of available hardware, system software, input/output devices, infrastructure and management practices.

**Functional Responsibility:** Works with senior team members to help users identify and formulate requirements, assists in information gathering for alternative approaches, assists in conducting feasibility studies.

**Minimum Education:** Bachelor’s Degree in Computer Science or Management Information Systems or a CPA or CISA with four (4) years’ experience. Also acceptable is a Masters Degree with two (2) years of technical experience or a non-technical Degree with six (6) years of technical experience or no degree with eight (8) years of experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** Systems Analysis Staff Analyst

**Minimum/General Experience:** Two (2) years of technical experience which applies to systems analysis and design techniques for complex computer systems. Requires competence in some phases of systems analysis techniques, concepts and methods; also requires some knowledge of available hardware, system software, input/output devices, infrastructure and management practices.

**Functional Responsibility:** Works with senior team members to help users identify and formulate requirements, assists in information gathering for alternative approaches, assists in conducting feasibility studies.

**Minimum Education:** Bachelor’s Degree in Computer Science or Management Information Systems or a CPA or CISA with two (2) years’ experience. Also acceptable is a Masters Degree with zero (0) years technical experience or a non-technical Degree with four (4) years of technical experience or no degree with six (6) years of technical experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.
**Job Title:** Systems Analysis Support

**Minimum/General Experience:** Zero (0) years of technical experience but has college course which applies to systems analysis and design techniques for complex computer systems. Classes in some phases of systems analysis techniques, concepts and methods.

**Functional Responsibility:** Works with senior team members to help users identify and formulate requirements, assists in information gathering for alternative approaches, assists in conducting feasibility studies.

**Minimum Education:** Bachelor’s Degree in Computer Science or Management Information Systems or a CPA or CISA. Also acceptable is a non-technical Degree with two (2) years of work experience or no degree with four (4) years of work experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** Systems Analysis Administrative Support

**Minimum/General Experience:** Zero (0) years of technical experience but has administrative support experience which applies to systems analysis and design techniques for complex computer systems. Has some experience in working with word processing applications, and spreadsheet applications.

**Functional Responsibility:** Works with team members to assist in document preparation, deliverable preparation, and other necessary administrative support.

**Minimum Education:** Non-technical undergraduate degree. Also acceptable is no degree with two (2) years of administrative support experience.

**IT and Telecom Strategy and Architecture**

**Job Title:** IT Design and Integration Services Task Manager

**Minimum/General Experience:** Thirteen (13) years of technical experience in aspects of system design and integration. Competence in systems design phases of requirements analysis, conversion of requirements into system architecture, and implementation of the architectures within an operational environment. Extensive experience in interfacing applications with system security features and services required. Knowledge of available hardware, system software, input/output devices, and management practices.

**Functional Responsibility:** Guides users in formulating requirements, integrating requirements into system design and development, and advises alternative approaches.

**Minimum Education:** Masters Degree in Computer Science or Management Information Systems. Also acceptable is a technical Bachelor’s Degree (Computer Science, Engineering, or Management Information Systems) with thirteen (13) years of technical experience, a CPA or CISA with thirteen (13) years’ experience, or a non-technical degree with fifteen (15) years of technical experience or no degree with seventeen (17) years of experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.
**Job Title:** IT Design and Integration Services Principal

**Minimum/General Experience:** Eleven (11) years of technical experience in aspects of systems design and integration techniques for complex computer systems. Competence in most phases of requirement analysis, conversion of requirements into system architecture, and implementation of the architectures within an operational environment required. Comprehensive experience in interfacing applications with system security features and services and knowledge of available hardware, system software, input/output devices, and management practices required.

**Functional Responsibility:** Guides users in formulating requirements, integrating requirements into system design and development, and advises alternative approaches.

**Minimum Education:** Bachelor's Degree in Computer Science or Management Information Systems. Also acceptable is a technical Masters Degree with nine (9) years of experience or an Engineering Degree or other Technical Degree with eleven (11) years of technical experience, a CPA or CISA with eleven (11) years' experience, or a non-technical Bachelor's degree with thirteen (13) years of technical experience or no degree with fifteen (15) years of experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

---

**Job Title:** IT Design and Integration Services Senior Analyst

**Minimum/General Experience:** Eight (8) years of technical experience, in aspects of system design and integration techniques for complex computer systems. Competence in most phases of requirement analysis, conversion of requirements into system architecture, and implementation of the architectures within an operational environment required. Experience in interfacing applications with system security features and services are also required. Knowledge of available hardware, system software, input/output devices, and management practices.

**Functional Responsibility:** Works with users in formulating requirements, researches and advises alternative approaches, gathers information for and conducts feasibility studies.

**Minimum Education:** Bachelor's Degree in Computer Science or Management Information Systems. Also acceptable is an Masters Degree with six (6) years of technical experience or Engineering Degree or other Technical Degree with eight (8) years of technical experience, a CPA or CISA with eight (8) years' experience, or a non-technical degree with ten (10) years of technical experience or no degree with twelve (12) years of technical experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

---

**Job Title:** IT Design and Integration Services Analyst

**Minimum/General Experience:** Six (6) years of technical experience in aspects of system design and integration techniques for complex computer systems. Competence in some phases of requirements analysis, conversion of requirements into system architecture, and implementation of the architectures within an operational environment required. Some experience in interfacing applications with system security features and services. Knowledge of available hardware, system software, input/output devices, and
management practices.

**Functional Responsibility:** Works with users in identifying and formulating requirements, advises alternative approaches, conducts feasibility studies.

**Minimum Education:** Bachelor's Degree in Computer Science or Management Information Systems. Also acceptable is an Masters Degree with four (4) years technical experience or an Engineering Degree or other Technical Degree with six (6) years of technical experience, a CPA or CISA with six (6) years’ experience, or a non-technical degree with eight (8) years of technical experience or no degree with ten (10) years of technical experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** IT Design and Integration Services Junior Analyst

**Minimum/General Experience:** Four (4) years of technical experience in aspects of system design and integration techniques for complex computer systems. Competence in some phases of requirement analysis, conversion, and implementation of the architecture required. Knowledge of available hardware, system software, input/output devices, and management practices.

**Functional Responsibility:** Works with senior team members to help users identify and formulate requirements, assists in information gathering for alternative approaches, assists in conducting feasibility studies.

**Minimum Education:** Bachelor's Degree in Computer Science or Management Information Systems or a CPA or CISA with four (4) years’ experience. Also acceptable is a Masters Degree with two (2) years of technical experience or a non-technical Degree with six (6) years of technical experience or no degree with eight (8) years of experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** IT Design and Integration Services Staff Analyst

**Minimum/General Experience:** Two (2) years of technical experience in aspects of system design and integration techniques for complex computer systems. Competence in some phases of requirement analysis, conversion, and implementation of the architecture required. Knowledge of available hardware, system software, input/output devices, and management practices.

**Functional Responsibility:** Works with senior team members to help users identify and formulate requirements, assists in information gathering for alternative approaches, assists in conducting feasibility studies.

**Minimum Education:** Bachelor's Degree in Computer Science or Management Information Systems or a CPA or CISA with two (2) years’ experience. Also acceptable is a Masters Degree with zero (0) years technical experience or a non-technical Degree with four (4) years of technical experience or no degree with six (6) years of technical experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.
**Job Title:** IT Design and Integration Services Support

**Minimum/General Experience:** No technical experience required, but has completed college level courses in aspects of system design and integration techniques for complex computer systems. Classes in some phases of systems analysis techniques, concepts and methods required.

**Functional Responsibility:** Works with senior team members to help users identify and formulate requirements, assists in information gathering for alternative approaches, assists in conducting feasibility studies.

**Minimum Education:** Bachelor's Degree in Computer Science or Management Information Systems or a CPA or CISA. Also acceptable is a non-technical Degree with two (2) years of work experience or no degree with four (4) years of work experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

---

**Job Title:** IT Design and Integration Services Administrative Support

**Minimum/General Experience:** No technical experience required. Possesses administrative support experience that applies to support efforts for system design and integration techniques for complex computer systems. Has some experience in working with word processing applications, and spreadsheet applications.

**Functional Responsibility:** Works with team members to assist in document preparation, deliverable preparation, and other necessary administrative support.

**Minimum Education:** Non-technical undergraduate degree. Also acceptable is no degree with two (2) years of administrative support experience.

---

**IT Backup and Cyber Security Services**

**Job Title:** IT Backup and Cyber Security Services Task Manager

**Minimum/General Experience:** Thirteen (13) years of technical experience which applies to the complex problems involving all phases of Cyber Security. Experience should include systems analysis, security analysis, vulnerability evaluations, controls reviews, and certification and accreditation. Requires competence in providing Cyber Security solutions, providing recommendations for consolidation into Cyber Security policies and procedures. Extensive experience required in all areas of technical support for secure software development, conducting general controls reviews, developing technical evaluations for various operating systems, executing Security Test and Evaluation Plans and Procedures, and demonstrated knowledge of the interrelationships of requirements from Public Laws and OMB Circulars.

**Functional Responsibility:** Guides users in formulating security requirements, integrating security requirements into existing system architectures, developing security test plans, overseeing the execution of security testing, and advises alternative approaches.
**Minimum Education:** Masters Degree in Computer Science or Management Information Systems. Also acceptable is a technical Bachelor's Degree (Computer Science, Engineering, or Management Information Systems) with thirteen (13) years of technical experience, a CPA or CISA with thirteen (13) years’ experience, or a non-technical degree with fifteen (15) years of technical experience or no degree with seventeen (17) years of experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** IT Backup and Cyber Security Services Principal

**Minimum/General Experience:** Eleven (11) years of technical experience which applies to the complex problems involving all phases of Cyber Security. Experience should include systems analysis, security analysis, vulnerability evaluations, controls reviews, and certification and accreditation. Requires competence in providing Cyber Security solutions, providing recommendations for consolidation into Cyber Security policies and procedures. Experience required in all areas of technical support for secure software development, conducting general controls reviews, developing technical evaluations for various operating systems, executing Security Test and Evaluation Plans and Procedures, and demonstrated knowledge of the interrelationships of requirements from Public Laws and OMB Circulars.

**Functional Responsibility:** Guides users in formulating security requirements, integrating security requirements into existing system architectures, and advises alternative approaches. Executes security test plans and develops reports on the results of the testing performed.

**Minimum Education:** Bachelor's Degree in Computer Science or Management Information Systems. Also acceptable is a technical Masters Degree with nine (9) years of experience or an Engineering Degree or other Technical Degree with eleven (11) years of technical experience, a CPA or CISA with eleven (11) years’ experience, or a non-technical Bachelor's degree with thirteen (13) years of technical experience or no degree with fifteen (15) years of experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** IT Backup and Cyber Security Services Senior Analyst

**Minimum/General Experience:** Eight (8) years of technical experience, which applies to the complex problems involving all phases of Cyber Security. Experience should include systems analysis, security analysis, and vulnerability evaluations, controls reviews or certification and accreditation. Requires competence in providing Cyber Security solutions, providing recommendations for consolidation into Cyber Security policies and procedures. Experience required in most areas of technical support for secure software development, conducting general controls reviews, developing technical evaluations for various operating systems, executing Security Test and Evaluation Plans and Procedures, and knowledge of the interrelationships of requirements from Public Laws and OMB Circulars.
**Functional Responsibility:** Assists senior team members in formulating security requirements, integrating security requirements into existing system architectures, and advises alternative approaches. Executes security test plans and contributes to reports on the results of the testing performed.

**Minimum Education:** Bachelor's Degree in Computer Science or Management Information Systems. Also acceptable is a Masters' Degree with six (6) years of technical experience or Engineering Degree or other Technical Degree with eight (8) years of technical experience, a CPA or CISA with eight (8) years’ experience, or a non-technical degree with ten (10) years of technical experience or no degree with twelve (12) years of technical experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** IT Backup and Cyber Security Services Analyst

**Minimum/General Experience:** Six (6) years of technical experience which applies to the complex problems involving all phases of Cyber Security. Experience should include security analysis, controls reviews or certification and accreditation. Requires experience in providing Cyber Security solutions, providing recommendations for consolidation into Cyber Security policies and procedures. Some experience required in areas of technical support for secure software development, conducting general controls reviews, developing technical evaluations for various operating systems, executing Security Test and Evaluation Plans and Procedures, and some knowledge of the interrelationships of requirements from Public Laws and OMB Circulars.

**Functional Responsibility:** Assists senior team members in formulating security requirements, and integrating security requirements into system architectures. Contributes to the analysis and recommendation of alternative approaches. Executes security test plans and contributes to reports on the results of the testing performed.

**Minimum Education:** Bachelor's Degree in Computer Science or Management Information Systems. Also acceptable is an Masters Degree with four (4) years technical experience or an Engineering Degree or other Technical Degree with six (6) years of technical experience, a CPA or CISA with six (6) years’ experience, or a non-technical degree with eight (8) years of technical experience or no degree with ten (10) years of technical experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** IT Backup and Cyber Security Services Junior Analyst

**Minimum/General Experience:** Four (4) years of technical experience which applies to the complex problems involving the phases of Cyber Security. Experience should include some systems analysis, security analysis, controls reviews or certification and accreditation. Requires competence in researching Cyber Security solutions and Cyber Security policies and procedures. Some experience required in areas of technical support for secure software development, executing general controls review procedures, executing Security Test and Evaluation Procedures, and knowledge of the interrelationships of requirements from Public Laws and OMB Circulars.
Functional Responsibility: Works with senior team members to research and formulate security requirements.

Minimum Education: Bachelor's Degree in Computer Science or Management Information Systems or a CPA or CISA with four (4) years' experience. Also acceptable is a Masters Degree with two (2) years of technical experience or a non-technical Degree with six (6) years of technical experience or no degree with eight (8) years of experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

Job Title: IT Backup and Cyber Security Services Staff Analyst

Minimum/General Experience: Two (2) years of technical experience which applies to the complex problems involving the phases of Cyber Security. Experience may include systems analysis, security analysis, controls reviews, or certification and accreditation. Requires research experience in Cyber Security solutions and Cyber Security policies and procedures. Experience required in executing general controls reviews, executing Security Test and Evaluation Plans and Procedures or demonstrated knowledge of the interrelationships of requirements from Public Laws and OMB Circulars.

Functional Responsibility: Works with senior team members to help formulate security requirements.

Minimum Education: Bachelor's Degree in Computer Science or Management Information Systems or a CPA or CISA with two (2) years' experience. Also acceptable is a Masters Degree with zero (0) years technical experience or a non-technical Degree with four (4) years of technical experience or no degree with six (6) years of technical experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

Job Title: IT Backup and Cyber Security Services Analysis Support

Minimum/General Experience: No technical experience required, but has completed college level courses which apply to any of the phases of Information Security. Requires research skills for Cyber Security and Cyber Security policies and procedures.

Functional Responsibility: Works with senior team members to help formulate security requirements.

Minimum Education: Bachelor's Degree in Computer Science or Management Information Systems or a CPA or CISA. Also acceptable is a non-technical Degree with two (2) years of work experience or no degree with four (4) years of work experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

Job Title: IT Backup and Cyber Security Services Administrative Support

Minimum/General Experience: No technical experience required. Must possess administrative support experience that applies to Cyber Security phases. Has some experience in working with word processing applications, and spreadsheet applications.
**Functional Responsibility:** Works with team members to assist in document preparation, deliverable preparation, and other necessary administrative support.

**Minimum Education:** Non-technical undergraduate degree. Also acceptable is no degree with two (2) years of administrative support experience.

---

**IT Network Management Services**

**Job Title:** IT Network Management Services Task Manager

**Minimum/General Experience:** Thirteen (13) years of technical experience which applies to network management, installation and configuration of complex local and wide area networks, and their associated components. Requires competence in all phases of network design, requirement analysis, implementation of network architecture, and maintenance of networks in an operational environment. Extensive experience required in development and use of secure network and network management software, firewall and router access controls and configurations, and the certification and accreditation process of local and wide area networks.

**Functional Responsibility:** Guides users in designing, securing, evaluating, and maintaining network environments.

**Minimum Education:** Bachelor’s Degree in Computer Science or Management Information Systems. Also acceptable is a technical Bachelor’s Degree (Computer Science, Engineering, or Management Information Systems) with thirteen (13) years of technical experience, a CPA or CISA with thirteen (13) years’ experience, or a non-technical degree with fifteen (15) years of technical experience or no degree with seventeen (17) years of experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** IT Network Management Services Principal

**Minimum/General Experience:** Eleven (11) years of technical experience which applies to network management, installation and configuration of complex local and wide area networks, and their associated components. Requires competence in network design, requirement analysis, implementation of network architecture, and maintenance of networks in an operational environment. Extensive experience required in development and use of secure network and network management software, firewall and router access controls and configurations, and the certification and accreditation process of local and wide area networks.

**Functional Responsibility:** Guides users in making recommendations for the designing, securing, evaluating, and maintaining of network environments.

**Minimum Education:** Bachelor’s Degree in Computer Science or Management Information Systems. Also acceptable is a technical Masters Degree with nine (9) years of experience or an Engineering Degree or other Technical Degree with eleven (11) years of technical experience, a CPA or CISA with eleven (11) years’ experience, or a non-technical Bachelor’s degree with thirteen (13) years of technical experience or no degree with fifteen (15) years of experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.
Job Title: IT Network Management Services Senior Analyst

Minimum/General Experience: Eight (8) years of technical experience, which applies to network management, installation and configuration of complex local and wide area networks, and their associated components. Requires competence in some phases of network design, requirements analysis, and implementation of network architecture. May also include some experience in the maintenance of networks in an operational environment. Some experience required in development and use of secure network and network management software, firewall and router access controls and configurations, and the certification and accreditation process of local and wide area networks.

Functional Responsibility: Work with Senior Team members in designing, securing, evaluating, and maintaining network environments.

Minimum Education: Bachelor's Degree in Computer Science or Management Information Systems. Also acceptable is a Masters Degree with six (6) years of technical experience or Engineering Degree or other Technical Degree with eight (8) years of technical experience, a CPA or CISA with eight (8) years' experience, or a non-technical degree with ten (10) years of technical experience or no degree with twelve (12) years of technical experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

Job Title: IT Network Management Services Analyst

Minimum/General Experience: Six (6) years of technical experience which applies to network management, installation and configuration of complex local and wide area networks, and their associated components. Requires competence in some phases of network design, requirements analysis, and implementation of network architecture. Some experience is also required in development and use of secure network and network management software, firewall and router access controls and configurations, or the certification and accreditation process of local and wide area networks.

Functional Responsibility: Works with Senior Team members in designing, securing, evaluating, and maintaining network environments.

Minimum Education: Bachelor's Degree in Computer Science or Management Information Systems. Also acceptable is an Masters Degree with four (4) years technical experience or an Engineering Degree or other Technical Degree with six (6) years of technical experience, a CPA or CISA with six (6) years' experience, or a non-technical degree with eight (8) years of technical experience or no degree with ten (10) years of technical experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

Job Title: IT Network Management Services Junior Analyst

Minimum/General Experience: Four (4) years of technical experience which applies to network management, installation and configuration of complex local and wide area networks, and their associated components. Experience required in development and use of secure network and network management software or in network maintenance.
**Functional Responsibility:** Works with senior team members in designing, securing, evaluating, and maintaining network environments.

**Minimum Education:** Bachelor's Degree in Computer Science or Management Information Systems or a CPA or CISA with four (4) years of experience. Also acceptable is a Masters Degree with two (2) years of technical experience or a non-technical Degree with six (6) years of technical experience or no degree with eight (8) years of experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** IT Network Management Services Staff Analyst

**Minimum/General Experience:** Two (2) years of technical experience which applies to network management, installation and configuration of complex local and wide area networks, and their associated components. Some experience required in development and use of secure network and networks management software or the certification and accreditation process of local and wide area networks.

**Functional Responsibility:** Works with senior team members in designing, securing, evaluating, and maintaining network environments.

**Minimum Education:** Bachelor's Degree in Computer Science or Management Information Systems or a CPA or CISA with two (2) years of experience. Also acceptable is a Masters Degree with zero (0) years technical experience or a non-technical Degree with four (4) years of technical experience or no degree with six (6) years of technical experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** IT Network Management Services Support

**Minimum/General Experience:** No technical experience required, but has completed college level courses which apply to the complex problems involving the phases of Network Management. Requires familiarity with development and use of secure network and network management software or the certification and accreditation process of local and wide area networks.

**Functional Responsibility:** Works with senior team members.

**Minimum Education:** Bachelor's Degree in Computer Science or Management Information Systems or a CPA or CISA. Also acceptable is a non-technical Degree with two (2) years of work experience or no degree with four (4) years of work experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** IT Network Management Services Administrative Support

**Minimum/General Experience:** No technical experience required. Must possess administrative support experience that applies to Network Management. Has some experience in working with word processing applications, and spreadsheet applications.
**Functional Responsibility:** Works with team members to assist in document preparation, deliverable preparation, and other necessary administrative support.

**Minimum Education:** Non-technical undergraduate degree. Also acceptable is no degree with two (2) years of administrative support experience.

**Other Information Technology Services**

**Job Title:** Information Technology Services Task Manager

**Minimum/General Experience:** Thirteen (13) years of technical experience in all phases of security, system design and integration, development, and network management. Experience can include Investigative Support services for information gathering through complex computer systems. Demonstrated experience in developing recommended system exposures and recommended procedures for gathering and assessing evidential matter. Extensive experience required in all areas of conducting audits and audit reviews in accordance with Yellow book standards and OMB requirements.

**Functional Responsibility:** Develops plans for the evidential data gathering of information through complex computer systems. Develops recommendations for system exposures and weaknesses based on the evidential information gathering.

**Minimum Education:** Bachelor’s Degree in Computer Science or Management Information Systems. Also acceptable is a technical Bachelor’s Degree (Computer Science, Engineering, or Management Information Systems) with thirteen (13) years of technical experience, a CPA or CISA with thirteen (13) years’ experience, or a non-technical degree with fifteen (15) years of technical experience or no degree with seventeen (17) years of experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** Information Technology Services Principal

**Minimum/General Experience:** Eleven (11) years of technical experience in all phases of security, system design and integration, development, and network management. Experience can include Investigative Support services for information gathering through complex computer systems. Demonstrated experience in developing recommended system exposures and recommended procedures for gathering and assessing evidential matter. Significant experience required in conducting audits and audit reviews in accordance with Yellow book standards and OMB requirements.

**Functional Responsibility:** Develops and executes plans for the evidential data gathering of information through complex computer systems. Develops recommendations for system exposures and weaknesses based on the evidential information gathering. Develops reports and briefings on the recommendations made.

**Minimum Education:** Bachelor’s Degree in Computer Science or Management Information Systems. Also acceptable is a technical Masters Degree with nine (9) years of experience or an Engineering Degree or other Technical Degree with eleven (11) years of technical experience, a CPA or CISA with eleven (11) years’ experience, or a non-technical Bachelor’s degree with thirteen (13) years of technical experience or no degree with fifteen (15) years of experience. A CISSP, CISM, CGEIT or other certification may
substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** Information Technology Services Senior Analyst

**Minimum/General Experience:** Eight (8) years of technical experience, in most phases of security, system design and integration, development, and network management. Experience can include Investigative Support services for information gathering through complex computer systems. Demonstrated experience in developing recommended system exposures and recommended procedures for gathering and assessing evidential matter. Some experience required in conducting audits and audit reviews in accordance with Yellow book standards and OMB requirements.

**Functional Responsibility:** Contributes to the development and execution of plans for the evidential data gathering of information through complex computer systems. Contributes recommendations for system exposures and weaknesses based on the evidential information gathering.

**Minimum Education:** Bachelor’s Degree in Computer Science or Management Information Systems. Also acceptable is a Masters Degree with six (6) years of technical experience or Engineering Degree or other Technical Degree with eight (8) years of technical experience, a CPA or CISA with eight (8) years’ experience, or a non-technical degree with ten (10) years of technical experience or no degree with twelve (12) years of technical experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** Information Technology Services Analyst

**Minimum/General Experience:** Six (6) years of technical experience in some phases of security, system design and integration, development, and network management. Experience can include Investigative Support services for information gathering through complex computer systems. Some experience in developing recommended system exposures and recommended procedures for gathering and assessing evidential matter. Experience required in executing audits and audit reviews in accordance with Yellow book standards and OMB requirements.

**Functional Responsibility:** Executes plans for the evidential data gathering of information through complex computer systems. Contributes recommendations for system exposures and weaknesses based on the evidential information gathering.

**Minimum Education:** Bachelor’s Degree in Computer Science or Management Information Systems. Also acceptable is an Masters Degree with four (4) years technical experience or an Engineering Degree or other Technical Degree with six (6) years of technical experience, a CPA or CISA with six (6) years’ experience, or a non-technical degree with eight (8) years of technical experience or no degree with ten (10) years of technical experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** Information Technology Services Junior Analyst

**Minimum/General Experience:** Four (4) years of technical experience in some phases of security, system design and integration, development, and network management.
Experience can include Investigative Support services for information gathering through complex computer systems. Some experience in developing recommended system exposures and recommended procedures for gathering and assessing evidential matter. Experience required in executing audits and audit reviews in accordance with Yellow book standards and OMB requirements.

**Functional Responsibility:** Executes plans for the evidential data gathering of information through complex computer systems.

**Minimum Education:** Bachelor's Degree in Computer Science or Management Information Systems or a CPA or CISA with four (4) years of experience. Also acceptable is a Masters Degree with two (2) years of technical experience or a non-technical Degree with six (6) years of technical experience or no degree with eight (8) years of experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** Information Technology Services Staff Analyst

**Minimum/General Experience:** Two (2) years of technical experience in a phase of security, system design and integration, development, or network management. Experience can include Investigative Support services for information gathering through complex computer systems. Experience required in executing audits and audit reviews in accordance with Yellow book standards or OMB requirements.

**Functional Responsibility:** Executes plans for the evidential data gathering of information through complex computer systems.

**Minimum Education:** Bachelor's Degree in Computer Science or Management Information Systems or a CPA or CISA with two (2) years’ experience. Also acceptable is a Masters Degree with zero (0) years technical experience or a non-technical Degree with four (4) years of technical experience or no degree with six (6) years of technical experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** Information Technology Services Analysis Support

**Minimum/General Experience:** No technical experience required, but has completed college level courses in security, system design and integration, development, network management, or criminal justice. Classes or experience in audit is also required.

**Functional Responsibility:** Works with senior team members to execute plans for the evidential data gathering of information through complex computer systems.

**Minimum Education:** Bachelor's Degree in Computer Science or Management Information Systems or a CPA or CISA. Also acceptable is a non-technical Degree with two (2) years of work experience or no degree with four (4) years of work experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** Information Technology Services Administrative Support

**Minimum/General Experience:** No technical experience required. Has some experience
in working with word processing applications, and spreadsheet applications.

**Functional Responsibility:** Works with team members to assist in document preparation, deliverable preparation, and other necessary administrative support.

**Minimum Education:** Non-technical undergraduate degree. Also acceptable is no degree with two (2) years of administrative support experience.

**SMEs All Proposed 54151S and 54151HACS SINs**

**Job Title:** Information Technology Services Subject Matter Expert (SME) IV

**Minimum/General Experience:** Thirteen (13) years of technical experience in phases of security, system design and integration, development, and network management. Experience can include Investigative Support services for information gathering through complex computer systems. Demonstrated experience in developing recommended system exposures and recommended procedures for gathering and assessing evidential matter. Extensive experience can also include all areas of conducting audits and audit reviews in accordance with FISMA, SOX, Yellow book standards, FISCAM and/or OMB requirements.

**Functional Responsibility:** Develops plans for the evidential data gathering of information through complex computer systems. Develop recommendations for system exposures and weaknesses based on the evidential information gathering.

**Minimum Education:** Masters Degree in Computer Science, Management Information Systems, or related discipline. Also acceptable is a technical Bachelor’s Degree (Computer Science, Engineering, or Management Information Systems) with fifteen (15) years of technical experience, a CPA or CISA with fifteen (15) years’ experience, or a non-technical degree with seventeen (17) years of technical experience or no degree with nineteen (19) years of experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** Information Technology Services SME III

**Minimum/General Experience:** Eleven (11) years of technical experience in all phases of security, system design and integration, development, and network management. Experience can include Investigative Support services for information gathering through complex computer systems. Demonstrated experience in developing recommended system exposures and recommended procedures for gathering and assessing evidential matter. Significant experience required in conducting audits and audit reviews in accordance with FISMA, SOX, Yellow book standards, FISCAM and/or OMB requirements.

**Functional Responsibility:** Develops and executes plans for the evidential data gathering of information through complex computer systems. Develop recommendations for system exposures and weaknesses based on the evidential information gathering. Develops reports and briefings on the recommendations made.

**Minimum Education:** Bachelor’s Degree in Computer Science, Management Information Systems or related discipline. Also acceptable is a technical Masters Degree with nine (9) years of experience or Technical Degree with eleven (11) years of technical experience, a
CPA or CISA with eleven (11) years' experience, or a non-technical Bachelor’s degree with thirteen (13) years of technical experience or no degree with fifteen (15) years of experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** Information Technology Services SME II

**Minimum/General Experience:** Eight (8) years of technical experience, in most phases of security, system design and integration, development, and network management. Experience can include Investigative Support services for information gathering through complex computer systems. Demonstrated experience in developing recommended system exposures and recommended procedures for gathering and assessing evidential matter. Some experience required in conducting audits and audit reviews in accordance with FISMA, SOX, Yellow book standards, FISCAM and/or OMB requirements.

**Functional Responsibility:** Contributes to the development and execution of plans for the evidential data gathering of information through complex computer systems. Contribute recommendations for system exposures and weaknesses based on the evidential information gathering.

**Minimum Education:** Bachelor's Degree in Computer Science, Management Information Systems, or related discipline. Also acceptable is a Masters Degree with six (6) years of technical experience or Technical Degree with eight (8) years of technical experience, a CPA or CISA with eight (8) years of experience, or a non-technical degree with ten (10) years of technical experience or no degree with twelve (12) years of technical experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** Information Technology SME I

**Minimum/General Experience:** Five (5) years of technical experience in some phases of security, system design and integration, development, and network management. Experience can include Investigative Support services for information gathering through complex computer systems. Some experience in developing recommended system exposures and recommended procedures for gathering and assessing evidential matter. Experience required in executing audits and audit reviews in accordance with FISMA, SOX, Yellow book standards, FISCAM and/or OMB requirements.

**Functional Responsibility:** Executes plans for the evidential data gathering of information through complex computer systems. Contribute recommendations for system exposures and weaknesses based on the evidential information gathering.

**Minimum Education:** Bachelor’s Degree in Computer Science, Management Information Systems, or related discipline. Also acceptable is an Masters Degree with three (3) years technical experience or other Technical Degree with five (5) years of technical experience, a CPA or CISA with five (5) years’ experience, or a non-technical degree with seven (7) years of technical experience or no degree with nine (9) years of technical experience. A CISSP, CISM, CGEIT or other certification may substitute for 3 general years of experience and 3 technical years of experience.
Highly Adaptive Cybersecurity Services (HACS) FSC/PSC Code D399

54151HACS Penetration Testing

Description of services offered under all FPDS Codes for 54151HACS Penetration Testing include but are not limited to:

1. Conducting and/or supporting authorized penetration testing on enterprise network assets.
2. Analyzing site/enterprise Computer Network Defense policies and configurations and evaluate compliance with regulations and enterprise directives.
3. Assisting with the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems, and processes).

Job Title: Penetration Testing and Technician SME IV

Minimum/General Experience: Thirteen (13) years of technical experience which applies to penetration testing and technician techniques for penetration testing. Demonstrated experience in all phases of penetration testing techniques, concepts and methods; also requires extensive knowledge of blue team, red team, and analysis of computer network defense policies and configurations.

Functional Responsibility: Develops plans for the penetration testing engagements, advises alternative approaches, and oversees penetration testing and technician activities.

Minimum Education: Masters Degree in Computer Science or Management Information Systems. Also acceptable is a technical Bachelor's Degree (Computer Science, Engineering, or Management Information Systems) with fifteen (15) years of technical experience, a recognized certifications such as CEH, CISSP, CISA, CISM or other with fifteen (15) years’ experience, or a non-technical degree with seventeen (17) years of technical experience or no degree with nineteen (19) years of experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

Job Title: Penetration Testing SME III

Minimum/General Experience: Eleven (11) years of technical experience in penetration testing and technician techniques for penetration testing. Demonstrated experience in all phases of penetration testing techniques, concepts and methods; also requires extensive knowledge of blue team, red team, and analysis of computer network defense policies and configurations.

Functional Responsibility: Develops and executes plans for penetration testing engagements, advises alternative approaches, and oversees penetration testing and technician activities.

Minimum Education: Bachelor's Degree in Computer Science, Management Information Systems or related discipline. Also acceptable is a technical Masters Degree with nine (9) years of experience or Technical Degree with eleven (11) years of technical experience, a recognized certification such as CEH, CISSP, CISA, CISM or other with eleven (11) years’ experience, or a non-technical Bachelor's degree with thirteen (13) years of technical experience or no degree with fifteen (15) years of experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

Job Title: Penetration Testing SME II

Minimum/General Experience: Eight (8) years of technical experience, in most phases of
penetration testing and technician techniques for penetration testing. Demonstrated experience in developing and conducting penetration testing techniques, concepts and methods; also requires extensive knowledge of blue team, red team, and analysis of computer network defense policies and configurations.

**Functional Responsibility:** Contributes to the development and execution of plans for penetration testing engagements, advises alternative approaches, and oversees penetration testing and technician activities.

**Minimum Education:** Bachelor’s Degree in Computer Science, Management Information Systems, or related discipline. Also acceptable is a Masters Degree with six (6) years of technical experience or Technical Degree with eight (8) years of technical experience, a recognized certification such as CEH, CISSP, CISA, CISM or other with eight (8) years of experience, or a non-technical degree with ten (10) years of technical experience or no degree with twelve (12) years of technical experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** Penetration Testing SME I

**Minimum/General Experience:** Five (5) years of technical experience in some phases of security, system design and integration, development, and network management. Some experience in developing and conducting penetration testing techniques, concepts and methods; also requires extensive knowledge of blue team, red team, and analysis of computer network defense policies and configuration.

**Functional Responsibility:** Executes plans for penetration testing engagements, advises alternative approaches, and oversees penetration testing and technician activities. Contribute recommendations for system exposures and weaknesses based on the evidential information gathering.

**Minimum Education:** Bachelor’s Degree in Computer Science, Management Information Systems, or related discipline. Also acceptable is an Masters Degree with three (3) years technical experience or other Technical Degree with five (5) years of technical experience, a recognized certification such as CEH, CISSP, CISA, CISM or other with five (5) years’ experience, or a non-technical degree with seven (7) years of technical experience or no degree with nine (9) years of technical experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** Penetration Testing and Technician Task Manager

**Minimum/General Experience:** Thirteen (13) years of technical experience which applies to penetration testing and technician techniques for penetration testing. Requires competence in all phases of penetration testing techniques, concepts and methods; also requires knowledge of blue team, red team, and analysis of computer network defense policies and configurations.

**Functional Responsibility:** Guides teams through penetration testing engagements, advises alternative approaches, and conducts penetration testing and technician activities.

**Minimum Education:** Bachelor’s Degree in Computer Science or Management Information Systems. Also acceptable is a Masters Degree with eleven (11) years of technical experience, a recognized certification such as CEH, CISSP, CISA, CISM or other with thirteen (13) years’ experience, or a non-technical degree with fifteen (15) years of technical experience or no degree with seventeen (17) years of experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.
Job Title: Penetration Testing and Technician Principal

Minimum/General Experience: Eleven (11) years of technical experience which applies to penetration testing and technician techniques for penetration testing. Requires competence in most phases of penetration testing techniques, concepts and methods; also requires knowledge of blue team, red team, and analysis of computer network defense policies and configurations.

Functional Responsibility: Active member of and guides teams through penetration testing engagements, advises alternative approaches, and conducts penetration testing and technician activities.

Minimum Education: Bachelor's Degree in Computer Science or Management Information Systems. Also acceptable is a technical Masters Degree with nine (9) years of experience or an Engineering Degree or other Technical Degree with eleven (11) years of technical experience, a recognized certification such as CEH, CISSP, CISA, CISM or other with eleven (11) years’ experience, or a non-technical Bachelor’s degree with thirteen (13) years of technical experience or no degree with fifteen (15) years of experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

Job Title: Penetration Testing and Technician Senior Analyst

Minimum/General Experience: Eight (8) years of technical experience, which applies to penetration testing and technician techniques for penetration testing. Requires competence in many phases of penetration testing techniques, concepts and methods; also requires knowledge of blue team, red team, and analysis of computer network defense policies and configurations.

Functional Responsibility: Works on penetration testing engagements, advises alternative approaches, and conducts penetration testing and technician activities.

Minimum Education: Bachelor’s Degree in Computer Science or Management Information Systems. Also acceptable is a Masters Degree with six (6) years of technical experience or Engineering Degree or other Technical Degree with eight (8) years of technical experience, a recognized certification such as CEH, CISSP, CISA, CISM or other with (6) six years’ experience, or a non-technical degree with ten (10) years of technical experience or no degree with twelve (12) years of technical experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

Job Title: Penetration Testing and Technician Analyst

Minimum/General Experience: Six (6) years of technical experience which applies to penetration testing and technician techniques for penetration testing. Requires competence in many phases of penetration testing techniques, concepts and methods; also requires some knowledge of blue team, red team, and analysis of computer network defense policies and configurations.

Functional Responsibility: Works on penetration testing engagements, advises alternative approaches, and conducts penetration testing and technician activities.

Minimum Education: Bachelor’s Degree in Computer Science or Management Information Systems. Also acceptable is a Masters Degree with four (4) years technical experience or an Engineering Degree or other Technical Degree with six (6) years of technical experience, a recognized certification such as CEH, CISSP, CISA, CISM or other with six (6) years’ experience, or a non-technical degree with eight (8) years of technical
experience or no degree with ten (10) years of technical experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** Penetration Testing and Technician Junior Analyst

**Minimum/General Experience:** Four (4) years of technical experience which applies to penetration testing and technician techniques for penetration testing. Requires competence in some phases of penetration testing techniques, concepts and methods; also requires some knowledge of blue team, red team, and analysis of computer network defense policies and configurations.

**Functional Responsibility:** Works with senior team members to help on penetration testing engagements, advises alternative approaches, and conducts penetration testing and technician activities.

**Minimum Education:** Bachelor’s Degree in Computer Science or Management Information Systems or a recognized certification such as CEH, CISSP, CISA, CISM or other with four (4) years’ experience. Also acceptable is a Masters Degree with two (2) years of technical experience or a non-technical Degree with six (6) years of technical experience or no degree with eight (8) years of experience. A may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** Penetration Testing and Technician Staff Analyst

**Minimum/General Experience:** Two (2) years of technical experience which applies to penetration testing and technician techniques for penetration testing. Requires competence in some phases of penetration testing techniques, concepts and methods; also requires some knowledge of blue team, red team, and analysis of computer network defense policies and configurations.

**Functional Responsibility:** Works with senior team members to help on penetration testing engagements, advises alternative approaches, and conducts penetration testing and technician activities.

**Minimum Education:** Bachelor’s Degree in Computer Science or Management Information Systems or a recognized certification such as CEH, CISSP, CISA, CISM or other with two (2) years’ experience. Also acceptable is a Masters Degree with zero (0) years technical experience or a non-technical Degree with four (4) years of technical experience or no degree with six (6) years of technical experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** Penetration Testing and Technician Support

**Minimum/General Experience:** Zero (0) years of technical experience but has college course which applies to penetration testing and technician techniques for penetration testing. Classes in some phases of penetration testing techniques, concepts and methods.

**Functional Responsibility:** Works with senior team members to help on penetration testing engagements, advises alternative approaches, and conducts penetration testing and technician activities.

**Minimum Education:** Bachelor’s Degree in Computer Science or Management Information Systems or a recognized certification such as CEH, Security+ or other. Also acceptable is a non-technical Degree with two (2) years of work experience or no degree with four (4) years of work experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.
Job Title: Penetration Testing and Technician Technical Writer Support

Minimum/General Experience: Zero (0) years of technical experience but has administrative support experience which applies to penetration testing and technician techniques for penetration testing. Has some experience in working with word processing applications, and spreadsheet applications.

Functional Responsibility: Works with team members to assist in document preparation, deliverable preparation, and other necessary administrative support.

Minimum Education: Non-technical undergraduate degree. Also acceptable is no degree with two (2) years of administrative support experience.

54151HACS Incident Response

Description of services offered under all FPDS Codes for 54151HACS Incident Response (IR) include but are not limited to:

1. Collect intrusion artifacts (e.g., source code, malware, and Trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise.
2. Perform command and control functions in response to incidents.
3. Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.

Job Title: Incident Response SME IV

Minimum/General Experience: Thirteen (13) years of technical experience in incident response. Demonstrated experience in helping organizations impacted by a Cybersecurity compromise determine the extent of the incident, remove the adversary from their systems, and restore their networks to a more secure state. Extensive experience in malware, Trojans, and current vulnerabilities used to exploit computer network defenses.

Functional Responsibility: Develops plans for the incident response policies, procedures, and processes to identify root cause of incidents, work to remove the incident remnants from the system and assist in restoring the network to a more secure state.

Minimum Education: Masters Degree in Computer Science or Management Information Systems. Also acceptable is a technical Bachelor’s Degree (Computer Science, Engineering, or Management Information Systems) with fifteen (15) years of technical experience, a recognized certifications such as CEH, CISSP, CISA, CISM or other with fifteen (15) years’ experience, or a non-technical degree with seventeen (17) years of technical experience or no degree with nineteen (19) years of experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

Job Title: Incident Response SME III

Minimum/General Experience: Eleven (11) years of technical experience in incident response. Demonstrated experience in helping organizations impacted by a Cybersecurity compromise determine the extent of the incident, remove the adversary from their systems, and restore their networks to a more secure state. Extensive experience in malware, Trojans, and current vulnerabilities used to exploit computer network defenses.

Functional Responsibility: Develops and executes plans for the incident response policies, procedures, and processes to identify root cause of incidents, work to remove the
incident remnants from the system and assist in restoring the network to a more secure state.

**Minimum Education:** Bachelor’s Degree in Computer Science, Management Information Systems or related discipline. Also acceptable is a technical Masters Degree with nine (9) years of experience or Technical Degree with eleven (11) years of technical experience, a recognized certification such as CEH, CISSP, CISA, CISM or other with eleven (11) years’ experience, or a non-technical Bachelor’s degree with thirteen (13) years of technical experience or no degree with fifteen (15) years of experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** Incident Response SME II

**Minimum/General Experience:** Eight (8) years of technical experience, in most phases of incident response. Demonstrated experience in helping organizations impacted by a Cybersecurity compromise determine the extent of the incident, remove the adversary from their systems, and restore their networks to a more secure state. Experience in malware, Trojans, and current vulnerabilities used to exploit computer network defenses.

**Functional Responsibility:** Contributes to the development and execution of plans for the incident response policies, procedures, and processes to identify root cause of incidents, work to remove the incident remnants from the system and assist in restoring the network to a more secure state.

**Minimum Education:** Bachelor’s Degree in Computer Science, Management Information Systems, or related discipline. Also acceptable is a Masters Degree with six (6) years of technical experience or Technical Degree with eight (8) years of technical experience, a recognized certification such as CEH, CISSP, CISA, CISM or other with eight (8) years of experience, or a non-technical degree with ten (10) years of technical experience or no degree with twelve (12) years of technical experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** Incident Response Testing SME I

**Minimum/General Experience:** Five (5) years of technical experience in some phases of incident response. Some experience in helping organizations impacted by a Cybersecurity compromise determine the extent of the incident, remove the adversary from their systems, and restore their networks to a more secure state. Some experience in malware, Trojans, and current vulnerabilities used to exploit computer network defenses.

**Functional Responsibility:** Executes plans for the incident response policies, procedures, and processes to identify root cause of incidents, work to remove the incident remnants from the system and assist in restoring the network to a more secure state.

**Minimum Education:** Bachelor’s Degree in Computer Science, Management Information Systems, or related discipline. Also acceptable is an Masters Degree with three (3) years technical experience or other Technical Degree with five (5) years of technical experience, a recognized certification such as CEH, CISSP, CISA, CISM or other with five (5) years’ experience, or a non-technical degree with seven (7) years of technical experience or no degree with nine (9) years of technical experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** Incident Response Task Manager

**Minimum/General Experience:** Thirteen (13) years of technical experience in aspects of incident response. Competence in helping organizations impacted by a Cybersecurity
compromise determine the extent of the incident, remove the adversary from their systems, and restore their networks to a more secure state. Extensive experience in collecting intrusion artifacts, responding to incidents, and correlating incident data to vulnerabilities. Knowledge of malware, Trojans, and current vulnerabilities used to exploit computer network defenses.

**Functional Responsibility**: Guides team in identifying root cause of incidents, working to remove the incident remnants from the system and assisting in restoring the network to a more secure state.

**Minimum Education**: Masters Degree in Computer Science or Management Information Systems. Also acceptable is a technical Bachelor’s Degree (Computer Science, Engineering, or Management Information Systems) with thirteen (13) years of technical experience, a recognized certification such as CEH, CISSP, CISA, CISM or other with thirteen (13) years’ experience, or a non-technical degree with fifteen (15) years of technical experience or no degree with seventeen (17) years of experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title**: Incident Response Principal

**Minimum/General Experience**: Eleven (11) years of technical experience in aspects of incident response. Competence in most phases of helping organizations impacted by a Cybersecurity compromise determine the extent of the incident, remove the adversary from their systems, and restore their networks to a more secure state. Comprehensive experience in collecting intrusion artifacts, responding to incidents, and correlating incident data to vulnerabilities. Knowledge of malware, Trojans, and current vulnerabilities used to exploit computer network defenses.

**Functional Responsibility**: Guides team in identifying root cause of incidents, working to remove the incident remnants from the system and assisting in restoring the network to a more secure state.

**Minimum Education**: Bachelor’s Degree in Computer Science or Management Information Systems. Also acceptable is a technical Masters Degree with nine (9) years of experience or an Engineering Degree or other Technical Degree with eleven (11) years of technical experience, a recognized certification such as CEH, CISSP, CISA, CISM or other with eleven (11) years’ experience, or a non-technical Bachelor’s degree with thirteen (13) years of technical experience or no degree with fifteen (15) years of experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title**: Incident Response Senior Analyst

**Minimum/General Experience**: Eight (8) years of technical experience, in aspects of incident response. Competence in most phases of helping organizations impacted by a Cybersecurity compromise determine the extent of the incident, remove the adversary from their systems, and restore their networks to a more secure state. Experience in collecting intrusion artifacts, responding to incidents, and correlating incident data to vulnerabilities. Knowledge of malware, Trojans, and current vulnerabilities used to exploit computer network defenses.

**Functional Responsibility**: Works with team in identifying root cause of incidents, working to remove the incident remnants from the system and assisting in restoring the network to a more secure state.

**Minimum Education**: Bachelor’s Degree in Computer Science or Management
Information Systems. Also acceptable is a Masters Degree with six (6) years of technical experience or Engineering Degree or other Technical Degree with eight (8) years of technical experience, a recognized certification such as CEH, CISSP, CISA, CISM or other with eight (8) years’ experience, or a non-technical degree with ten (10) years of technical experience or no degree with twelve (12) years of technical experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** Incident Response Analyst

**Minimum/General Experience:** Six (6) years of technical experience in aspects of incident response. Competence in some phases of helping organizations impacted by a Cybersecurity compromise determine the extent of the incident, remove the adversary from their systems, and restore their networks to a more secure state. Some experience in collecting intrusion artifacts, responding to incidents, and correlating incident data to vulnerabilities. Knowledge of malware, Trojans, and vulnerabilities used to exploit computer network defenses.

**Functional Responsibility:** Works with team in identifying root cause of incidents, working to remove the incident remnants from the system and assisting in restoring the network to a more secure state.

**Minimum Education:** Bachelor’s Degree in Computer Science or Management Information Systems. Also acceptable is a Masters Degree with four (4) years technical experience or an Engineering Degree or other Technical Degree with six (6) years of technical experience, a recognized certification such as CEH, CISSP, CISA, CISM or other with six (6) years’ experience, or a non-technical degree with eight (8) years of technical experience or no degree with ten (10) years of technical experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** Incident Response Junior Analyst

**Minimum/General Experience:** Four (4) years of technical experience in aspects of incident response. Competence in some phases of helping organizations impacted by a Cybersecurity compromise determine the extent of the incident and restore their networks to a more secure state. Knowledge of malware and Trojans.

**Functional Responsibility:** Works with senior team members to identify root cause of incidents, remove the incident remnants from the system and assist in restoring the network to a more secure state.

**Minimum Education:** Bachelor’s Degree in Computer Science or Management Information Systems or a recognized certification such as CEH, CISSP, CISA, CISM or other with four (4) years’ experience. Also acceptable is a Masters Degree with two (2) years of technical experience or a non-technical Degree with six (6) years of technical experience or no degree with eight (8) years of experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** Incident Response Staff Analyst

**Minimum/General Experience:** Two (2) years of technical experience in aspects of incident response. Competence in some phases helping organizations impacted by a Cybersecurity compromise determine the extent of the incident and restore their networks to a more secure state. Knowledge of malware and Trojans.

**Functional Responsibility:** Works with senior team members to identify root cause of incidents, remove the incident remnants from the system and assist in restoring the
network to a more secure state.

**Minimum Education:** Bachelor’s Degree in Computer Science or Management Information Systems or a recognized certification such as CEH, CISSP, CISA, CISM or other with two (2) years’ experience. Also acceptable is a Masters Degree with zero (0) years technical experience or a non-technical Degree with four (4) years of technical experience or no degree with six (6) years of technical experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** Incident Response Support

**Minimum/General Experience:** No technical experience required, but has completed college level courses in aspects incident response. Classes in some phases of helping organizations impacted by a Cybersecurity compromise determine the extent of the incident and restore their networks to a more secure state.

**Functional Responsibility:** Works with senior team members to identify root cause of incidents, remove the incident remnants from the system and assist in restoring the network to a more secure state.

**Minimum Education:** Bachelor’s Degree in Computer Science or Management Information Systems or a recognized certification such as CEH, CISSP, CISA, CISM or other. Also acceptable is a non-technical Degree with two (2) years of work experience or no degree with four (4) years of work experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** Incident Response Technical Writer Support

**Minimum/General Experience:** No technical experience required. Possesses administrative support experience that applies to support efforts for incident response. Has some experience in working with word processing applications, and spreadsheet applications.

**Functional Responsibility:** Works with team members to assist in document preparation, deliverable preparation, and other necessary administrative support.

**Minimum Education:** Non-technical undergraduate degree. Also acceptable is no degree with two (2) years of administrative support experience.

54151HACS Risk and Vulnerability Assessment

**Description of services offered under all FPDS Codes for 54151HACS Risk and Vulnerability Assessment (RVA) include but are not limited to:**

1. Network Mapping - consists of identifying assets on an agreed upon IP address space or network range(s).
2. Vulnerability Scanning - comprehensively identifies IT vulnerabilities associated with agency systems that are potentially exploitable by attackers.
3. Phishing Assessment - includes activities to evaluate the level of awareness of the agency workforce with regard to digital form of social engineering that uses authentic looking, but bogus, emails request information from users or direct them to a fake Website that requests information. Phishing assessments can include scanning, testing, or both and can be conducted as a one-time event or as part of a larger campaign to be conducted over several months.
4. Wireless Assessment - includes wireless access point (WAP) detection, penetration testing or both and is performed while onsite at a customer’s facility.
5. **Web Application Assessment** - includes scanning, testing or both of outward facing web applications for defects in Web service implementation may lead to exploitable vulnerabilities. Provide report on how to implement Web services securely and that traditional network security tools and techniques are used to limit access to the Web Service to only those networks and systems that should have legitimate access.

6. **Operating System Security Assessment (OSSA)** - assesses the configuration of select host operating systems (OS) against standardized configuration baselines.

7. **Database Assessment** - assesses the configuration of selected databases against configuration baselines in order to identify potential misconfigurations and/or database vulnerabilities.

8. **SIN 132-45A Penetration Testing** - conducting and/or supporting authorized Penetration Testing on enterprise network assets.

**Job Title:** Risk and Vulnerability Assessment (RVA) SME IV

**Minimum/General Experience:** Thirteen (13) years of technical experience in risk and vulnerability assessments, audits and/or compliance. Demonstrated experience in risk assessments, vulnerability assessments, IT audit and/or compliance. Extensive experience required in network mapping, vulnerability scanning, phishing, wireless assessments, web application assessments, operating system assessments or database assessments.

**Functional Responsibility:** Develops plans for the RVA policies, procedures, and processes to assess, identify vulnerabilities, and recommend mitigation or countermeasure efforts.

**Minimum Education:** Masters Degree in Computer Science or Management Information Systems. Also acceptable is a technical Bachelor's Degree (Computer Science, Engineering, or Management Information Systems) with fifteen (15) years of technical experience, a recognized certifications such as CEH, CISSP, CISA, CISM or other with fifteen (15) years' experience, or a non-technical degree with seventeen (17) years of technical experience or no degree with nineteen (19) years of experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** SVA SME III

**Minimum/General Experience:** Eleven (11) years of technical experience in risk and vulnerability assessments, audits and/or compliance. Demonstrated experience in risk assessments, vulnerability assessments, IT audit and/or compliance. Extensive experience required in network mapping, vulnerability scanning, phishing, wireless assessments, web application assessments, operating system assessments or database assessments.

**Functional Responsibility:** Develops and executes plans for RVA policies, procedures, and processes to assess, identify vulnerabilities, and recommend mitigation or countermeasure efforts.

**Minimum Education:** Bachelor's Degree in Computer Science, Management Information Systems or related discipline. Also acceptable is a technical Masters Degree with nine (9) years of experience or Technical Degree with eleven (11) years of technical experience, a recognized certification such as CEH, CISSP, CISA, CISM or other with eleven (11) years' experience, or a non-technical Bachelor's degree with thirteen (13) years of technical experience or no degree with fifteen (15) years of experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** RVA SME II
**Minimum/General Experience**: Eight (8) years of technical experience, in most phases of risk and vulnerability assessments, audits and/or compliance. Demonstrated experience in risk assessments, vulnerability assessments, IT audit and/or compliance. Experience in network mapping, vulnerability scanning, phishing, wireless assessments, web application assessments, operating system assessments or database assessments.

**Functional Responsibility**: Contributes to the development and execution of plans for RVA policies, procedures, and processes to assess, identify vulnerabilities, and recommend mitigation or countermeasure efforts.

**Minimum Education**: Bachelor’s Degree in Computer Science, Management Information Systems, or related discipline. Also acceptable is a Masters Degree with six (6) years of technical experience or Technical Degree with eight (8) years of technical experience, a recognized certification such as CEH, CISSP, CISA, CISM or other with eight (8) years of experience, or a non-technical degree with ten (10) years of technical experience or no degree with twelve (12) years of technical experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title**: RVA SME I

**Minimum/General Experience**: Five (5) years of technical experience in some phases of risk and vulnerability assessments, audits and/or compliance. Some experience in risk assessments, vulnerability assessments, IT audit and/or compliance. Some experience in network mapping, vulnerability scanning, phishing, wireless assessments, web application assessments, operating system assessments or database assessments.

**Functional Responsibility**: Executes plans for RVA policies, procedures, and processes to assess, identify vulnerabilities, and recommend mitigation or countermeasure efforts.

**Minimum Education**: Bachelor’s Degree in Computer Science, Management Information Systems, or related discipline. Also acceptable is an Masters Degree with three (3) years technical experience or Technical Degree with five (5) years of technical experience, a recognized certification such as CEH, CISSP, CISA, CISM or other with five (5) years’ experience, or a non-technical degree with seven (7) years of technical experience or no degree with nine (9) years of technical experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title**: RVA Task Manager

**Minimum/General Experience**: Thirteen (13) years of technical experience which applies to risk and vulnerability assessments, audits and/or compliance. Requires competence in all phases of risk assessments, vulnerability assessments, IT audit and/or compliance. Extensive experience required in network mapping, vulnerability scanning, phishing, wireless assessments, web application assessments, operating system assessments or database assessments.

**Functional Responsibility**: Guides team in conducting risk and vulnerability assessments, identifying vulnerabilities and making recommendations for mitigation or countermeasure.

**Minimum Education**: Bachelor’s Degree in Computer Science or Management Information Systems. Also acceptable is a technical Bachelor's Degree (Computer Science, Engineering, or Management Information Systems) with thirteen (13) years of technical experience, a recognized certification such as CEH, CISSP, CISA, CISM or other with thirteen (13) years’ experience, or a non-technical degree with fifteen (15) years of experience.
technical experience or no degree with seventeen (17) years of experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** RVA Principal

**Minimum/General Experience:** Eleven (11) years of technical experience which applies to risk and vulnerability assessments, audits and/or compliance. Requires competence in phases of risk assessments, vulnerability assessments, IT audit and/or compliance. Extensive experience required in network mapping, vulnerability scanning, phishing, wireless assessments, web application assessments, operating system assessments or database assessments.

**Functional Responsibility:** Guides team in conducting risk and vulnerability assessments, identifying vulnerabilities and making recommendations for mitigation or countermeasure.

**Minimum Education:** Bachelor’s Degree in Computer Science or Management Information Systems. Also acceptable is a technical Masters Degree with nine (9) years of experience or an Engineering Degree or other Technical Degree with eleven (11) years of technical experience, a recognized certification such as CEH, CISSP, CISA, CISM or other with eleven (11) years’ experience, or a non-technical Bachelor’s degree with thirteen (13) years of technical experience or no degree with fifteen (15) years of experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** RVA Senior Analyst

**Minimum/General Experience:** Eight (8) years of technical experience, which applies to risk and vulnerability assessments, audits and/or compliance. Requires competence in some phases of risk assessments, vulnerability assessments, IT audit and/or compliance. Some experience required in network mapping, vulnerability scanning, phishing, wireless assessments, web application assessments, operating system assessments or database assessments.

**Functional Responsibility:** Work with senior team members in conducting risk and vulnerability assessments, identifying vulnerabilities and making recommendations for mitigation or countermeasure.

**Minimum Education:** Bachelor's Degree in Computer Science or Management Information Systems. Also acceptable is a Masters Degree with six (6) years of technical experience or Engineering Degree or other Technical Degree with eight (8) years of technical experience, a recognized certification such as CEH, CISSP, CISA, CISM or other with eight (8) years’ experience, or a non-technical degree with ten (10) years of technical experience or no degree with twelve (12) years of technical experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** RVA Analyst

**Minimum/General Experience:** Six (6) years of technical experience which applies to risk and vulnerability assessments, audits and/or compliance. Requires competence in some phases of risk assessments, vulnerability assessments, IT audit and/or compliance. Some experience in network mapping, vulnerability scanning, phishing, wireless assessments, web application assessments, operating system assessments or database assessments.

**Functional Responsibility:** Works with senior team members in conducting risk and
vulnerability assessments, identifying vulnerabilities and making recommendations for mitigation or countermeasure.

**Minimum Education:** Bachelor’s Degree in Computer Science or Management Information Systems. Also acceptable is an Masters Degree with four (4) years technical experience or an Engineering Degree or other Technical Degree with six (6) years of technical experience, a recognized certification such as CEH, CISSP, CISA, CISM or other with six (6) years’ experience, or a non-technical degree with eight (8) years of technical experience or no degree with ten (10) years of technical experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** RVA Junior Analyst

**Minimum/General Experience:** Four (4) years of technical experience which applies to risk and vulnerability assessments, audits and/or compliance. Experience required in network mapping, vulnerability scanning, phishing, wireless assessments, web application assessments, operating system assessments or database assessments.

**Functional Responsibility:** Works with senior team members in conducting risk and vulnerability assessments, identifying vulnerabilities and making recommendations for mitigation or countermeasure.

**Minimum Education:** Bachelor’s Degree in Computer Science or Management Information Systems or a recognized certification such as CEH, CISSP, CISA, CISM or other with four (4) years of experience. Also acceptable is a Masters Degree with two (2) years of technical experience or a non-technical Degree with six (6) years of technical experience or no degree with eight (8) years of technical experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** RVA Staff Analyst

**Minimum/General Experience:** Two (2) years of technical experience which applies to risk and vulnerability assessments, audits and/or compliance. Some experience required in network mapping, vulnerability scanning, phishing, wireless assessments, web application assessments, operating system assessments or database assessments.

**Functional Responsibility:** Works with senior team members in conducting risk and vulnerability assessments, identifying vulnerabilities and making recommendations for mitigation or countermeasure.

**Minimum Education:** Bachelor’s Degree in Computer Science or Management Information Systems or a recognized certification such as CEH, CISSP, CISA, CISM or other with two (2) years of technical experience or a non-technical Degree with zero (0) years technical experience or no degree with four (4) years of technical experience or no degree with six (6) years of technical experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

**Job Title:** RVA Support

**Minimum/General Experience:** No technical experience required, but has completed college level courses which apply to risk and vulnerability assessments, audits and/or compliance. Requires familiarity with network mapping, vulnerability scanning, phishing, wireless assessments, web application assessments, operating system assessments or database assessments.

**Functional Responsibility:** Works with senior team members.
Minimum Education: Bachelor’s Degree in Computer Science or Management Information Systems or a recognized certification such as CEH, CISSP, CISA, CISM or other. Also acceptable is a non-technical Degree with two (2) years of work experience or no degree with four (4) years of work experience. A certification may substitute for 3 general years of experience and 3 technical years of experience.

Job Title: RVA Technical Writer Support

Minimum/General Experience: No technical experience required. Must possess administrative support experience that applies to risk and vulnerability assessments, audits and/or compliance. Has some experience in working with word processing applications, and spreadsheet applications.

Functional Responsibility: Works with team members to assist in document preparation, deliverable preparation, and other necessary administrative support.

Minimum Education: Non-technical undergraduate degree. Also acceptable is no degree with two (2) years of administrative support experience.