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

SPECIAL ITEM NUMBER: 132-51 INFORMATION TECHNOLOGY PROFESSIONAL SERVICES

132-51 - Information Technology Professional Services - SUBJECT TO COOPERATIVE PURCHASING Includes resources and facilities management, database planning and design, systems analysis and design, network services, programming, millennium conversion services, conversion and implementation support, network services project management, data/records management, subscriptions/publications (electronic media), and other services.

FPDS Code D302	IT Systems Development Services
FPDS Code D306	IT Systems Analysis Services
FPDS Code D307	Automated Information Systems Design and Integration Services
FPDS Code D308	Programming Services
FPDS Code D310	IT Backup and Security Services
FPDS Code D311	IT Data Conversion Services
FPDS Code D316	IT Network Management Services
FPDS Code D317	Automated News Services, Data Services, or Other Information Services
FPDS Code D399	Other Information Technology Services, Not Elsewhere Classified

SIN 132-45A – Penetration Testing

SIN 132-45B – Incident Response

SIN 132-45C – Cyber Hunt

SIN 132-45D – Risk and Vulnerability Assessment

Amyx, Inc.
1768 Business Center Drive, Ste. 300
Reston, VA 20190
Telephone: 703-373-1984
Fax: 571-612-4365
Web site address: www.amyx.com
DUNS Number: 136794802; Cage Code: 1QNC9

Contract Number: **GS-35F-0481L**
Period Covered by Contract: **June 28, 2016 through June 27, 2021**

General Services Administration
Federal Supply Service

Pricelist current through A518 – Schedule 70 - Refresh 37.

Products and ordering information in this Authorized FSS Information Technology Schedule Pricelist are also on the GSA Advantage! System.
Agencies can browse GSA Advantage! By accessing the Federal Supply Service's Home Page via the Internet at http://www.fss.gsa.gov/

Contents

SECTION 1:
INFORMATION FOR ORDERING OFFICES

SPECIAL NOTICE TO AGENCIES:

SMALL BUSINESS PARTICIPATION

SBA strongly supports the participation of small business concerns in the Federal Supply Schedules Program. To enhance Small Business Participation, SBA policy allows agencies to include in their procurement base and goals, the dollar value of orders expected to be placed against the Federal Supply Schedules, and to report accomplishments against these goals.

For orders exceeding the micro purchase threshold, FAR 8.404 requires agencies to consider the catalogs/pricelist of at least three Schedule Contractors or consider reasonably available information by using GSA Advantage!™ on-line shopping service (www.fss.gsa.gov). The catalogs/pricelists, GSA Advantage!™ and the Federal Supply Service Home Page (www.fss.gsa.gov) contain information on a broad array of products and services offered by small business concerns.

This information should be used as tool to assist ordering activities in meeting or exceeding established small business goals. It should also be used as a tool to assist in including small, disadvantaged, and women-owned small businesses among those considered when selecting pricelist for best value determination.

For orders exceeding the micro purchase threshold, customers are to give preference to small business concerns when two or more items at the same delivered price will satisfy the requirement.

1. Geographic Scope of Contract:

The geographic scope of this contract will be domestic and overseas delivery..

2. Contractor's Ordering Address and Payment Information:

(a) Contractor's Ordering/Payment address:

Amyx, Inc.
1768 Business Center Drive, Ste.
300 Reston, VA 20190
Telephone: 703-373-1984
Fax: 571-612-4365
Attn: Contracts Department

(b) Credit Card Orders

Contractors are required to accept the Government purchase card for payments equal to or less than the micro-purchase threshold for oral or written delivery orders. Government purchase cards will be acceptable for payment above the micro-purchase threshold. In addition, bank account information for wire transfer payments will be shown on the invoice.

(c) Technical Ordering Assistance

The following telephone number can used by ordering activity centers to obtain technical and/or ordering assistance: (703) 373-1436.

3. LIABILITY FOR INJURY OR DAMAGE

The Contractor shall not be liable for any injury to Government personnel or damage to Government property arising from the use of equipment maintained by the Contractor, unless such injury or damage is due to the fault or negligence of the Contractor.

4. STATISTICAL DATA FOR GOVERNMENT ORDERING OFFICE COMPLETION OF STANDARD FORM 279:

Block 9: G. Order/Modification Under Federal Schedule

Block 16: Data Universal Numbering System (DUNS) Number: 136794802

Block 30: Type of Contractor – B

Block 31: Woman-Owned Small Business - No

Block 36: Contractor's Taxpayer Identification Number (TIN): 54-1979772

4.1 CAGE Code: 1QNC9

4.2 Contractor has registered with the Central Contractor Registration Database/Systems for Award Management/SAM.

5. FOB: DESTINATION

6. DELIVERY SCHEDULE

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

SPECIAL ITEM NUMBER	DELIVERY TIME (Days ARO)
132-51A-D, 132-51	As mutually agreed upon per order.

b. URGENT REQUIREMENTS: When the Federal Supply Schedule contract delivery period does not meet the bona fide urgent delivery requirements of an ordering agency, agencies are encouraged, if time permits, to contact the Contractor for the purpose of obtaining accelerated delivery. The Contractor shall reply to the inquiry within 3 workdays after receipt. (Telephonic replies shall be confirmed by the Contractor in writing.) If the Contractor offers an accelerated delivery time acceptable to the ordering agency, any order(s) placed pursuant to the agreed upon accelerated delivery time frame shall be delivered within this shorter delivery time and in accordance with all other terms and conditions of the contract.

7. DISCOUNTS: Prices shown are NET Prices; Basic Discounts have been deducted.

(a)	Prompt Payment	None
(b)	Quantity	None
(c)	Dollar Value	None
(d)	Government Educational Institutions	None
(e)	Other	None

8. **TRADE AGREEMENTS ACT OF 1979, AS AMENDED:**
All items are U.S. made end products, designated country end products, Caribbean Basin country end products, Canadian end products, or Mexican end products as defined in the Trade Agreements Act of 1979, as amended.

9. **STATEMENT CONCERNING AVAILIBILITY OF EXPORT PACKING:**
Not applicable.

10. **SMALL REQUIREMENTS:**
The minimum dollar value of orders to be issued is $100.00

11. **MAXIMUM ORDER $500,000**
The Maximum Order value for the following Special Item Numbers (SINs) is $500,000:

Special Item Number 132-51 - Information Technology (IT) Professional Services

Note: This is not a restriction on the contract value.

12. **USE OF FEDERAL SUPPLY SERVICE INFORMATION TECHNOLOGY SCHEDULE CONTRACTS.**
In accordance with FAR 8.404:
Ordering activities shall use the ordering procedures of FAR 8.404, when placing an order.

13. **FEDERAL INFORMATION TECHNOLOGY/TELECOMMUNICATION STANDARDS REQUIREMENTS:**
Federal departments and agencies acquiring products from this Schedule must comply with the provisions of the Federal Standards Program, as appropriate (reference: NIST Federal Standards Index). Inquiries to determine whether or not specific products listed herein comply with Federal Information Processing Standards (FIPS) or Federal Telecommunication Standards (FED-STDS), which are cited by ordering offices, shall be responded to promptly by the Contractor.

13.1 **FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATIONS (FIPS PUBS):**

Information Technology products under this Schedule that do not conform to Federal Information Processing Standards (FIPS) should not be acquired unless a waiver has been granted in accordance with the applicable "FIPS Publication." Federal Information Processing Standards Publications (FIPS PUBS) are issued by the U.S. Department of Commerce, National Institute of Standards and Technology (NIST), pursuant to National Security Act. Information concerning their availability and applicability should be obtained from the National Technical Information Service (NTIS), 5285 Port Royal Road, Springfield, Virginia 22161. FIPS PUBS include voluntary standards when these are adopted for Federal use. Individual orders for FIPS PUBS should be referred to the NTIS Sales Office, and orders for subscription service should be referred to the NTIS Subscription Officer, both at the above address, or telephone number (703) 487-4650.

13.2 **FEDERAL TELECOMMUNICATION STANDARDS (FED-STDS):**

Telecommunication products under this Schedule that do not conform to Federal Telecommunication Standards (FED-STDS) should not be acquired unless a waiver has been granted in accordance with the applicable "FED-STD." Federal Telecommunication Standards are issued by the U.S. Department of Commerce, National Institute of Standards and Technology (NIST), pursuant to National Security Act. Ordering information and information concerning the availability of FED-STDS should be obtained from the GSA, Federal Supply Service, Specification Section, 470 East L’Enfant Plaza, Suite 8100, SW, Washington, DC 20407, telephone number (202)619-8925. Please include a self-addressed mailing label when requesting information by mail. Information concerning their applicability can be obtained by writing or calling the U.S. Department of Commerce, National Institute of Standards and Technology, Gaithersburg, MD 20899, telephone number (301)975-2833.

14. SECURITY REQUIREMENTS:

In the event security requirements are necessary, the ordering activities may incorporate, in their delivery orders, a security clause in accordance with current laws, regulations, and individual agency policy; however, the burden of administering the security requirements shall be with the ordering agency. If any costs are incurred as a result of the inclusion of security requirements, such costs will not exceed ten percent (10%) or $100,000, of the total dollar value of the order, whichever is less.

15. CONTRACT ADMINISTRATION FOR ORDERING OFFICES:

Any ordering office, with respect to any one or more delivery orders placed by it under this contract, may exercise the same rights of termination as might the GSA Contracting Officer under provisions of FAR 52.212-4, paragraphs (l) Termination for the Government’s convenience, and (m) Termination for Cause (See C.1.)

16. GSA ADVANTAGE!

GSA Advantage! is an on-line, interactive electronic information and ordering system that provides on-line access to vendors' schedule prices with ordering information. GSA Advantage! will allow the user to perform various searches across all contracts including, but not limited to:

(1) Manufacturer;
(2) Manufacturer's Part Number; and
(3) Product categories.

Agencies can browse GSA Advantage! by accessing the Internet World Wide Web utilizing a browser. The Internet address is http://www.fss.gsa.gov/.

17. PURCHASE OF INCIDENTAL, NON-SCHEDULE ITEMS:

For administrative convenience, open market (non-contract) items may be added to a Federal Supply Schedule Blanket Purchase Agreement (BPA) or an individual order, provided that the items are clearly labeled as such on the order, all applicable regulations have been followed, and price reasonableness has been determined by the ordering activity for the open market (non-contract) items.

18. CONTRACTOR COMMITMENTS, WARRANTIES AND REPRESENTATIONS:

a. For the purpose of this contract, commitments, warranties and representations include, in addition to those agreed to for the entire schedule contract:

(1) Time of delivery/installation quotations for individual orders;

(2) Technical representations and/or warranties of products concerning performance, total system performance and/or configuration, physical, design and/or functional characteristics and capabilities of a product/equipment/ service/software package submitted in response to requirements which result in orders under this schedule contract.

(3) Any representations and/or warranties concerning the products made in any literature, description, drawings and/or specifications furnished by the Contractor.

b. The above is not intended to include items not currently covered by the GSA Schedule contract.

19. OVERSEAS ACTIVITIES:

The terms and conditions of this contract shall apply to all orders for installation, maintenance and repair of equipment in areas listed in the pricelist outside the 48 contiguous states and the District of Columbia, except as indicated below:

Not Applicable

Upon request of the Contractor, the Government may provide the Contractor with logistics support, as available, in accordance with all applicable Government regulations. Such Government support will be provided on a reimbursable basis, and will only be provided to the Contractor's technical personnel whose services are exclusively required for the fulfillment of the terms and conditions of this contract.

20. BLANKET PURCHASE AGREEMENTS (BPAs):

Federal Acquisition Regulation (FAR) 13.303-1(a) defines Blanket Purchase Agreements (BPAs) as "…a simplified method of filling anticipated repetitive needs for supplies or services by establishing 'charge accounts' with qualified sources of supply." The use of Blanket Purchase Agreements under the Federal Supply Schedule Program is authorized in accordance with FAR 13.303-2(c)(3), which reads, in part, as follows:

"BPAs may be established with Federal Supply Schedule Contractors, if not inconsistent with the terms of the applicable schedule contract."

21. CONTRACTOR TEAM ARRANGEMENTS:

Contractors participating in contractor team arrangements must abide by all terms and conditions of their respective contracts. This includes compliance with Clauses 552.238-74; Contractor's Reports of Sales and 552.238-76, Industrial Funding Fee, i.e., each contractor (team member) must report sales and remit the IFF for all products and services provided under its individual contract.

SECTION 2:
TERMS AND CONDITIONS APPLICABLE TO INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES (SPECIAL ITEM NUMBER 132-51

1. SCOPE

a. The prices, terms and conditions stated under Special Item Number 132-51 Information Technology Professional Services apply exclusively to IT Services within the scope of this Information Technology Schedule.

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

2. PERFORMANCE INCENTIVES

a. When using a performance based statement of work, performance incentives may be agreed upon between the Contractor and the ordering office on individual fixed price orders or Blanket Purchase Agreements, for fixed price tasks, under this contract in accordance with this clause.

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

c. To the maximum extent practicable, ordering offices shall consider establishing incentives where performance is critical to the agency's mission and incentives are likely to motivate the contractor. Incentives shall be based on objectively measurable tasks.

3. ORDER

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

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

4. PERFORMANCE OF SERVICES

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

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

c. The Agency should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner.

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

5. INSPECTION OF SERVICES

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

6. RESPONSIBILITIES OF THE CONTRACTOR

The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character.

7. RESPONSIBILITIES OF THE GOVERNMENT

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

8. INDEPENDENT CONTRACTOR

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

9. ORGANIZATIONAL CONFLICTS OF INTEREST

a. Definitions.

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

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

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

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

10. INVOICES

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

11. PAYMENTS

For firm-fixed price orders the Government shall pay the Contractor, upon submission of proper invoices or vouchers, the prices stipulated in this contract for service rendered and accepted. Progress payments shall be made only when authorized by the order. For time-and-materials orders, the Payments under Time-and-Materials and Labor-Hour Contracts (Alternate I (APR 1984)) at FAR 52.232-7 applies to time-and-materials orders placed under this contract. For labor-hour orders, the Payment under Time-and-Materials and Labor-Hour Contracts (FEB 1997) (Alternate II (JAN 1986)) at FAR 52.232-7 applies to labor-hour orders placed under this contract.

12. RESUMES

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

13. INCIDENTAL SUPPORT COSTS

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

14. APPROVAL OF SUBCONTRACTS

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

SECTION 3:
DESCRIPTION OF SERVICES AND PRICING SIN 135-51

Amyx, Inc. GSA Labor Category Descriptions:

1. Sr. Information Management Systems Specialist

Experience: Acts independently on the most specialized areas of the program or project. Leads and participates in major system implementations. Applies knowledge of leading edge organizational and behavioral management techniques. Specializes in the areas of: IT Applications and User Experience, Graphical User Interface, Organization Development, Human Behavior and Learning, and other similar methods and tools.

Responsibility: Able to analyze organizations using proven methods and techniques, prepare surveys, interview management level personnel and report out on findings. Evaluates organizational behavior and recommends improvements in User Experience. Designs training programs supporting the deployment of new IT Applications or Systems and participates in delivery and/or monitoring of training effectiveness.

Minimum Education: Minimum of Master’s Degree and 10 years of specialized experience. A PhD is preferred.

2. Sr. Program Manager

Minimum/General Experience: Twenty (20) years of leading teams or projects to include integration of various information technology projects using proven program management techniques and skill sets, such as: measuring performance against cost, schedule and quality; sizing tasks and provides work breakdown structures to the government.

Functional Responsibility: Acts as senior level focal point for projects within the program; this includes consultation on staffing, financial, performance and delivery issues. Ensures the overall quality of the product and monitors against financial profile. Possess significant planning and management experience over multiple projects.

Minimum Education: Bachelor’s Degree in Computer Science, Business, or other related field.

3. Program Manager

Minimum/General Experience: 15 years experience total with a combination of Eight (8) years of general experience and Seven (7) years of specialized experience. Knowledge of systems development life cycle and planning through production phase. Expertise in managing and controlling information technology projects including budgets and resources using automated project management tools; demonstrated capability in managing multiple task contracts and/or subcontracts. General experience includes increasingly complex responsibilities in information technology systems design and/or management levels.

Functional Responsibility: Manages mid-size projects and/or large complex task orders. Provides overall functional or technical lead direction to functional or technical staff. Sizes work effort, defines deliverables and work projects. Participates in technical execution of work.

Coordinates deliverables and communicates with client's technical representatives, contracting officers and government end-users. May also serve as Sr. Technical Expert.

Minimum Education: A Bachelor's Degree in Computer Science, Business or other related area.

4. Sr. Information Technology Architect/Subject Matter Consultant

Minimum/General Experience: 15 years experience total with a combination of Eight (8) years of general experience and Seven (7) years of specialized experience. Working knowledge of system information scope for development of enterprise-wide or large-scale information systems. Experience in the design of architecture to include: hardware, communication, operations, software, and/or security to support the total requirement for current and/or future interfaces and operations. Qualified to lead a staff of analysts and/or engineers if required.

Functional Responsibility: Provides senior level knowledge and/or leadership in all areas of technical implementation. Establishes system information scope for development of enterprise-wide or large-scale information systems. Contributes to design of architecture to include: hardware, communication, operations, software, and/or security to support the total requirement for current and/or future interfaces and operations. Ensures system compatibility with applicable standards and reference models.

Minimum Education: Bachelor's Degree in information systems, engineering, mathematics, computer science or related technical area. Master's Degree may substitute for 2 years of generalized experience.

5. Information Technology Architect/Subject Matter Consultant

Minimum/General Experience: 10 years experience total with a combination of Six (6) years of general experience and Four (4) years of specialized experience. Experience in multiple specialties including: operations/statistical research, enterprise resource planning, electronic commerce, data communications analysis and design, database management systems, systems, network and data security, software testing/quality assurance and end-user instruction. Provides knowledge and/or leadership in all areas of technical implementation. Progressive experience in business analysis or programming.

Functional Responsibility: Assists with system information scope for development of enterprise-wide or large-scale information systems. Contributes to design of architecture to include: hardware, communication, operations, software, and/or security to support the total requirement for current and/or future interfaces and operations

Minimum Education: Bachelor’s Degree in information systems, engineering, mathematics, computer science or related technical area. Master’s Degree may substitute for 2 years of generalized experience.

6. Sr. Functional Analyst

Minimum/General Experience: 15 years experience total with a combination of Eight (8) years of general experience and Seven (7) years of specialized experience. Experience in a variety of business disciplines such as: procurement, human resources, finance, logistics, medical, enterprise resource planning, electronic commerce and electronic data interchange, security, and requirements determination. Applies functional experience to business or technology problems. Qualified to lead a staff of analysts and/or engineers if required.

Functional Responsibility: Provides senior level analysis and leadership to the project in all areas of functional implementation. Provides program and/or technical guidance concerning information technology solutions to complex business and information processing issues.

Minimum Education: Bachelor’s Degree; Masters Degree may substitute for 2 years of general experience.

7. Sr. Logistics Business Process Reengineering (BPR) Consultant

Minimum/General Experience: 15 years experience total with a combination of Eight (8) years of general experience and Seven (7) years of specialized experience. Specialized program and/or technical guidance concerning business process reengineering of major complex information technology systems. Experience in a variety of business disciplines such as: procurement, human resources, finance, logistics, medical, enterprise resource planning, electronic commerce and electronic data interchange, security, and requirements determination. Qualified to lead a staff of analysts and/or engineers if required.

Functional Responsibility: Provides senior level BPR analysis and leadership to the project in all areas of process implementation. Demonstrated knowledge of data flows, standards and process solutions to complex business and information processing issues. Applies functional experience to business or technology problems.

Minimum Education: Bachelor’s Degree; Masters Degree may substitute for 2 years of general experience.

8. Sr. Systems Analyst

Minimum/General Experience: 15 years experience total with a combination of Eight (8) years of general experience and Seven (7) years of specialized experience. Specialized systems experience, which may include data warehousing, enterprise resource planning, graphical user interface, middleware integration, legacy systems and processes. Qualified to lead a staff of analysts, or engineers if required.

Functional Responsibility: Provides senior level IT expertise and leadership to the project in all areas of information systems. Demonstrated knowledge of automated information systems, applications, and relationship to legacy systems and processes.

Minimum Education: Bachelor’s Degree; Masters Degree may substitute for 2 years of general experience.

9. Functional Analyst

Minimum/General Experience: 10 years experience total with a combination of Six (6) years general and Four (4) years of specialized experience. Experience in a variety of business disciplines such as: procurement, human resources, finance, logistics, medical, enterprise resource planning, electronic commerce and electronic data interchange, security, and requirements determination. Qualified to lead a staff of analysts and/or engineers if required.

Functional Responsibility: Provides analysis to the project in all areas of functional implementation. Applies functional experience to business or technology problems. Provides specialized program and/or technical guidance concerning information technology solutions to complex business and information processing issues.

Minimum Education: Bachelor’s Degree.

10. Data Analyst

Minimum/General Experience: 8 years experience total with a combination of Six (6) years general and Two (2) years of specialized experience. Demonstrated experience in database management system design and system analysis, operating systems software and data definition and manipulation languages. Knowledge of legacy and current storage and retrieval methods. General knowledge of data structures, design, views and data dictionaries.

Functional Responsibility: Provides data analysis to the project in all areas of data and database implementation. Increasing responsibilities in DMBS logical and/or physical design and implementation; experience in modeling, analysis, hierarchical or relational databases and data modeling tools and/or methods. Assists functional, logistical and technical staff. Works independently or under only general direction.

Minimum Education: Bachelor’s Degree

11. Sr. Electronic Commerce Systems Engineer

Minimum/General Experience: 10 years experience total with a combination of Six (6) years of general experience and Four (4) years of specialized experience. Knowledge of servers, workstations, and programmable devices such as handhelds. Knowledge of network operations and protocols, EC tools and protocols, configuration management tools and methodologies (such as Tivoli) and ability to design overall network configuration. Experience with networking equipment to include configuration, installation and troubleshooting. Qualified to lead technical staff and users in a consultative role as required.

Functional Responsibility: Provides senior level support and leadership to the project in all areas of systems development and technical implementation. Applies Electronic Commerce (EC) principles and technology to network environment. Able to translate system designs and specifications into functioning and architecturally compliant systems. Ability to plan, design, develops, install, modify and test networks, application programs and/or computer based systems.

Minimum Education: Bachelor’s Degree in engineering discipline or applicable certification.

12. Sr. Electronic Commerce Systems Analyst

Minimum/General Experience: 10 years experience total with a combination of Six (6) years of general experience and Four (4) years of specialized experience. Expertise in information technology disciplines or specific functional area related to information technology including Electronic Commerce (EC) and/or eBusiness related technologies.

Functional Responsibility: Expertise in information technology disciplines or specific functional area related to information technology including Electronic Commerce (EC) and/or eBusiness related technologies.
Minimum Education: Bachelor’s Degree in engineering discipline or applicable certification.

13. Systems Requirements Consultant

Minimum/General Experience: 8 years experience total with a combination of Six (6) years general, Two (2) years specialized. Specialized experience with IT systems and applications, which may include background in any of the following areas: data warehousing, enterprise resource planning, graphical user interface, middleware integration, legacy systems and processes. Experience in requirements determination, functional testing, life cycle development and application of requirements to technology.

Functional Responsibility: Provides IT requirements analysis; works with functional and technical senior staff to ensure system design meets end user requirements. Utilizes software tools to build system/project requirements and tracks accordingly; provides requirement studies, data calls, collects and consolidates requirements for technical team and presents to senior management.

Minimum Education: Bachelor’s Degree; Masters Degree may substitute for 2 years of general experience.

14. Web/Internet Consultant

Experience: Knowledge of web related experience and languages (such as HTML). Understanding of graphic formats used on the World Wide Web; knowledge of advanced techniques using mark-up languages including tables, forms and using word process to web mark up converters to maximize efficiency. Experience with web graphics, implementing image files, animation, icons and other advanced multi-media options for web pages. Uses Internet development tools and designs static and dynamic web pages. Progressive experience in web related technologies and information technology assignments.

Responsibility: Design of web pages, development and placement of content, works with functional and technical staff to incorporate front-end content with back end data and content. Works independently or only under general direction.

Minimum Education: Bachelor’s Degree; 4 years general and 1 year specialized experience.

15. Sr. Technical Advisor

Minimum/General Experience: Requires fifteen (15) years of general experience in information systems, including ten (10) years of specialized experience providing state-of-the art solutions in information systems technology.

Functional Responsibility: Provides expert independent services and leadership in specialized technical areas. Provides expertise on an as needed basis to all task assignments. Identifies, evaluates, and specifies system architecture and high-level design. Provides advice and counsel to project and senior management through broad technical specialization of scientific theory and principals.

Minimum Education: Bachelor’s Degree; Masters Degree may substitute for 2 years of general experience.

16. Business Re-Engineering Expert

Minimum/General Experience: A minimum of six (6) years of Business Process Reengineering experience with three (3) years experience with the last five (5) years in the analysis, design/redesign, development, integration, and implementation of large scale business processes/systems.

Functional Responsibility: Provides expert independent services and leadership in specialized technical areas to agency heads, directors, and senior managers on quality improvement. Design organize, lead, and conduct executive level workshops, benchmarking, and surveys. Facilitate process improvement efforts through custom programming, commercial off the shelf (COTS), or other means. Manage a team of senior consultants and analysts that coordinate the evaluation and redesign of current business technology and resources, and improve process performance.

Minimum Education: Bachelor’s degree; Master’s degree substitutes for two (2) years specialized experience.

17. Sr. Information Engineer

Minimum/General Experience: Requires a minimum of six (6) years experience managing or performing software engineering activities, of which three (3) years must be specialized. Specialized experience includes: Demonstrated experience working with third/fourth generation languages in the design and implementation of systems and using database management systems. General experience includes increasing responsibilities in software engineering activities.

Functional Responsibility: Analyzes and studies complex system requirements. Design software tools and subsystems to support software reuse and domain analysis and manages their implementation. Manages software development and support using formal specifications, data flow diagrams, other accepted design techniques and Computer Aided Software Engineering (CASE) tools. Estimates software development costs and schedule. Reviews existing programs and assists in making refinements, reducing operating time, and improving current techniques. Supervises software configuration management.

Minimum Education: Bachelor’s Degree or Master of Sciences degree in Computer Science, Information Systems, Engineering, Business will be considered equivalent to one year specialized experience and two years general experience.

18. Information Engineer

Minimum/General Experience: Requires a minimum of three (3) years experience as a software engineer; two (2) years experience working with third/fourth generation languages in the design and implementation of systems and one (1) year working with data base management.

Functional Responsibility: Analyzes and studies complex system requirements. Design software tools and subsystems to support software reuse and domain analysis and manages their implementation. Manages software development and support using formal specifications, data flow diagrams, other accepted design techniques and Computer Aided Software Engineering (CASE) tools.

Minimum Education: Bachelor's degree in Computer Science, Information systems, Engineering, Business, or other related discipline.

19. Jr. Functional Analyst

Minimum/General Experience: 6 years experience total with a combination of Four (4) years general and Two (2) years of specialized experience. Experience in a variety of business disciplines such as: procurement, human resources, finance, logistics, medical, enterprise resource planning, electronic commerce and electronic data interchange, security, and requirements determination.

Functional Responsibility: Provides analysis to the project in all areas of functional implementation. Applies functional experience to business or technology problems. Provides specialized program and/or technical guidance concerning information technology solutions to complex business and information processing issues.

Minimum Experience: 4 years general and 2 year specialized experience.

20. Jr. Web/Internet Consultant

Experience: Knowledge of web related experience and languages (such as HTML). Understanding of graphic formats used on the World Wide Web; knowledge of techniques using mark-up languages including tables, forms and using word process to web mark up converters to maximize efficiency. Experience with web graphics, implementing image files, animation, icons and other advanced multi- media options for web pages. Uses Internet development tools and designs static and dynamic web pages. Journeyman experience in web related technologies and information technology assignments.

Responsibility: Design of web pages, development and placement of content, works with functional and technical staff to incorporate front-end content with back end data and content.

Minimum Experience: 2 years general and 1-year specialized experience.

Amyx Labor Rate List: current rates: SIN 132-51

Period of Performance	06/28/2016 - 06/27/2017	06/28/2017 - 06/27/2018	06/28/2018 - 06/27/2019	06/28/2019 - 06/27/2020	06/28/2020 - 06/28/2021
Labor Category	**Hourly Rate**	**Hourly Rate**	**Hourly Rate**	**Hourly Rate**	**Hourly Rate**
Sr. Information Management Systems Specialist	$333.74	$339.75	$345.87	$352.09	$358.43
Sr. Program Manager	$224.64	$228.68	$232.80	$236.99	$241.25
Program Manager	$221.43	$225.42	$229.47	$233.60	$237.81
Sr. Information Technology Architect/ Subject Matter Consultant	$200.01	$203.61	$207.28	$211.01	$214.81
Information Technology Architect/ Subject Matter Consultant	$174.71	$177.85	$181.05	$184.31	$187.63
Sr. Functional Analyst	$192.90	$196.37	$199.90	$203.50	$207.16
Sr. Logistics Business Process Reengineering (BPR) Consultant	$200.01	$203.61	$207.28	$211.01	$214.81
Sr. Systems Analyst	$192.90	$196.37	$199.90	$203.50	$207.16
Functional Analyst	$161.07	$163.97	$166.92	$169.92	$172.98
Jr. Functional Analyst	$138.27	$140.76	$143.29	$145.87	$148.49
Data Analyst	$155.29	$158.08	$160.93	$163.83	$166.78
Sr. Electronic Commerce (EC) Systems Engineer	$163.25	$166.19	$169.18	$172.22	$175.32
Sr. Electronic Commerce (EC) Systems Analyst	$163.25	$166.19	$169.18	$172.22	$175.32
Systems Requirements Consultant	$150.66	$153.37	$156.13	$158.94	$161.80
Web Internet Consultant	$171.42	$174.51	$177.65	$180.85	$184.10
Jr. Web Internet Consultant	$129.83	$132.17	$134.55	$136.97	$139.44
Sr. Technical Advisor	$162.99	$165.92	$168.91	$171.95	$175.05
Business Re-engineering Expert	$228.18	$232.29	$236.47	$240.73	$245.06
Sr. Information Engineer	$213.99	$217.84	$221.76	$225.75	$229.82
Information Engineer	$197.51	$201.06	$204.68	$208.37	$212.12

SECTION 3:
TERMS AND CONDITIONS APPLICABLE TO INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES SPECIAL ITEM NUMBERS (SINs) 132-45A, 132-45B, 132-45C and 132-45D

1. SCOPE

a. The labor categories, prices, terms and conditions stated under Special Item Numbers 132-45A, 132- 45B, 132-45C and 132-45D High Adaptive Cybersecurity Services apply exclusively to High Adaptive Cybersecurity Services within the scope of this Information Technology Schedule.

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

2. PERFORMANCE INCENTIVES

a. When using a performance based statement of work, performance incentives may be agreed upon between the Contractor and the ordering office on individual fixed price orders or Blanket Purchase Agreements, for fixed price tasks, under this contract in accordance with this clause.

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

c. To the maximum extent practicable, ordering offices shall consider establishing incentives where performance is critical to the agency’s mission and incentives are likely to motivate the contractor. Incentives shall be based on objectively measurable tasks.

3. ORDER

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

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

4. PERFORMANCE OF SERVICES

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

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

c. The Agency should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner.

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

5. INSPECTION OF SERVICES

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

6. RESPONSIBILITIES OF THE CONTRACTOR

The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character.

7. RESPONSIBILITIES OF THE GOVERNMENT

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

8. INDEPENDENT CONTRACTOR

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

9. ORGANIZATIONAL CONFLICTS OF INTEREST

a. Definitions.

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

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

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

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

10. INVOICES

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

11. PAYMENTS

For firm-fixed price orders the Government shall pay the Contractor, upon submission of proper invoices or vouchers, the prices stipulated in this contract for service rendered and accepted. Progress payments shall be made only when authorized by the order. For time-and-materials orders, the Payments under Time-and-Materials and Labor-Hour Contracts (Alternate I (APR 1984)) at FAR 52.232-7 applies to time-and-materials orders placed under this contract. For labor-hour orders, the Payment under Time-and-Materials and Labor-Hour Contracts (FEB 1997) (Alternate II (JAN 1986)) at FAR 52.232-7 applies to labor-hour orders placed under this contract.

12. RESUMES

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

13. INCIDENTAL SUPPORT COSTS

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

14. APPROVAL OF SUBCONTRACTS

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

SECTION 4:
DESCRIPTION OF SERVICES AND PRICING SERVICES SPECIAL ITEM NUMBERS (SINs) 132-45A, 132-45B, 132-45C and 132-45D

Amyx, Inc. GSA Labor Category Descriptions:

1. Network Security Analyst

Experience in defining network security requirements for local and wide area networks, evaluation of approved network security product capabilities, configuring standard communications protocols, detecting and analyzing network vulnerabilities, and developing proper computer system security solutions. Analyzes and determines security requirements for local and wide area networks. Designs, develops, engineers, and implements solutions that meet network security requirements. Responsible for integration and implementation of the network security solution. Performs vulnerability/risk analyses of computer systems and applications during all phases of the system development lifecycle.

Minimum Experience:
Five (5) years relevant experience

Required Skills:
Must possess IT-II security clearance or have a current National Agency Check with Local Agency Check and Credit Check (NACLC) at time of proposal submission.
Relevant certification from a nationally recognized technical authority.

2. Computer Security Systems Specialist

Basic Level: Provides specialized experience in determining computer security requirements for high-level applications, evaluating approved security product capabilities, and developing solutions to multilevel security (MLS) problems. Analyzes and defines security requirements for MLS issues. Designs, develops, engineers, and implements solutions to MLS requirements. Gathers and organizes technical information about an organization's mission goals and needs, existing security products, and ongoing programs in the MLS arena. Performs risk analysis, which includes risk assessment.

Senior Level: In addition to the above, provides daily supervision of, and direction to, staff.

Minimum Experience:
Five (5) years relevant experience

Required Skills:

Must possess IT-II security clearance or have a current National Agency Check with Local Agency Check and Credit Check (NACLC) at time of proposal submission.
Relevant certification from a nationally recognized technical authority.

3. Data Security Analyst

Maintains systems to protect data from unauthorized users. Identifies, reports, and resolves security violations. Minimum Experience:

Five (5) years relevant experience

Required Skills:
Must possess IT-II security clearance or have a current National Agency Check with Local Agency Check and Credit Check (NACLC) at time of proposal submission.
Relevant certification from a nationally recognized technical authority.

4. Web Security Analyst

Performs all procedures necessary to ensure the safety of the organization's website and transactions across the Internet/intranet. Applies Internet firewall technologies to maintain security. Ensures that the user community understands and adheres to necessary procedures to maintain security. Updates and deletes users, monitors and performs follow-up on compliance violations, and develops security policies, practices, and guidelines.

Minimum Experience:
Five (5) years relevant experience

Required Skills:
Must possess IT-II security clearance or have a current National Agency Check with Local Agency Check and Credit Check (NACLC) at time of proposal submission.
Relevant certification from a nationally recognized technical authority.

5. Computer Network Defense (CND) Analyst

Performs actions to protect, monitor, detect, analyze, and respond to unauthorized activity within assigned information systems and computer networks. Employs Cybersecurity capabilities and deliberate actions to respond to a CND alert or emerging situational awareness/threat. Serves as an expert on CND requirements and compliance to such requirements by using IA tools and techniques to perform compliance analysis and correlation, tracking and remediation coordination, and escalating CND non-compliance. Provides technical analysis and sustainment support for the enterprise for IA tools and applications, and assists with the application of Defense-In-Depth signatures and perimeter defense controls to diminish network threats.

Minimum Experience:
Five (5) years relevant experience

Required Skills:
Must possess a current DOD Top Secret Clearance and be eligible for an IT-1 at time of proposal submission.
Relevant certification from a nationally recognized technical authority meeting DOD 8570.01 IAT level II.
Must possess and maintain CNDSP-IR certification.

6. Cybersecurity Technology Management Analyst

Serves as an IA Subject Matter Expert (SME) with regards to IA Architecture policies and procedures. Provides IA Management support to Program Executive Officer (PEO) or Program Management Offices

(PMO) for emerging information systems through the acquisition lifecycle and where applicable into sustainment. Provides technical support and guidance to facilitate the identification and integration of IA controls at the onset of the acquisition lifecycle for emerging IT capabilities. Serves as a principal liaison for Enterprise-level boundary defense initiatives to ensure consistent and sufficient identification and implementation of applicable IA controls. Provides oversight for the design and implementation of Enterprise-level IA solutions providing standards for access control capabilities across the Enterprise.

Minimum Experience:

- Five (5) years of relevant experience
- Relevant certification meeting DOD 8570.01 IAM level III
- Ten years of practical industry, government and/or consulting experience in information technology management.
- IT project management experience using various Microsoft tools
- Knowledge and experience in managing information technology services and strategies.
- Proficiency in basic analytical software such as Microsoft Excel and Access, proficiency with the Microsoft Office suite, to include Word, PowerPoint and SharePoint.
- Must possess IT-III security clearance or have a current National Agency Check with written Inquiries (NACI) at time of task order proposal submission.

Special Skills (are desired but not required):

- Ten (10) years of relevant Certification and Accreditation (C&A) experience
- National Institute of Standards and Technology (NIST) C&A experience
- DOD IA experience

7. Control Validation Security Specialist

Under general supervision, performs IT audits on complex information systems, applications, and enclaves to ensure that appropriate controls exist, are correctly implemented, and that procedures are in compliance with Federal and DOD. Conducts accurate evaluation of the level of security required. Performs procedures necessary to ensure the safety of information systems assets and to protect systems from intentional or inadvertent access or destruction. Competent to work on most phases of information systems auditing. Provides technical support in the areas of vulnerability assessment, risk assessment, network security, and security implementation. Provides technical evaluations of customer systems and assists with making security improvements. Conducts cybersecurity control validation exercises on classified and unclassified networks, applications and systems to validate the effectiveness of current security measures. Must understand the concept of weighing business needs against security concerns and analyze applied mitigations to evaluate whether they meet security requirements.

Qualifications:

- Possesses a certification meeting the DOD 8570.01 IAM level III upon assignment.
- 2 years of experience working with DOD1 8500.2 or NIST SP 800-53, and understands the principles of the risk management framework.
- Strong analytical and problem solving skills for resolving security issues
- Proficiency in basic analytical software such as Microsoft Excel and Access, proficiency with the Microsoft Office suite, to include Word, PowerPoint
- Strong skills implementing and configuring networks and network components
- Understanding of eMASS and VMS
- Knowledge of DIACAP
- Required to possess a DOD SECRET Clearance, and be eligible for an IT-II upon assignment
- IAT level II certification

8. Cybersecurity Auditor – Senior

Demonstrated ability to independently perform complex security analysis of classified and unclassified applications, systems and enclaves for compliance with security requirements. Performs Command Cyber Readiness Inspections and cybersecurity vulnerability evaluations. Uses a variety of security techniques, technologies, and tools to evaluate security posture in highly complex computer systems and networks. Ability to perform vulnerability and risk analysis, and participate in a variety of computer security penetration studies.

Analyzes and defines security requirements for computer and networking systems, to include mainframes, workstations, and personal computers. Recommends solutions to meet security requirements. Gathers and organizes technical information about an organization's mission goals and needs, and makes recommendations to improve existing security posture. Demonstrated experience and ability to provide enterprise-wide technical analysis and direction for problem definition, analysis and remediation for complex systems and enclaves. Ability to provide workable recommendations and advice to client executive management on system improvements, optimization and maintenance in the following areas: Information Systems Architecture, Automation, Telecommunications, Networking, Communication Protocols, Application Software, Electronic Email, VOIP and VTC. Competent to work at the highest level of all phases of information systems auditing.

Qualifications:

- Proven proficiency performing CCRI/ vulnerability assessment/ penetration testing on networks, databases, computer applications and IT frameworks
- Seven years IT experience
- Five years IA experience
- Strong analytical and problem solving skills for resolving security issues
- Strong skills implementing and configuring networks and network components
- 2 years of experience with DOD Vulnerability Management System
- Command Cyber Readiness Inspection certification in at least one of the following areas:
    - Retina scan analysisOperating Systems (Windows, Unix)
    - Boundary defense (network policy, router, firewall)
    - Internal defense (L2 switch, L3 switch)
    - DNS (policy, BIND/Windows)
    - HBSS (remote console, AV, ABM, PA, HIPS, ePO)
    - Traditional security (Common, Basic, NCV, SCV)
    - Wireless communications (BES, handhelds)

- Tenable Certified NESSUS Auditor, IAM level III and IAT level II certifications.
- Knowledge and understanding of DOD security regulations, DISA Security Technical Implementation Guides
- Understanding of SCAP
- Knowledge of and proficiency with:
    - VULNERATOR
    - USCYBERCOM CTO Compliance Program
    - Wireless vulnerability assessment
    - Web Services (IIS, Apache, Proxy)
    - Database (SQL Server, Oracle)
    - Email Services (Exchange)
    - Vulnerability Scans (NESSUS, SCCM)
    - Knowledge of Phishing exercises
    - USB Detect
    - Physical Security

- Required to possess a DOD SECRET Clearance, and be eligible for an IT-II upon assignment.
- At least one contractor assigned to the team is required to be a DISA FSO certified CCRI Team Lead and have a certification in penetration testing, such as:
    - Licensed Penetration Tester (LPT)
    - Certified Expert Penetration Tester (CEPT)
    - Certified Ethical Hacker (CEH)
    - Global Information Assurance Certification Penetration Tester (GPEN)

- DoD 8570 CNDSP Analyst Certification
- Familiarity with AUTOCHECKLIST Tool

9. Cybersecurity Auditor – Intermediate

Under general supervision, performs complex security analysis of classified and unclassified applications, systems and enclaves for compliance with security requirements. Performs Command Cyber Readiness Inspections and cybersecurity vulnerability evaluations. Uses a variety of security techniques, technologies, and tools to evaluate security posture in highly complex computer systems and networks. Ability to perform vulnerability and risk analysis, and participate in a variety of computer security penetration studies. Analyzes and defines security requirements for computer and networking systems, to include mainframes, workstations, and personal computers. Works with senior auditor to recommend solutions to meet security requirements. Gathers and organizes technical information about an organization's mission goals and needs, and assists in making recommendations to improve existing security posture. Demonstrated experience and ability to provide enterprise-wide technical analysis and direction for problem definition, analysis and remediation for systems and enclaves. Ability to provide workable recommendations and advice to client management on system improvements, optimization and maintenance in the following areas: Information Systems Architecture, Automation, Telecommunications, Networking, Communication Protocols, Application Software, Electronic Email, VOIP and VTC. Competent to work on most phases of information systems auditing.

- Qualifications
    - Proven proficiency performing vulnerability assessment/ penetration testing on networks, databases, computer applications and IT frameworks
    - Five years of relevant IT experience
    - Three years IA experience
    - Strong analytical and problem solving skills for resolving security issues
    - Strong skills implementing and configuring networks and network components
    - Understanding of DOD Vulnerability Management System
    - DISA FSO training in at least one of the following areas:
        - Retina scan analysis
        - Operating Systems (Windows, Unix)
        - Boundary defense (network policy, router, firewall)
        - Internal defense (L2 switch, L3 switch)
        - DNS (policy, BIND/Windows)
        - HBSS (remote console, AV, ABM, PA, HIPS, ePO)
        - Traditional security (Common, Basic, NCV, SCV)
        - Wireless communications (BES, handhelds)

- Tenable Certified NESSUS Auditor, IAM level III and IAT level II certifications.
- Knowledge and understanding of DOD security regulations, DISA Security Technical Implementation Guides
- Understanding of SCAP
- Understanding of:

    - VULNERATOR
    - USCYBERCOM CTO Compliance Program
    - Wireless vulnerability assessment
    - Web Services (IIS, Apache, Proxy)
    - Database (SQL Server, Oracle)
    - Email Services (Exchange)
    - Vulnerability Scans (NESSUS, SCCM)
    - Knowledge of Phishing exercises
    - USB Detect
    - Physical Security
- Required to possess a DOD SECRET Clearance, and be eligible for an IT-II upon assignment.
- One of the following certifications:
    - Licensed Penetration Tester (LPT)
    - Certified Expert Penetration Tester (CEPT)
    - Certified Ethical Hacker (CEH)
    - Global Information Assurance Certification Penetration Tester (GPEN)
    - DoD 8570 CNDSP Analyst Certification
- Familiarity with AUTOCHECKLIST Tool
- Knowledge of VOIP, VTC
- Successful DISO FSO CCRI OJT

10. Penetration Tester – Senior

Demonstrated ability to independently perform penetration testing of applications, systems and enclaves.. Identifies security flaws in computing platforms and applications and devise strategies and techniques to mitigate identified cybersecurity risks. Perform application and network penetration testing and wireless security assessments. Apply offensive cybersecurity testing techniques, coordinate testing projects with internal and external system owners. Reports the nature of identified cyber security risks and recommends risk mitigation measures to improve the cyber security posture of the enterprise.

- Qualifications
    - 6 years proven proficiency in performing extensive vulnerability assessment and penetration testing.
    - Possess a certification meeting the DOD 8570.01 IAM level III (for non-CERT personnel), or IAT level II (for CERT personnel).
    - Required to possess a DOD TOP SECRET Clearance and be eligible for an IT-I upon assignment.
    - 3 years of experience with testing tools, including NESSUS, METASPLOIT, CANVAS, NMAP, Burp Suite, and Kismet3 years of experience with network vulnerability assessments and penetration testing methods
    - 3 years of experience with writing testing assessment reports
    - 2 years of experience with using, administering, and troubleshooting a WINDOWS Server, IIS
    - Knowledge of TCP/IP protocols and networking architectures
    - 2 years of experience with using, administering, and troubleshooting a major version of Linux
    - 2 years of experience PCI DSS testing
    - Possess a certification in penetration testing, such as:
        - Licensed Penetration Tester (LPT)
        - Certified Expert Penetration Tester (CEPT)
        - Certified Ethical Hacker (CEH)
        - Global Information Assurance Certification Penetration Tester (GPEN)

    - Excellent written documentation and oral presentation skills
    - Knowledge of open security testing standards and projects, including OWASP
    - Knowledge of database, applications, and Web server design and implementation
    - Experience scripting in Perl, Python, Ruby, Bash, or Java
    - Experience with wireless LAN security testing
    - Possess oral and written communication skills

11. Penetration Tester – Intermediate

Under general supervision, perform penetration testing of applications, systems and enclaves. . Identify security flaws in computing platforms and applications and devise strategies and techniques to mitigate identified cybersecurity risks. Perform application and network penetration testing and wireless security assessments. Apply offensive cybersecurity testing techniques, coordinate testing projects with internal and external system owners. Reports the nature of identified cyber security risks and recommends risk mitigation measures to improve the cyber security posture of the enterprise.

- Qualifications
    - 3 years proven proficiency in performing vulnerability assessment and penetration testing.
    - Possess a certification meeting the DOD 8570.01 IAM level III (for non-CERT personnel), or IAT level II (for CERT personnel).
    - Required to possess a DOD SECRET Clearance, and be eligible for an IT-II upon assignment.
    - 2 years of experience with testing tools, including NESSUS, METASPLOIT, CANVAS, NMAP, Burp Suite, and Kismet
    - 2 years of experience with network vulnerability assessments and penetration testing methods
    - 1 year of experience with writing testing assessment reports
    - 2 years of experience with using, administering, and troubleshooting WINDOWS Server, IIS or LINUX server, Apache.
    - Knowledge of TCP/IP protocols and networking architectures
    - 2 years of experience with using, administering, and troubleshooting Linux
    - Understanding of PCI DSS testing
    - Possess a certification in penetration testing, such as:
        - Licensed Penetration Tester (LPT)
        - Certified Expert Penetration Tester (CEPT)
        - Certified Ethical Hacker (CEH)
        - Global Information Assurance Certification Penetration Tester (GPEN)
    - Written documentation and oral presentation skills
    - Knowledge of open security testing standards and projects, including OWASP
    - Knowledge of database, applications, and Web server design and implementation
    - Experience scripting in Perl, Python, Ruby, Bash, or Java
    - Experience with wireless LAN security testing
    - Possess oral and written communication skills

12. Cybersecurity Engineer

Performs a variety of routine project tasks applied to specialized Cybersecurity problems. Tasks involve integration of electronic processes or methodologies to resolve total system problems, or technology problems as they relate to cybersecurity requirements. Analyzes information security requirements. Applies analytical and systematic approaches in the resolution of problems of work flow, organization, and planning. Provides security engineering support for planning, design, development, testing, demonstration, integration of information systems.

- Minimum Experience:
    - Seven (7) years of relevant IT experience
    - DOD Secret Clearance.
    - Must be eligible for IT II
    - Relevant certification meeting DOD 8570.01 IAM level II (for non-CERT personnel).
    - Relevant certification meeting DOD 8570.01 IAT level II for CERT personnel.
    - Computing Environment: ArcSight Enterprise Security Manager (ESM) 5.0 Security Analyst; ArcSight Logger 5.0 Administration and Operations; HBSS Administrator; HBSS Advanced; McAfee Network Security Platform Administration

13. Cybersecurity Certification and Accreditation Analyst

Serves as a cybersecurity Subject Matter Expert (SME) with regards to Authorization of information systems and all associated cybersecurity policies and procedures. Fully versed in the general tenets supporting the overall DOD implementation of its authorization process, to include supporting cybersecurity policy, procedures and processes. Performs a DOD cybersecurity process while either authorizing an information system or serving as a SME for an information system undergoing authorization. Possess an understanding of how the security controls identified in the NIST 800-53 apply to the process of assessing and authorizing a large organization’s IT infrastructure, in which there is a compilation of large and small enclaves, AIS applications and outsourced IT processes. Determines the applicable severity value for an identified vulnerability (e.g., non- compliant security control), and determines the possible ramifications on the system’s current or future authorization. Required to brief senior management on the progress or results of an information system undergoing the authorization process.

- Minimum Experience:
    - Five (5) years of relevant C&A experience; Risk Management Framework (RMF) and NIST C&A experience; DOD cybersecurity experience
    - DOD Secret Clearance.
    - Must be eligible for IT II
    - Relevant certification meeting DOD 8570.01 IAM level III (for non-CERT personnel), or IAT level II (for CERT personnel).
    - Experience in assessing security controls and conducting authorization reviews for large, complex organizations.
    - Computing Environment: AC & PHY SEC, CompTIA A+, CompTIA Network +, CompTIA Security +, CISSP, MCDST, MCITP EDST, MCITP EDA, MCITP SA, MCITP EA, MCM, MCA: MS Windows Server: Directory, Windows XP 3, Windows 7 9, MCSA, MCSE

14. Cybersecurity Policy Analyst

Reviews, consolidates and develops cybersecurity policy in accordance with RFP requirements. Fully versed in the general tenets supporting the overall DOD implementation of its cybersecurity policies, procedures and process and able to provide technical support and assistance to federal agencies and assess IT policies, standards, guidelines or procedures to ensure a balance of security and operational requirements. Required to brief senior management on cybersecurity policy changes, updates and progress.

- Minimum Experience:
    - Seven(7) years of relevant cybersecurity policy experience

    - DOD Secret Clearance.
    - Relevant certification meeting DOD 8570.01 IAM level III (for non-CERT personnel), or IAT level II (for CERT personnel).

15. Cybersecurity Compliance Reporting Analyst

Reviews, consolidates and develops compliance reports in accordance with RFP requirements. Required to be an expert in data management and software engineering and be able to coordinate effectively with the various organizations. Must be able to prepare reports and properly utilize the report data effectively.
Recommends establishment of new or modified reporting methods and procedures to improve report content and completeness of information.

- Minimum Experience:
    - Five (5) years of relevant IT experience
    - DOD Secret Clearance
    - Must be eligible for IT II
    - Relevant certification meeting DOD 8570.01 IAM level III

16. Cybersecurity Task Order Project Manager

Serves as the project manager for a large, complex task order (or a group of task orders affecting the same migration system) and shall assist the Program Manager in working with the Government Contracting Officer (KO), the task order-level COR and COTRs, Government management personnel and customer agency representatives. Under the guidance of the Program Manager, responsible for the overall management of the specific task order(s) and ensuring that the technical solutions and schedules in the task order are implemented in a timely manner. Performs enterprise wide horizontal integration planning and interfaces to other functional systems.

- Qualifications
    - Demonstrated leadership experience in projects of similar size and complexity
    - Six years general IT experience
    - Six years cybersecurity experience
    - Must possess a DOD Secret Clearance, and be eligible for an IT-II upon assignment. Must possess certification meeting the DOD 8570.01 IAM level III
    - Must possess a Risk Management Professional credential
    - Must possess a PMP or equivalent
    - Strong knowledge of RMF and DIACAP

17. Cybersecurity Subject Matter Expert – Lead

Provides expert support, research and analysis of exceptionally complex problems, and processes relating to them. Serves as technical expert to the Cybersecurity Assessment Program providing technical direction, interpretation and alternatives to complex problems. Thinks independently and demonstrates exceptional written and oral communications skills. Applies advanced technical principles, theories, and concepts. Contributes to the development of new principles, concepts, and methodologies. Works on unusually complex technical problems and provides highly innovative and ingenious solutions. Recommends cybersecurity software tools and assists in the development of software tool requirements and selection criteria to include the development of product specific STIGs from applicable DISA SRGs. Works under consultative direction toward predetermined long- range goals and objectives. Assignments are often self-initiated. Determines and pursues courses of action necessary to obtain desired results. Develops advanced technological ideas and guides their development into a final product. Expertise is in the area of cybersecurity and evaluations.

- Qualifications
    - Proven proficiency performing CCRI/ vulnerability assessment/ penetration testing on networks, databases, computer applications and IT frameworks
    - Seven years IT experience
    - Five years IA experience
    - Strong analytical and problem solving skills for resolving security issues
    - Strong skills implementing and configuring networks and network components
    - 3 years of experience with DOD Vulnerability Management System
    - Command Cyber Readiness Inspection certification in at least one of the following areas:
        - Retina scan analysis
        - Operating Systems (Windows, Unix)
        - Boundary defense (network policy, router, firewall)
        - Internal defense (L2 switch, L3 switch)
        - DNS (policy, BIND/Windows)
        - HBSS (remote console, AV, ABM, PA, HIPS, ePO)
        - Traditional security (Common, Basic, NCV, SCV)
        - Wireless communications (BES, handhelds)
    - Tenable Certified NESSUS Auditor, IAM level III and IAT level II certifications
    - Knowledge and understanding of DOD security regulations, DISA STIGs
    - Strong knowledge of SCAP
    - Strong knowledge of DIACAP
    - Excellent knowledge of and proficiency with:
        - VULNERATOR
        - USCYBERCOM CTO Compliance Program
        - Wireless vulnerability assessment
        - Web Services (IIS, Apache, Proxy)
        - Database (SQL Server, Oracle)
        - Email Services (Exchange)
        - Vulnerability Scans (NESSUS, SCCM)
        - Knowledge of Phishing exercises
        - USB Detect
        - Physical Security
    - Required to possess a DOD SECRET Clearance, and be eligible for an IT-II upon assignment.
    - DISA FSO certified CCRI Team Lead and certification in penetration testing, such as:
        - Licensed Penetration Tester (LPT)
        - Certified Expert Penetration Tester (CEPT)
        - Certified Ethical Hacker (CEH)
        - Global Information Assurance Certification Penetration Tester (GPEN)

18. Control Validation Security Specialist – Senior

Demonstrated ability to independently perform IT audits on complex information systems, applications, and enclaves to ensure that appropriate controls exist, are correctly implemented, and that procedures are in compliance with Federal and DOD standards. Conducts accurate evaluation of the level of security required. Performs all procedures necessary to ensure the safety of information systems assets and to protect systems from intentional or inadvertent access or destruction. Competent to work at the highest level of all phases of information systems auditing. Provides technical support in the areas of vulnerability assessment, risk assessment, network security, and security implementation. Provides technical evaluations of customer systems and assists with making security improvements. Conducts cybersecurity control validation exercises on classified and unclassified networks, applications and systems to validate the effectiveness of current security measures. Must be able to weigh business needs against security concerns and be able to analyze applied mitigations to evaluate whether they meet security requirements.

- Qualifications
  - Possesses a certification meeting the DOD 8570.01 IAM level III upon assignment.
  - 3 years of experience working with DOD1 8500.2 or NIST SP 800-53, and understand the principles of the risk management framework.
  - Strong analytical and problem solving skills for resolving security issues
  - Proficiency in basic analytical software such as Microsoft Excel and Access, proficiency with the Microsoft Office suite, to include Word, PowerPoint
  - Strong skills implementing and configuring networks and network components
  - 2 years of experience with eMASS and VMS
  - Understanding of DIACAP
  - Required to possess a DOD SECRET Clearance, and be eligible for an IT-II upon assignment.
  - IAT level II certification

19. IA Access Management Analyst

Performs various Identity and Access Management services to ensure the confidentiality, availability, integrity and non-repudiation of sensitive and classified information and information systems. Serves as an IA SME with regards to Access and Identity Management and all associated IA policies and procedures. Fully versed in the general tenets supporting the overall DOD implementation of its identity, credential and access management service in accordance with DOD policy, procedures and processes. Possess an understanding of how DOD Instruction 8520.03, Identity Authentication for Information, is used for access management by validating entities are granted or denied access to resources such as computer systems or data.

Minimum Experience:

- Minimum Seven (7) years of relevant IT experience; relevant certification meeting DOD 8570.01 IAM level I.

Security/Certification Requirements:

- Sensitivity Level: IT-II – Non-critical Sensitive Clearance: Secret
- IA Level: IAM-I
- Computing Environment: AC & PHY SEC, CompTIA A+, CompTIA Network +, CompTIA Security +, CISSP, MCDST, MCITP EDST, MCITP EDA, MCITP SA, MCITP EA, MCM, MCA: MS Windows Server: Directory, Windows XP 3, Windows 7 9, MCSA, MCSE

20. IA Project Engineer

Serve as the process manager that directs the execution of day-to-day tasks. Responsible for all aspects of the development and implementation of assigned projects and provides a single point of contact for those projects. Defines project scope and objectives, develops detailed work plans, schedules, project estimates, resource plans, and status reports. Conducts project meetings and is responsible for project tracking and analysis. Ensures adherence to quality standards and reviews project deliverables. Manages the integration of project tasks and tracks and reviews vendor deliverables. Provides technical and analytical guidance to project team. Recommends and takes action to direct the analysis and solutions of problems.

Minimum Experience:

- Seven (7) years of relevant IT experience
- Eight (8) years DOD IA experience

Security/Certification Requirements:

- Sensitivity Level: IT-I – Critical Sensitive
- Clearance: Top Secret
- Relevant certification meeting DOD 8570.01 IAM level I
- Computing Environment: M2003 2; MCSA; MCSE; M2008 6; MCITP SA; MCITP EA; MCITP EMA; MCITP DBA; MCM; MCA: MS SQL Server; MCA: MS Exchange Server; MCA: MS Windows Server Directory; GCWN; HP UX CSA; GCUX; SCSA

21. Cyberspace Exercise Planner

Assists in the coordination of Cyberspace Exercise Planner activities, both integrating and facilitating DoD and Cyber exercise requirements. Must have ability to understand Cyber Terrain and perform in- depth J6 mission analysis for specified, implied, and essential tasks. s. The contractor shall support exercise events in accordance with the Joint Operational Planning Process (JOPP) from the J6 and cyberspace perspective. The contractor shall develop and coordinate exercise training objectives, building the Master Scenario Events List (MSEL), and entering MSELs into applicable databases for Chairman Joint Chiefs of Staff (CJCS), COCOM, and other stakeholder exercises. The contractor shall assist in designing, planning, coordinating, and integrating cyber effects into exercises to achieve the command's training objectives. The contractor shall assist in observing and evaluating personnel against the training objectives. The contractor shall provide assessment and lessons learned inputs post exercise and shall assist in addressing any follow-on action items. The contractor shall provide communications, cyberspace and exercise planning support using the Government provided automated software tools, when applicable, and IAW the suspense assigned by the Government or through the Government staffing process.

Minimum Experience:

- Five (5) years relevant experience in IT/CS
- Ten (10) years relevant DoD Logisticians experience

Required Skills:

- Must have an active DOD Top Secret Clearance at time of proposal submission and be eligible for IT-1 upon assignment.
- IA Level: IAM II

22. Cyberspace Readiness and Joint Training Specialist

The contractor shall assist the organization with Cyberspace readiness and joint training. The contractor shall support all phases of the Joint Training System to include analyzing mission requirements; developing training, objectives and plans; executing/observing/evaluating training events, and conducting ongoing readiness/assessments. The contractor shall evaluate the the readiness reports to determine if they adequately provide sufficient information and help compile the data into meaningful
readiness indicators. The contractor must enable/solicit understanding of integrated Cyber mission requirements during times of mission constraints. Contractor to propose Cyberspace courses of action to mitigate risk, preferably, to pre-position federal agencies with acceptable risk mitigation and readiness before any exercise. The contractor shall assist in making recommendations
to leadership and staff concerning updates/changes and in assessment criteria. The contractor shall assist in preparing for joint
training meetings and completing any after actions. The contractor shall provide lessons learned and after action reports, tracking integrated actions until closure and escalating to support integrated business risk governance. The contractor shall provide support using the Government provided automated software tools,

when applicable, and IAW the suspense assigned by the Government or through the Government staffing process

Minimum Experience:

- Five (5) years relevant experience in IT/CS

Required Skills:

- Must have an active DOD Top Secret Clearance at time of proposal submission and be eligible for IT-1 upon assignment.
- IA Level: IAM III

23. Industrial Control System (ICS) Supervisory Control and Data Acquisition (SCADA) Specialist

Control Systems Cybersecurity (CSC) Specialist: The Control Systems Cybersecurity specialist shall have a minimum of five years' experience in control system network and security design. The Control Systems Cybersecurity specialist must have demonstrated knowledge and experience applying Information Technology (IT) and Operational Technology (OT) security strategies such as the application of the National Institute of Standards and Technology (NIST) security controls, exploitation techniques and methods, continuous monitoring, and ICS acquisition life cycle as outlined in the NIST Special Publication (SP) 800-82 (Current version).

The CSC Specialist must also possess broad knowledge of and experience in the following areas:

Utility Control System (UCS) A type of field control system used for control of utility systems such as electrical distribution and generation, sanitary sewer collection and treatment, water generation and pumping, etc. Building controls are excluded from a UCS, however it is possible to have a Utility Control System and a Building Control System in the same facility, and for those systems to share components such as the Field Point of Connection (FPOC). A UCS is a subsystem of a Utility Monitoring and Control System (CS) and is a class of Field Control System (FCS).

Utility Monitoring and Control System (CS) The system consisting of one or more building control systems and/or utility control systems and the associated CS Infrastructure. In other words, it is the complete utility monitoring system – from the front end to equipment controllers. At the highest level the CS is composed of a CS Platform Enclave and CS Front End (jointly referred to as CS Infrastructure), and connected Field Control System(s).

Manufacturing and Distribution Manufacturing can be categorized into process-based and discrete-based processes; 1) Continuous processes associated with fuel, steam, and other types of flows such as logistic distributions of solid material; 2) Batch processes, distinct steps – conducted on quantity of material leading to a finished product like food manufacturing and distribution as an example.

Other Types of Control Systems Other types of controls systems (That share similar characteristics of ICS) operating in different modes than ICS such as Emergency Management Systems, Public Safety, Communication Systems, etc. utilizing system specific protocols, ports & services.

Qualifications:

- Minimum Five (5) years of relevant experience
- Certification meeting DOD 8570.01 IAM level III
- Global Industrial Cyber Security Professional (GICSP)
- Ten years of practical industry, government and/or consulting experience in information technology management.
- IT project management experience using various Microsoft tools
- Knowledge and experience in managing information technology services and strategies.
- Proficiency in basic analytical software such as Microsoft Excel and Access, proficiency with the Microsoft Office suite, to include Word, PowerPoint and SharePoint.
- Required to possess a DOD SECRET Clearance and be eligible for an IT II upon assignment.

- Ten (10) years of relevant Certification and Accreditation (C&A) experience
- National Institute of Standards and Technology (NIST) C&A experience
- DOD IA experience

24. Information Security Analyst (Data Protection)

Serves as information security analyst performing incident response (identification, containment, eradication, recovery) for Personally Identifiable Information (PII) incidents and PII-related data breaches. Utilizes data loss prevention (DLP) tools to identify improperly stored PII data at rest and improperly transmitted PII data. Performs the quarantining of improperly stored PII data. Recommends appropriate actions to mitigate the risk of unauthorized access to PII data and ensures the implementation of appropriate security controls to safeguard PII data. Engages with stakeholders and mission partners to facilitate containment, eradication, and recovery for PII incidents. Validates remedial actions and ensures compliance with DOD information security and privacy policy.

Minimum Experience:

- Five (5) years relevant experience

Required Skills:

- Required to possess a DOD SECRET Clearance, and be eligible for an IT-II upon assignment.
- IAT level II certification
- Hands-on experience performing computer security incident handling
- Hands-on experience with data loss prevention software/tools

25. Operational Technology Security Engineer

Performs a variety of routine project tasks applied to specialized information assurance problems with operational technology (OT) systems. Tasks involve integration of OT processes or methodologies with information systems to resolve total system problems, or technology problems as they relate to IA requirements. Analyzes information security requirements. Applies analytical and systematic approaches in the resolution of problems of work flow, organization, and planning. Provides security engineering support for planning, design, development, testing, demonstration, integration of OT systems.

- Minimum Experience:
  - Seven (7) years of relevant OT experience
  - DOD Secret Clearance
  - Must be eligible for IT II
  - Relevant certification meeting DOD 8570.01 IAM level II
  - Experience with Modbus/TCP, EtherNet/IP, IEC 61850, ICCP and DNP3, BACnet, and other OT protocols

26. Operational Technology Specialist

Basic Level: Ability to evaluate operational technology (OT) systems, and to interface with other information technology (IT) and OT equipment and systems. Ability to troubleshoot bottlenecks and propose recommendations for their elimination, and make recommendations for system improvements that will result in optimization of development and/or maintenance efforts. Ability to analyze and suggest recommended improvements to the OT system programs and systems to meet industry standards and best practices. OT systems include, but are not limited to, Utility Monitoring and Control Systems (UMCS), Electronic Security Systems (ESS), Building Automation Systems (BAS), Fire and Emergency Services Systems, Fuels Supervisory Control and Data Acquisition (SCADA) systems, Fuels Dispensing, Tank Gauging systems, Material Handling systems, and all other OT control systems having automated operational control functions.

Minimum Experience:

- Five (5) years relevant experience

Required Skills:

- Must possess IT-II security clearance or have a current National Agency Check with Local Agency Check and Credit Check (NACLC) at time of proposal submission.
- Experience with various vendors and types of OT systems, including PLCs, VFDs, HMIs, and network protocols
- Experience with Cybersecurity standards, best practices for OT systems, evaluating security vulnerabilities, developing mitigation strategies and how to integrate them, and developing policy and procedure for DoD risk management framework requirements.
- Possession of excellent research and analytical skills
- Possession of excellent oral and written communication skills|

Senior Level: Demonstrated ability to lead or supervise a team of specialists in developing, managing, maintaining, and evaluating OT systems and their integration with other OT and IT systems. Able to evaluate applications in support of specific OT requirements and interface with other equipment and systems. Ability to determine potential and current bottlenecks; propose workable recommendations for their elimination; and make recommendations for systems improvements that will result in optimal hardware and software usage. Ability to analyze and suggest recommended improvements to the OT system programs and systems to meet industry standards and best practices.

Minimum Experience:

- Eight (8) years relevant experience

Required Skills:

- Must possess IT-II security clearance or have a current National Agency Check with Local Agency Check and Credit Check (NACLC) at time of proposal submission.
- Relevant certification or training certificate from a nationally recognized technical authority in the relevant OT system.
- Expert knowledge of security issues, techniques, and implications across OT platforms.
- Capacity to perform risk assessments and recommend risk-based security solutions for OT systems
- Strong conceptual thinking and communication skills — the ability to conceptualize complex business and technical requirements into comprehensible models and templates
- Proven ability to work effectively in a team setting, as well as independently, with minimal error and guidance
- Exceptional verbal and written communication skills with the ability to communicate with all levels of personnel to include Managers and field level employees
- Excellent planning and organizational skills with an ability to understand the long-term ("big picture")
- Ability to think strategically and implement iteratively
- Excellent interpersonal skills in areas such as teamwork, facilitation, and negotiation
- Experience with Cybersecurity standards, best practices for OT systems, evaluating security vulnerabilities, developing mitigation strategies and how to integrate them, and developing policy and procedure for DoD risk management framework requirements.

27. Vulnerability Management Analyst (Application)

Serves as vulnerability management analyst for assigned applications. Analyzes vulnerabilities and characterizes risk. Engages with stakeholders and mission partners to facilitate application vulnerability assessments. Performs code review, software assurance testing, and application vulnerability scanning. Facilitates the coordination of remediation efforts, prioritizing remediation efforts based on risk. Recommends

appropriate actions to remediate vulnerabilities and mitigate risks and ensures the implementation of appropriate security settings to include those required by Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG).
Tracks and reports security and compliance issues. Validates remedial actions and ensures compliance with Federal and DOD information security policy.

Minimum Experience:

- Five (5) years relevant experience

Required Skills:

- Required to possess a DOD SECRET Clearance, and be eligible for an IT-II upon assignment.
- IAT level II certification
- Hands-on experience developing code
- Hands-on experience performing code review and software assurance testing
- Hands-on experience working with application vulnerability scanners
- Understanding of application vulnerabilities and remediation techniques

28. Vulnerability Management Analyst (OS/Infrastructure)

Serves as vulnerability management analyst for assigned information systems and computer networks. Analyzes vulnerabilities and characterizes risk to networks, operating systems, applications, databases, and other information system components. Engages with stakeholders and mission partners to facilitate vulnerability discovery through manual review and/or the use of vulnerability scanners. Facilitates the coordination of remediation efforts, prioritizing remediation efforts based on risk. Recommends appropriate actions to remediate vulnerabilities and mitigate risks and ensures the implementation of appropriate security settings to include those required by Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG).
Supports and ensures compliance with DOD Information Assurance Vulnerability Management (IAVM) program. Tracks and reports security and compliance issues. Validates remedial actions and ensures compliance with Federal and DOD information security policy.

Minimum Experience:

- Five (5) years relevant experience

Required Skills:

- Required to possess a DOD SECRET Clearance, and be eligible for an IT-II upon assignment.
- IAT level II certification
- Hands-on experience working with vulnerability scanners
- Understanding of vulnerabilities and remediation techniques

29. Vulnerability Management Analyst (Web Applications)

Serves as vulnerability management analyst for assigned web applications. Analyzes vulnerabilities and characterizes risk. Engages with stakeholders and mission partners to facilitate vulnerability discovery through manual review and/or the use of web application vulnerability scanners. Facilitates the coordination of remediation efforts, prioritizing remediation efforts based on risk. Recommends appropriate actions to remediate vulnerabilities and mitigate risks and ensures the implementation of appropriate security settings to include those required by Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG). Tracks and reports security and compliance issues. Validates remedial actions and ensures compliance with Federal and DOD information security policy.
Minimum Experience:

- Five (5) years relevant experience

Required Skills:

- Required to possess a DOD SECRET Clearance, and be eligible for an IT-II upon assignment.
- IAT level II certification
- Hands-on experience working with web application vulnerability scanners
- Understanding of web application vulnerabilities and remediation techniques

Period of Performance	**1/4/2018-1/3/2019**	**1/4/2018-1/3/2019**
Labor Category (Inclusive of IFF)	**Government Site**	**Contractor Site**
Network Security Analyst	$81.38	$89.52
Computer Security Systems Specialist - Basic	$66.23	$72.85
Computer Security Systems Specialist - Senior	$76.66	$84.33
Data Security Analyst	$82.01	$90.21
Web Security Analyst	$75.76	$83.34
Computer Network Defense (CND) Analyst	$131.74	$144.19
Cybersecurity Technology Management Analyst	$138.16	$151.98
Control Validation Security Specialist – Intermediate	$109.64	$120.60
Cybersecurity Auditor - Senior	$158.67	$174.53
Cybersecurity Auditor - Intermediate	$133.71	$147.07
Penetration Tester - Senior	$129.16	$142.08
Penetration Tester - Intermediate	$120.69	$132.76
Cybersecurity Engineer	$141.28	$155.42
Cybersecurity Certification and Accreditation Analyst	$132.55	$142.89
Cybersecurity Technical Writer	$88.19	$90.60
Cybersecurity Policy Analyst	$123.64	$135.99
Cybersecurity Compliance Reporting Analyst	$105.18	$137.27
Cybersecurity Task Order Project Manager	$143.77	$158.16
Cybersecurity Subject Matter Expert - Lead	$147.07	$186.30
Control Validation Security Specialist – Senior	$121.67	$133.84
IA Access Management Analyst	$114.10	$125.50
IA Project Engineer	$124.79	$137.27
Cyberspace Exercise Planner	$133.17	$146.49
Cyberspace Readiness and Joint Training Specialist	$124.88	$137.36
Industrial Control System (ICS) Supervisory Control and Data Acquisition (SCADA) Specialist	$168.46	$185.31
Information Security Analyst (Data Protection)	$120.15	$132.17
Operational Technology Security Engineer	$129.42	$142.37
Operational Technology Specialist - Basic	$88.70	$97.56
Operational Technology Specialist - Senior	$121.23	$133.34
Vulnerability Management Analyst (Application)	$118.11	$129.92
Vulnerability Management Analyst (OS/Infrastructure)	$119.09	$131.00
Vulnerability Management Analyst (Web Applications)	$122.83	$135.12

SECTION 5: USA COMMITMENT TO PROMOTE SMALL BUSINESS PARTICIPATION PROCUREMENT PROGRAMS

PREAMBLE

Amyx, Inc. provides commercial products and services to the Federal Government. We are committed to promoting participation of small, small disadvantaged and women-owned small businesses in our contracts. We pledge to provide opportunities to the small business community through reselling opportunities, mentor-protégé programs, joint ventures, teaming arrangements, and subcontracting.

COMMITMENT

To actively seek and partner with small businesses.

To identify, qualify, mentor and develop small, small disadvantaged and women-owned small businesses by purchasing from these businesses whenever practical.

To develop and promote company policy initiatives that demonstrates our support for awarding contracts and subcontracts to small business concerns.

To undertake significant efforts to determine the potential of small, small disadvantaged and women- owned small business to supply products and services to our company.

To insure procurement opportunities are designed to permit the maximum possible participation of small, small disadvantaged, and women-owned small businesses.

To attend business opportunity workshops, minority business enterprise seminars, trade fairs, procurement conferences, etc., to identify and increase small businesses with whom to partner.

To publicize in our marketing publications our interest in meeting small businesses that may be interested in subcontracting opportunities.

We signify our commitment to work in partnership with small, small disadvantaged and women-owned small businesses to promote and increase their participation in Federal Government contracts. To accelerate potential opportunities, please contact:

Amyx, Inc.
Attn: Contracts Dept.
Phone (703) 373-1984
Fax (571) 612-4365
Website: Amyx.com

SECTION 5:
BEST VALUE
BLANKET PURCHASE
AGREEMENT FEDERAL SUPPLY

(Insert Customer Name)

In the spirit of the Federal Acquisition Streamlining Act (Agency) and (Contractor) enter into a cooperative agreement to further reduce the administrative costs of acquiring commercial items from the General Services Administration (GSA) Federal Supply Schedule Contract(s)___________________________.

Federal Supply Schedule contract BPAs eliminate contracting and open market costs such as: search for sources; the development of technical documents, solicitations and the evaluation of offers. Teaming Arrangements are permitted with Federal Supply Schedule Contractors in accordance with Federal Acquisition Regulation (FAR) 9.6.

This BPA will further decrease costs, reduce paperwork, and save time by eliminating the need for repetitive, individual purchases from the schedule contract. The end result is to create a purchasing mechanism for the Government that works better and costs less.

Signatures

_________________________________   _________________________________
Agency Date   Contractor Date

BPA NUMBER_____________

Blanket Purchase Agreement

(CUSTOMER NAME)

Pursuant to GSA Federal Supply Schedule Contract Number(s)____________, Blanket Purchase Agreements, the Contractor agrees to the following terms of a Blanket Purchase Agreement (BPA) EXCLUSIVELY WITH (Ordering Agency):

(1) The following contract items can be ordered under this BPA. All orders placed against this BPA are subject to the terms and conditions of the contract, except as noted below:

MODEL NUMBER/PART NUMBER *SPECIAL
BPA DISCOUNT/PRICE

________________________________ ______________________________
________________________________ ______________________________
________________________________ ______________________________

(2) Delivery:

DESTINATION DELIVERY SCHEDULES / DATES

________________________________ ______________________________
________________________________ ______________________________
________________________________ ______________________________

(3) The Government estimates, but does not guarantee, that the volume of purchases through this agreement will be__________________________.

(4) This BPA does not obligate any funds.

(5) This BPA expires on__________________or at the end of the contract period, whichever is earlier.

(6) The following office(s) is hereby authorized to place orders under this BPA:

OFFICE POINT OF CONTACT

________________________________ ______________________________
________________________________ ______________________________
________________________________ ______________________________

(7) Orders will be placed against this BPA via Electronic Data Interchange (EDI), FAX, or paper.

(8) Unless otherwise agreed to, all deliveries under this BPA must be accompanied by delivery tickets or sales slips that must contain the following information as a minimum:

(a) Name of Contractor;

(b) Contract Number;

(c) BPA Number;

(d) Model Number or National Stock Number (NSN);

(e) Purchase Order Number;

(f) Date of Purchase;

(g) Quantity, Unit Price, and Extension of Each Item (unit prices and extensions need not be shown when incompatible with the use of automated systems; provided, that the invoice is itemized to show the information); and

(h) Date of Shipment.

(9) The requirements of a proper invoice are specified in the Federal Supply Schedule contract. Invoices will be submitted to the address specified within the purchase order transmission issued against this BPA.

(10) The terms and conditions included in this BPA apply to all purchases made pursuant to it. In the event of an inconsistency between the provisions of this BPA and the Contractor's invoice, the provisions of this BPA will take precedence.

BASIC GUIDELINES FOR USING "CONTRACTOR TEAM ARRANGEMENTS"

Federal Supply Schedule Contractors may use "Contractor Team Arrangements" (see FAR 9.6) to provide solutions when responding to a customer agency requirements.

These Team Arrangements can be included under a Blanket Purchase Agreement (BPA). BPAs are permitted under all Federal Supply Schedule contracts.

Orders under a Team Arrangement are subject to terms and conditions or the Federal Supply Schedule Contract.

Participation in a Team Arrangement is limited to Federal Supply Schedule Contractors.

Customers should refer to FAR 9.6 for specific details on Team Arrangements.

Here is a general outline on how it works:

- The customer identifies their requirements.
- Federal Supply Schedule Contractors may individually meet the customer's needs, or -
- Federal Supply Schedule Contractors may individually submit a Schedules "Team Solution" to meet the customer's requirement.
- Customers make a best value selection.