GENERAL SERVICES ADMINISTRATION

Federal Acquisition Service

Authorized Federal Supply Schedule FSS Price List

Online access to contract ordering information, terms and conditions, pricing, and the option to create an electronic delivery order are available through GSA Advantage!®. The website for GSA Advantage!® is: https://www.GSAAdvantage.gov.

Multiple Award Schedule (MAS)
Federal Supply Group: Professional Services
Contract Number: GS-00F-175DA
For more information on ordering go to the following website: https://www.gsa.gov/schedules.
Contract Period: June 03, 2016 - June 02, 2026
Supplement No. PS-0020, effective 2/8/2023
Prices Shown Herein are Net (discount deducted)

Contractor:

ARCHARITHMS, INC
1002 Meridian
Street N
Huntsville, AL 35801
(256) 763-8781
randy.riley@archarithms.com

Business Size: Small

Telephone: (256) 763-8781
FAX Number: None
Web Site: www.archarithms.com
E-mail: randy.riley@archarithms.com
Contract Administration: Randy Riley

CUSTOMER INFORMATION:

1a. Table of Awarded Special Item Number(s) with appropriate cross reference to item descriptions and awarded price(s):

SIN	RC	SIN Description
541330ENG	541330ENGRC	Engineering Services
541380	541380RC	Testing Laboratory Services
541715	541715RC	Engineering Research and Development and Strategic Planning
541420	541420RC	Engineering System Design and Integration Services
54151S	54151SRC	Information Technology Professional Services
54151HACS	54151HACSRC	Highly Adaptive Cybersecurity Services
OLM	OLMRC	Order Level Materials

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

See Pricelist (Government net price based on a unit of one)

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

See Pricelist (includes discount and IFF).

2. Maximum Order: max

541330ENG: $1,000,000
541380: $250,000
541715: $1,000,000
541420: $1,000,000
54151S: $500,000
54151HACS: $500,000

3. Minimum Order: $100

4. Geographic coverage (delivery Area): Domestic and Overseas

5. **Point(s) of production (city, county, and state or foreign country):** 1002 Meridian Street N Huntsville, AL 35801-4661

6. **Discount from list prices or statement of net price:** Government net prices (discounts already deducted).

7. **Quantity discounts:** N/A

8. **Prompt payment terms:** Net 30 days. Information for Ordering Offices: Prompt payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions

9. **Foreign items (list items by country of origin):** Not Applicable

10a. **Time of Delivery (Contractor insert number of days):** Contact Contractor

10b. **Expedited Delivery. The Contractor will insert the sentence "Items available for expedited delivery are noted in this price list." under this heading. The Contractor may use a symbol of its choosing to highlight items in its FSS price list that have expedited delivery.** Contact Contractor

10c. **Overnight and 2-day delivery. The Contractor must indicate whether overnight and 2-day delivery are available. Also, the Contractor must indicate that the ordering activity may contact the Contractor for rates for overnight and 2-day delivery.** Contact Contractor

10d. **Urgent Requirements. The Contractor must note in its FSS price list that ordering agencies can request accelerated delivery for urgent requirements.** Contact Contractor

11. **F.O.B Points(s):** Destination

12a. **Ordering Address(es):** Same as Contractor

12b. **Ordering procedures:** See Federal Acquisition Regulation (FAR) 8.405-3.

13. **Payment address(es):** Same as company address

14. **Warranty provision.:** Contractor's standard commercial warranty.

15. **Export Packing Charges (if applicable):** N/A

16. Terms and conditions of rental, maintenance, and repair (if applicable): N/A

17. Terms and conditions of installation (if applicable): N/A

18a. Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices (if applicable): N/A

18b. Terms and conditions for any other services (if applicable): N/A

19. List of service and distribution points (if applicable): N/A

20. List of participating dealers (if applicable): N/A

21. Preventive maintenance (if applicable): N/A

22a. Special attributes such as environmental attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants). N/A

22b. If applicable, indicate that Section 508 compliance information is available for the information and communications technology (ICT) products and services offered and show where full details can be found (e.g., Contractor's website or other location). ICT accessibility standards can be found at https://www.section508.gov/. Archarithms complies with Section 508

23. Unique Entity Identifier (UEI) number: LYSTBJSGN458

24. Notification regarding registration in System for Award Management (SAM) database: Contractor registered and active in SAM

FINAL PRICING

The rates shown below include the Industrial Funding Fee (IFF) of 0.75%.

		Year 7		Year 8	Year 9	Year 10
		6/2/2022 - 2/7/2023-	2/8/2023- 6/2/2023	6/3/2023 - 6/2/2024	6/3/2024 - 6/2/2025	6/3/2025 - 6/2/2026
SIN	**Labor Category**	**GSA PRICE including IFF**	**GSA PRICE including IFF**	**GSA PRICE including IFF**	**GSA PRICE including IFF**	**GSA PRICE including IFF**
54151HACS	Senior Cyber/System Engineer	N/A	$179.46	$183.05	$186.71	$190.45
54151HACS	Mid Cyber/Systems Engineer	N/A	$143.03	$145.89	$148.82	$151.79
54151HACS	Junior Cyber/Systems Engineer **	N/A	$108.47	$110.64	$112.86	$115.11
54151HACS	Senior Cyber Application Engineer	N/A	$219.41	$223.80	$228.27	$232.84
54151HACS	Mid Cyber Application Engineer	N/A	$184.16	$187.85	$191.61	$195.44
54151HACS	Junior Cyber Application Engineer **	N/A	$128.45	$131.02	$133.64	$136.31
54151HACS	Senior Cyber Intrusion Analyst	N/A	$197.00	$200.94	$204.96	$209.06
54151HACS	Mid Cyber Intrusion Analyst	N/A	$179.40	$182.98	$186.64	$190.37
54151HACS	Junior Cyber Intrusion Analyst **	N/A	$125.32	$127.83	$130.39	$133.00
54151HACS	Senior/Advanced Cyber Threat Analyst (ACTA)	N/A	$178.94	$182.52	$186.17	$189.89
54151HACS	Mid Cyber Threat Analyst (ACTA)	N/A	$169.97	$173.37	$176.84	$180.37

54151HACS	Junior Cyber Threat Analyst (ACTA) **	N/A	$132.21	$134.85	$137.55	$140.30
541330ENG, 541380, 541715, 541420, 54151S	Executive Consultant	$229.91	$229.91	$234.51	$239.20	$243.98
541330ENG, 541380, 541715, 541420, 54151S	Program Manager	$223.33	$223.33	$227.79	$232.35	$237.00
541330ENG, 541380, 541715, 541420, 54151S	Project Manager	$89.38	$89.38	$91.17	$92.99	$94.85
541330ENG, 541380, 541715, 541420, 54151S	Engineer Advanced VI	$216.08	$216.08	$220.40	$224.81	$229.30
541330ENG, 541380, 541715, 541420, 54151S	Engineer/Scientist VI	$211.67	$211.67	$215.91	$220.22	$224.63
541330ENG, 541380, 541715, 541420, 54151S	Engineer/Scientist V	$200.02	$200.02	$204.02	$208.10	$212.26
541330ENG, 541380, 541715, 541420, 54151S	Engineer/Scientist IV	$176.83	$176.83	$180.36	$183.97	$187.65
541330ENG, 541380, 541715, 541420, 54151S	Engineer/Scientist III	$149.63	$149.63	$152.62	$155.67	$158.79
541330ENG, 541380, 541715, 541420, 54151S	Engineer/Scientist II	$131.60	$131.60	$134.23	$136.92	$139.65
541330ENG, 541380, 541715, 541420, 54151S	Engineer/Scientist I	$87.49	$87.49	$89.24	$91.03	$92.85
541330ENG, 541380, 541715, 541420, 54151S	Senior Principal Investigator	$181.55	$181.55	$185.18	$188.88	$192.66
541330ENG, 541380, 541715, 541420, 54151S	Engineer Advanced V	$175.35	$175.35	$178.86	$182.44	$186.09
541330ENG, 541380, 541715, 541420, 54151S	Engineer Basic	$78.03	$78.03	$79.59	$81.18	$82.81

541330ENG, 541380, 541715, 541420, 54151S	Electrical Design Engineer II	$144.18	$144.18	$147.07	$150.01	$153.01
541330ENG, 541380, 541715, 541420, 54151S	Software Engineer III	$121.22	$121.22	$123.64	$126.11	$128.64
541330ENG, 541380, 541715, 541420, 54151S	Security & Information Processing Specialist	$79.15	$79.15	$80.74	$82.35	$84.00
541330ENG, 541380, 541715, 541420, 54151S	Program Analyst IX	$168.25	$168.25	$171.61	$175.05	$178.55
541330ENG, 541380, 541715, 541420, 54151S	Program Analyst IV	$108.42	$108.42	$110.59	$112.80	$115.05
541330ENG, 541380, 541715, 541420, 54151S	Program Analyst	$46.31	$46.31	$47.23	$48.18	$49.14

SERVICE CONTRACT LABOR STANDARDS (SCLS) MATRIX

Eligible Contract Labor Category	Equivalent Code - Title	WD Number
Junior Cyber/Systems Engineer	30082 - Engineering Technician II	2015-4603
Junior Cyber Application Engineer	30082 - Engineering Technician II	2015-4603
Junior Cyber Intrusion Analyst	14103 - Computer Systems Analyst III	2015-4603
Junior Cyber Threat Analyst (ACTA)	14103 - Computer Systems Analyst III	2015-4603

The Service Contract Labor Standards, formerly the Service Contract Act (SCA), apply to this contract and it includes SCLS applicable labor categories. Labor categories and fixed price services marked with a (**) in this pricelist are based on the U.S. Department of Labor Wage Determination Number(s) identified in the SCLS/ SCA matrix. The prices awarded are in line with the geographic scope of the contract (i.e., nationwide).

Labor Category Descriptions

Lcat Title	Description
Senior Cyber/System Engineer	The Senior System Engineer shall have the ability to advise Government personnel on streamlined processes and techniques for conducting the items listed below. This individual shall act as a subject matter expert (SME) in the following areas: • Experience with Windows server & desktop • Experience with VMWare Elastic Sky X Integrated (ESXi) • Preferred experience in Python • Preferred experience with the development and update of procedures for IT tasks • Experience with configuration and administration of cloud services and infrastructure • Preferred experience with Splunk and MISP • Preferred experience in managing distributed deployment architecture, index clusters, and search head clusters for Splunk • Preferred ability to manage and develop custom sourcetypes and dashboards for Splunk • Administration of Linux platforms • Administration of Active Directory and DNS • Ability to manage routed network architecture, firewalls, switches, and VPNs • Experience in the cyber security and Network Operations field • Strong technical and consulting skills in one or more of the following specialties: - Cyber Intelligence Analysis - IP Networking - Intrusion Detection - Incident Response - IT System Administration - Federal Law Enforcement, Military, or Intelligence disciplines - Security Information Management - Penetration Testing - Computer Forensics - Familiarity of tools used in incident detection and handling • Understanding of network protocols, network devices, computer security devices, or system administration in support of network and network security operations Experience working in teams and possess strong written and verbal communication skills

Mid Cyber/Systems Engineer	This individual shall act as a lead in the following areas: • Experience with Windows server & desktop • Experience with VMWare Elastic Sky X Integrated (ESXi) • Preferred experience in Python • Preferred experience with the development and update of procedures for IT tasks • Experience with configuration and administration of cloud services and infrastructure • Preferred experience with Splunk and MISP • Preferred experience in managing distributed deployment architecture, index clusters, and search head clusters for Splunk • Preferred ability to manage and develop custom sourcetypes and dashboards for Splunk • Administration of Linux platforms • Administration of Active Directory and DNS • Ability to manage routed network architecture, firewalls, switches, and VPNs • Experience in the cyber security and Network Operations field • Strong technical and consulting skills in one or more of the following specialties: - Cyber Intelligence Analysis - IP Networking - Intrusion Detection - Incident Response - IT System Administration - Federal Law Enforcement, Military, or Intelligence disciplines - Security Information Management - Penetration Testing - Computer Forensics - Familiarity of tools used in incident detection and handling • Understanding of network protocols, network devices, computer security devices, or system administration in support of network and network security operations Experience working in teams and possess strong written and verbal communication skills

Junior Cyber/System Engineer	This individual shall demonstrate experience in the following areas: • Experience with Windows server & desktop • Experience with VMWare Elastic Sky X Integrated (ESXi) • Preferred experience in Python • Preferred experience with the development and update of procedures for IT tasks • Experience with configuration and administration of cloud services and infrastructure • Preferred experience with Splunk and MISP • Preferred experience in managing distributed deployment architecture, index clusters, and search head clusters for Splunk • Preferred ability to manage and develop custom sourcetypes and dashboards for Splunk • Administration of Linux platforms • Administration of Active Directory and DNS • Ability to manage routed network architecture, firewalls, switches, and VPNs • Experience in the cyber security and Network Operations field • Strong technical and consulting skills in one or more of the following specialties: - Cyber Intelligence Analysis - IP Networking - Intrusion Detection - Incident Response - IT System Administration - Federal Law Enforcement, Military, or Intelligence disciplines - Security Information Management - Penetration Testing - Computer Forensics - Familiarity of tools used in incident detection and handling • Understanding of network protocols, network devices, computer security devices, or system administration in support of network and network security operations • Experience working in teams and possess strong written and verbal communication skills
Senior Cyber Application Engineer	The Senior Cyber Application Engineer shall have the ability to advise Government personnel on streamlined processes and techniques for conducting the items listed below. This individual shall act as a subject matter expert (SME) in the following areas: • 3-5+ years (103 Jr.) of Splunk development experience supporting data analytics • Extensive Splunk administration experience, including managing distributed deployment architecture, index clusters, and search head clusters • Extensive Splunk development experience creating dashboards, reports, and complex custom queries • Ability to manage and develop custom sourcetypes and dashboards for Splunk • Experience normalizing disparate data sets, integrating multiple data streams and feeds from networks and infrastructure services, into near real-time dashboards for use in analysis • Experience creating and managing Splunk knowledge objects • Experience with MISP • Experience with Apache, Docker, Structure Query Language (SQL) Server, • Experience in Python, Hypertext Preprocessor (PHP), and JavaScript Experience with configuration and administration of cloud services and infrastructure

Mid Cyber Application Engineer	This individual shall act as a lead in the following areas: • 3-5+ years (103 Jr.) of Splunk development experience supporting data analytics • Extensive Splunk administration experience, including managing distributed deployment architecture, index clusters, and search head clusters • Extensive Splunk development experience creating dashboards, reports, and complex custom queries • Ability to manage and develop custom sourcetypes and dashboards for Splunk • Experience normalizing disparate data sets, integrating multiple data streams and feeds from networks and infrastructure services, into near real-time dashboards for use in analysis • Experience creating and managing Splunk knowledge objects • Experience with MISP • Experience with Apache, Docker, Structure Query Language (SQL) Server, • Experience in Python, Hypertext Preprocessor (PHP), and JavaScript Experience with configuration and administration of cloud services and infrastructure
Junior Cyber Application Engineer	This individual shall demonstrate experience in the following areas: • 3-5+ years (103 Jr.) of Splunk development experience supporting data analytics • Extensive Splunk administration experience, including managing distributed deployment architecture, index clusters, and search head clusters • Extensive Splunk development experience creating dashboards, reports, and complex custom queries • Ability to manage and develop custom sourcetypes and dashboards for Splunk • Experience normalizing disparate data sets, integrating multiple data streams and feeds from networks and infrastructure services, into near real-time dashboards for use in analysis • Experience creating and managing Splunk knowledge objects • Experience with MISP • Experience with Apache, Docker, Structure Query Language (SQL) Server, • Experience in Python, Hypertext Preprocessor (PHP), and JavaScript Experience with configuration and administration of cloud services and infrastructure

Senior Cyber Intrusion Analyst	The Senior Cyber Intrusion Analyst shall have the ability to advise Government personnel on streamlined processes and techniques for conducting the items listed below. This individual shall act as a subject matter expert (SME) in the following areas: • Experience drafting and reviewing analytical products • Experience conducting all source research and link analysis in a cyber threat hunting context • Conduct research, binary analysis, and reverse engineering of suspicious and malicious software to determine functionality, complexity, and impact of its implementation on victim/compromised systems of interest • Link and correlate digital information, such as, threat data (victim/source IP addresses, URL, malicious software), actor contacts or personal data, system logs, obtained from single or multiple sources and develop attribution • Experience with analysis of security and event logs, web logs, 0365 logs, and net flow data • sysExperience analyzing cyber intrusion activities • Conduct analysis using open source and provided technologies and threat intelligence to make recommendations on analytical procedures for NDCA to address cyber threats and vulnerabilities targeting U.S. interests • Experience in the analysis and recovery of encrypted and plaintext passwords or secure keys; identify software programs, hidden rootkit activity, hidden or clear network traffic information, active registry hives, specific command lines, and other system activity • Experience participating in tactical and strategic collaboration, teaming, and coordination opportunities • Experience with Splunk conducting cyber threat hunting or data analytics • Ability to brief analytical findings to a variety of audiences • All Analysts must be able to participate in workshops, briefings and all other programs which provide a foundation for the analyst to gain better insight on bureau matters, other government agency matters, private sector and/or other matters which would enhance the employees' subject matter expertise as it pertains to cyber Additional duties as determined by the government

Mid Cyber Intrusion Analyst	This individual shall act as a lead in the following areas: • Experience drafting and reviewing analytical products • Experience conducting all source research and link analysis in a cyber threat hunting context • Conduct research, binary analysis, and reverse engineering of suspicious and malicious software to determine functionality, complexity, and impact of its implementation on victim/compromised systems of interest • Link and correlate digital information, such as, threat data (victim/source IP addresses, URL, malicious software), actor contacts or personal data, system logs, obtained from single or multiple sources and develop attribution • Experience with analysis of security and event logs, web logs, 0365 logs, and net flow data • Experience analyzing cyber intrusion activities • Conduct analysis using open source and provided technologies and threat intelligence to make recommendations on analytical procedures for NDCA to address cyber threats and vulnerabilities targeting U.S. interests • Experience in the analysis and recovery of encrypted and plaintext passwords or secure keys; identify software programs, hidden rootkit activity, hidden or clear network traffic information, active registry hives, specific command lines, and other system activity • Experience participating in tactical and strategic collaboration, teaming, and coordination opportunities • Experience with Splunk conducting cyber threat hunting or data analytics • Ability to brief analytical findings to a variety of audiences • All Analysts must be able to participate in workshops, briefings and all other programs which provide a foundation for the analyst to gain better insight on bureau matters, other government agency matters, private sector and/or other matters which would enhance the employees' subject matter expertise as it pertains to cyber • Additional duties as determined by the government

Junior Cyber Intrusion Analyst	This individual shall demonstrate experience in the following areas: • Experience drafting and reviewing analytical products • Experience conducting all source research and link analysis in a cyber threat hunting context • Conduct research, binary analysis, and reverse engineering of suspicious and malicious software to determine functionality, complexity, and impact of its implementation on victim/compromised systems of interest • Link and correlate digital information, such as, threat data (victim/source IP addresses, URL, malicious software), actor contacts or personal data, system logs, obtained from single or multiple sources and develop attribution • Experience with analysis of security and event logs, web logs, 0365 logs, and net flow data • Experience analyzing cyber intrusion activities • Conduct analysis using open source and provided technologies and threat intelligence to make recommendations on analytical procedures for NDCA to address cyber threats and vulnerabilities targeting U.S. interests • Experience in the analysis and recovery of encrypted and plaintext passwords or secure keys; identify software programs, hidden rootkit activity, hidden or clear network traffic information, active registry hives, specific command lines, and other system activity • Experience participating in tactical and strategic collaboration, teaming, and coordination opportunities • Experience with Splunk conducting cyber threat hunting or data analytics • Ability to brief analytical findings to a variety of audiences • All Analysts must be able to participate in workshops, briefings and all other programs which provide a foundation for the analyst to gain better insight on bureau matters, other government agency matters, private sector and/or other matters which would enhance the employees' subject matter expertise as it pertains to cyber • Additional duties as determined by the government

Senior/Advanced Cyber Threat Analyst (ACTA)	The Senior/Advanced Cyber Threat Analyst shall have the ability to advise Government personnel on streamlined processes and techniques for conducting the items listed below. This individual shall act as a subject matter expert (SME) in the following areas: • Experience analyzing cyber intrusion activities • Experience participating in tactical and strategic collaboration, teaming, and coordination opportunities • Ability to provide subject matter information and context in briefings, discussions with subject matter experts • Experience in research, review, and analysis of intelligence information • Experience in providing tactical analysis • Experience conducting all source research, link analysis • Experience with analysis of network logs, security logs, web logs, 0365 logs, and net flow data • Experience analyzing cyber intrusion activities • Ability to identify and report new issues, trends, patterns, intelligence gaps, and anomalies • Experience in the exploitation of intelligence information derived from cases/operations • Experience preparing full scope intelligence products such as intelligence notes, briefings, and other consumer-driven investigative/intelligence report • Experience applying analytical expertise to formulate conclusions or recommendations • Experience in compiling and disseminating targeting packages • Ability to brief analytical findings to a variety of audiences
Mid Cyber Threat Analyst (ACTA)	This individual shall act as a lead in the following areas: • Experience analyzing cyber intrusion activities • Experience participating in tactical and strategic collaboration, teaming, and coordination opportunities • Ability to provide subject matter information and context in briefings, discussions with subject matter experts • Experience in research, review, and analysis of intelligence information • Experience in providing tactical analysis • Experience conducting all source research, link analysis • Experience with analysis of network logs, security logs, web logs, 0365 logs, and net flow data • Experience analyzing cyber intrusion activities • Ability to identify and report new issues, trends, patterns, intelligence gaps, and anomalies • Experience in the exploitation of intelligence information derived from cases/operations • Experience preparing full scope intelligence products such as intelligence notes, briefings, and other consumer-driven investigative/intelligence report • Experience applying analytical expertise to formulate conclusions or recommendations • Experience in compiling and disseminating targeting packages • Ability to brief analytical findings to a variety of audiences

Junior Cyber Threat Analyst (ACTA)	This individual shall demonstrate experience in the following areas: • Experience analyzing cyber intrusion activities • Experience participating in tactical and strategic collaboration, teaming, and coordination opportunities • Ability to provide subject matter information and context in briefings, discussions with subject matter experts • Experience in research, review, and analysis of intelligence information • Experience in providing tactical analysis • Experience conducting all source research, link analysis • Experience with analysis of network logs, security logs, web logs, 0365 logs, and net flow data • Experience analyzing cyber intrusion activities • Ability to identify and report new issues, trends, patterns, intelligence gaps, and anomalies • Experience in the exploitation of intelligence information derived from cases/operations • Experience preparing full scope intelligence products such as intelligence notes, briefings, and other consumer-driven investigative/intelligence report • Experience applying analytical expertise to formulate conclusions or recommendations • Experience in compiling and disseminating targeting packages • Ability to brief analytical findings to a variety of audiences
Executive Consultant	Responsible for providing unique functional expertise necessary to interpret requirements, ensure responsiveness and achieve successful performance. Individual maintains a comprehensive knowledge of the statement of work areas and the ability to perform in these areas.
Program Manager	Responsible for day to day management of specific contract support, involving multiple projects and groups of personnel at multiple locations Demonstrates written and oral communication skills, Establishes corporate management structure to direct effective contract support activities.
Project Manager	Responsible for effectively managing funds and personnel ensuing quality and on-time delivery of contractual items. Provides client interface and response, as well as interface to contractual, and company business issues. Ensures required resources including manpower and facilities are available for program implementation and establishes proper relationship between customer, teaming partner and vendors to facilitate the delivery of enginemen services.
Engineer Advanced VI	Responsible for leading and executing extensive engineering/scientific support on systems, system elements, interfacing systems, components, devices and/or processes for complex developmental and operational system programs. Possesses in-depth technical and theoretical knowledge. Capable of working independently, as a team member, or leading teams/task to solve engineering/scientific problems. May include daily supervisionand direction to support team
Engineer/Scientist VI	Responsible for requirements analysis, cost performance trade-off analysis, feasibility analysis, regulatory compliance support, technology conceptual design and special studies and analysis. May include some supervisory role requirements.
Engineer/Scientist V	Responsible for requirements analysis, cost performance trade-off analysis, feasibility analysis, regulatory compliance support, technology conceptual design and special studies and analysis. May include some supervisory role requirements.
Engineer/Scientist IV	Responsible for requirements analysis, cost performance trade-off analysis, feasibility analysis, regulatory compliance support, technology conceptual design and special studies and analysis

Engineer/Scientist III	Responsible for requirements analysis, cost performance trade-off analysis, feasibility analysis, regulatory compliance support, technology conceptual design and special studies and analysis
Engineer/Scientist II	Responsible for requirements analysis, cost performance trade-off analysis, feasibility analysis, regulatory compliance support, technology conceptual design and special studies and analysis
Engineer/Scientist I	Responsible for requirements analysis, cost performance trade-off analysis, feasibility analysis, regulatory compliance support, technology conceptual design and special studies and analysis
Senior Principal Investigator	Responsible for the management and integrity of the design, conduct, and reporting of the research project and for managing, monitoring, and ensuring the integrity of any collaborative relationships. Knowledgeable in all technical aspects of the application and capable of leading the research effort. Additionally, responsible for the direction and oversight of compliance, personnel, and other related aspects of the research project
Engineer Advanced V	Responsible for leading and executing extensive engineering/scientific support on systems, system elements, interfacing systems, components, devices and/or processes for complex developmental and operational system program. Provide in-depth technical and theoretical knowledge. Capable of working independently, as a team member, or leading teams/task to solve engineering/scientific problems. May include daily supervision and direction to support team
Engineer Basic	Responsible for assisting in the executing engineering support tasks. Assists with implementing the engineering requirements across the program acquisition life cycle. Follows established procedures, and solves routine problems.
Electrical Design Engineer II	Responsible for providing technical leadership on engineering related projects; managing high complexity multi·task efforts; briefing or leading strategic level client meetings; leading design or implementation efforts of programs, projects or tasks; ability to serve as primary interface with client management personnel regarding strategic issues; and ensure work products adhere to customer requirements
Software Engineer III	Responsible for Providing technical analysis or support to programs, projects or tasks and performs a variety of engineering tasks, either independently or under supervision, which is broad in nature. These efforts may include design and implementation, including personnel, hardware, software and support facilities and/or equipment
Security & Information Processing Specialist	Responsible for document control, physical security, personnel security, or computer security with experience revising or updating security measures due to new or revised regulations. Establish measures and procedures for handling, storing, safekeeping, and destroying classified records and documents.
Program Analyst IX	Responsible for providing technical analysis or support to programs, projects or tasks and performs a variety of engineering tasks, either independently or under supervision, which is broad in nature. These efforts may include design, and implementation including personnel, hardware, software and support facilities and/or !equipment. Additional areas may include oversight of project or task deliverables. Support Engineer/Scientists as required and perform other duties as assigned.

Program Analyst IV	Responsible for providing technical analysis or support to programs, projects or tasks and performs a variety of engineering tasks, either independently or under supervision, which is broad in nature. These efforts may include design, and implementation including personnel, hardware, software and support facilities and/or equipment. Additional areas may include oversight of project or task deliverables. Support Engineer/Scientists as required and perform other duties as assigned
Program Analyst	Responsible for applying appropriate scientific and engineering processes and modeling techniques to the development of systems, Performs analysis and studies related to operational issues and reviews test plans to meet the applicable requirements