REDCEDAR
TECHNOLOGY GROUP

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

Contract Number:	47QTCA24D0087
Contract Period:	23 APR 2024 – 22 APR 2029
Business Size:	8(a) Small Disadvantaged Business
Special Item Number (SIN):	511210, 512180C, 54151, 54151HACS, 54151S, 541519ICAM, OLM

Schedule Title: Multiple Award Schedule
Federal Supply Group: Information Technology

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

For more information on ordering go to the following website: https://www.gsa.gov/schedules.

Red Cedar TG-MTE, LLC
2115 Stephens Place, Suite 310
New Braunfels, TX 78130
(830) 549-3111
https://redcedartg.com/
RCTG-Biz@redcedartg.com

Contract Administrator:
Steven McDonald (steven.mcdonald@redcedartg.com)

NAOB

SBA U.S. Small Business Administration 8(a) CERTIFIED

ISBEE Certified

Pricelist current through Modification PS-0017, effective 09/02/2026

TABLE OF CONTENTS

CONTRACTOR INFORMATION 1
SIN 511210 SOFTWARE TERM LICENSING 4
SIN 518210C CLOUD COMPUTING & RELATED IT SERVICES 10
SIN 54151 SOFTWARE MAINTENANCE SERVICES 24
SIN 54151HACS HIGHLY ADAPTIVE CYBERSECURITY SERVICES 26
SIN 54151S PROFESSIONAL IT SERVICES 47
SIN 541519ICAM IDENTITY, CREDENTIALING & ACCESS MANAGEMENT 87

Offerors and Agencies are advised that the Multiple Award Schedules (MAS) contract is not to be used to procure services which properly fall under the Brooks Act. These services include, but are not limited to, architecture, engineering, mapping, cartographic production, remote sensing, geographic information systems, and related services. FAR 36.6 distinguishes between mapping services of an A/E nature and mapping services which are not connected nor incidental to the traditionally accepted A/E Services.

CONTRACTOR INFORMATION

1a. Table of Awarded Special Item Number(s) with appropriate cross-reference to page numbers:

SIN	SIN Description	Page
511210	Software Term Licensing	4
518210C	Cloud Computing and Related IT Professional Services	10
54151	Software Maintenance Services	24
54151HACS	Highly Adaptive Cybersecurity Services (HACS)	26
54151S	Professional Information Technology Services	47
541519ICAM	Identity, Credentialing and Access Management (ICAM)	87
OLM	Order-Level Materials (OLMs)	N/A

1b. Identification of the lowest priced model number and lowest unit price for that model for each special item number awarded in the contract. See pricing beginning on page 4.

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, indicate "Not applicable" for this item. See labor category descriptions beginning on page 11.

2. Maximum Order:

SIN 511210:	$500,000
SIN 518210C:	$500,000
SIN 54151:	$500,000
SIN 54151HACS:	$500,000
SIN 54151S:	$500,000
SIN 541519ICAM:	$1,000,000
SIN OLM:	$250,000

3. Minimum Order: $100.00

4. Geographic Coverage: Domestic.

5. Point(s) of production: Same as company address.

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

7. Quantity discounts: Not Applicable.

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: None**.**

10a. Time of Delivery: Specified on the Task Order.

10b. Expedited Delivery: Contact Contractor.

10c. Overnight and 2-day delivery: Contact Contractor.

10d. Urgent Requirements: Contact Contractor.

11. F.O.B Points: Destination.

12a. Ordering Address: Contract Management
2115 Stephens Place, Suite 310
New Braunfels, TX 78130
(P) 830-549-3111
RCTG-Biz@redcedartg.com

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

13. Payment address (is): Red Cedar TG-MTE, LLC
ATTN: Accounting
2115 Stephens Place, Suite 310
New Braunfels, TX 78130
(P) 830-549-3111
MTEA.AP-AR@mteauthority.com

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

15. Export Packing Charges: Not Applicable.

16. Terms and conditions of rental, maintenance, and repair: Not Applicable.

17. Terms and conditions of installation: Not Applicable.

18a. Terms and conditions of repair parts: Not Applicable.

18b. Terms and conditions for any other services: Not Applicable.

19. List of service and distribution points: Not Applicable.

20. List of participating dealers: Not Applicable.

21. Preventive maintenance: Not Applicable.

22a. Environmental attributes, e.g., recycled content, energy efficiency, and/or reduced pollutants:
Not Applicable.

22b. If applicable, indicate that Section 508 compliance information is available for the information and communications technology (ICT) products and services and show where full details can be found (e.g. contractor's website or other location.) ICT accessibility standards can be found at: https:// Section508.gov/.
Not Applicable.

23. Unique Entity Identifier (UEI) Number: M9XRJJKC8DS4

24. Notification regarding registration in System for Award Management (SAM) database:
Red Cedar TG-MTE, LLC is registered at SAM.gov.

SIN 511210 SOFTWARE TERM LICENSING

OEM	PART NUMBER	DESCRIPTION	PRICE
WSO2	P-API-AP-QA-R	WSO2 API Manager: Analytics Profile (Pre-Prod Renewal Only)	$378.55
WSO2	P-API-AP-R	WSO2 API Manager: Analytics Profile (Renewal Only)	$1,514.23
WSO2	P-EI-BP-QA-R	WSO2 Enterprise Integrator: Business Process Profile (Pre-Prod Renewal Only)	$5,847.41
WSO2	P-EI-BP-R	WSO2 Enterprise Integrator: Business Process Profile (Renewal Only)	$23,389.65
WSO2	SUB-API-CP	WSO2 API Platform Subscription (Per Core)	$13,554.86
WSO2	SUB-API-BASE	WSO2 API Platform Base Fee	$6,188.57
WSO2	SUB-API-API	WSO2 API Platform Subscription (Per API)	$1,863.69
WSO2	SUB-API-TX	WSO2 API Platform (Per MTx)	$113.81
WSO2	SUB-EI	WSO2 Enterprise Integrator Subscription (Per Core)	$13,972.04
WSO2	SUB-IS-I	WSO2 Identity Server Subscription - Internal (Per Core)	$17,810.45
WSO2	SUB-IS-E	WSO2 Identity Server Subscription - External (Per Core)	$22,143.74
WSO2	SUB-IS-IE	WSO2 Identity Server Subscription - Int+Ext (Per Core)	$27,952.09
WSO2	SUB-INT	WSO2 Integrator Subscription (Per Integration)	$2,788.41
WSO2	SUB-IS-B2C	WSO2 Identity Server Subscription B2C (Per Core)	$21,436.90
WSO2	SUB-IS-B2B	WSO2 Identity Server Subscription B2B (Per Core)	$22,472.59
WSO2	SUB-IS-B2E	WSO2 Identity Server Subscription B2E (Per Core)	$17,261.93
WSO2	SUB-IS-B2C+B	WSO2 Identity Server Subscription B2C+B2B (Per Core)	$27,014.95
WSO2	SUB-IS-B2C+E	WSO2 Identity Server Subscription B2C+B2E (Per Core)	$24,391.34
WSO2	SUB-IS-B2B+E	WSO2 Identity Server Subscription B2B+B2E (Per Core)	$25,421.95
WSO2	SUB-IS-B2C+B+E	WSO2 Identity Server Subscription B2B+B2C+B2E (Per Core)	$31,453.45
WSO2	SLA-E	WSO2 Enterprise Support Plan	$48,312.33
WSO2	Dev-25	Subscription Query Support - 25 Hours	$7,876.87
WSO2	SUB-API-DP	API Portal & MCP Hub	$4,352.64
WSO2	SUB-API-CP-B1	API Control Plane (Managed Interfaces / APIs) - Band 1	$957.18
WSO2	SUB-API-CP-B2	API Control Plane (Managed Interfaces / APIs) - Band 2	$821.16
WSO2	SUB-API-CP-B3	API Control Plane (Managed Interfaces / APIs) - Band 3	$644.84
WSO2	SUB-API-CP-FED-B1	API Control Plane (Federated Interfaces / APIs) - Band 1	$473.55

OEM	PART NUMBER	DESCRIPTION	PRICE
WSO2	SUB-API-CP-FED-B2	API Control Plane (Federated Interfaces / APIs) - Band 2	$413.10
WSO2	SUB-API-CP-FED-B3	API Control Plane (Federated Interfaces / APIs) - Band 3	$322.42
WSO2	SUB-API-APIGW-B1	Gateway Events (Managed) - Band 1	$352.64
WSO2	SUB-API-APIGW-B2	Gateway Events (Managed) - Band 2	$332.49
WSO2	SUB-API-APIGW-B3	Gateway Events (Managed) - Band 3	$302.27
WSO2	SUB-INT-INT-B1	WSO2 Integrator Integrations - Band 1	$1,088.16
WSO2	SUB-INT-INT-B2	WSO2 Integrator Integrations - Band 2	$1,007.56
WSO2	SUB-INT-INT-B3	WSO2 Integrator Integrations - Band 3	$896.73
WSO2	SUB-INT-TX-B1	WSO2 Integration Transactions - Band 1	$1,088.16
WSO2	SUB-INT-TX-B2	WSO2 Integration Transactions - Band 2	$806.05
WSO2	SUB-INT-TX-B3	WSO2 Integration Transactions - Band 3	$503.78
WSO2	SUB-INT-AM-B1	WSO2 Integration Automation Core Minutes - Band 1	$957.18
WSO2	SUB-INT-AM-B2	WSO2 Integration Automation Core Minutes - Band 2	$418.14
WSO2	SUB-INT-AM-B3	WSO2 Integration Automation Core Minutes - Band 3	$342.57
WSO2	SUB-INT-AIAGENT-B1	WSO2 AI Agents - Band 1	$1,088.16
WSO2	SUB-INT-AIAGENT-B2	WSO2 AI Agents - Band 2	$1,007.56
WSO2	SUB-INT-AIAGENT-B3	WSO2 AI Agents - Band 3	$886.65
WSO2	SUB-INT-AIACTION-B1	WSO2 AI Agent Actions - Band 1	$1,057.93
WSO2	SUB-INT-AIACTION-B2	WSO2 AI Agent Actions - Band 2	$654.91
WSO2	SUB-INT-AIACTION-B3	WSO2 AI Agent Actions - Band 3	$539.04
WSO2	SUB-PRE	Pre-Production Environment	$2,015.11





SIN 511210 SOFTWARE TERM LICENSING INFORMATION

1. Inspection / Acceptance

The Contractor shall only tender for acceptance those items that conform to the requirements of this contract. The ordering activity reserves the right to inspect or test any software that has been tendered for acceptance. The ordering activity may require repair or replacement of nonconforming software at no increase in contract price. The ordering activity must exercise its post acceptance rights (1) within a reasonable time after the defect was discovered or should have been discovered; and (2) before any substantial change occurs in the condition of the software, unless the change is due to a defect in the software.

2. Guarantee / Warranty

The Contractor warrants that:

- Services will be performed in a timely, workmanlike and professional manner with reasonable skill and care and in accordance with sound and generally accepted industry standards and practices and in accordance with any and all applicable laws, codes, rules, regulations or other governmental or regulatory requirements,
- It has and will maintain all necessary licenses, consents, and permissions necessary for the performance of its obligations under this Agreement,
- The Services and Products will not violate the patent, copyright, trademark, trade secrets or other proprietary or intellectual property rights of any third party,
- The Products and/or Services will not contain or transmit to Customer any Harmful Code. Harmful Code means viruses, worms, time bombs, Trojan horses and other malicious code, files, scripts, agents, or programs.

3. Software Maintenance

Software Maintenance as a product (SIN 511210) includes the publishing of bug/defect fixes via patches and updates/upgrades in function and technology to maintain the operability and usability of the software product. It may also include other no charge support that are included in the purchase price of the product in the commercial marketplace. No charge support includes items such as user blogs, discussion forums, on-line help libraries and FAQs (Frequently Asked Questions), hosted chat rooms, and limited telephone, email and/or web-based general technical support for user's self-diagnostics.

Software maintenance as a product does NOT include the creation, design, implementation, integration, etc. of a software package. These examples are considered software maintenance as a service. Software Maintenance as a product is billed at the time of purchase.

4. Periods of Term Licenses (SIN 511210)

- The Contractor will honor orders for periods for the duration of the contract period or a lessor period of time.
- Term licenses and/or maintenance may be discontinued by the ordering activity on thirty (30) calendar days written notice to the Contractor.
- Annual Funding. When annually appropriated funds are cited on an order for term licenses and/or maintenance, the period of the term licenses and/or maintenance shall automatically expire on September 30 of the contract period, or at the end of the contract period, whichever occurs first. Renewal of the term licenses and/or maintenance orders citing the

new appropriation shall be required, if the term licenses and/or maintenance is to be continued during any remainder of the contract period.

- Cross-Year Funding Within Contract Period. Where an ordering activity's specific appropriation authority provides for funds in excess of a 12-month (fiscal year) period, the ordering activity may place an order under this schedule contract for a period up to the expiration of the contract period, notwithstanding the intervening fiscal years.
- Ordering activities should notify the Contractor in writing thirty (30) calendar days prior to the expiration of an order, if the term licenses and/or maintenance is to be terminated at that time. Orders for the continuation of term licenses and/or maintenance will be required if the term licenses and/or maintenance is to be continued during the subsequent period.

1. Conversion from Term License to Perpetual License

Conversions of term licenses to perpetual licenses is not available.

2. Term License Cessation

Software product term licenses are valid for a period of 12 months and will require the Customer to renew.

3. Utilization Limitations – (SIN 511210)

a. Software acquisition is limited to commercial computer software defined in FAR Part 2.101.
b. When acquired by the ordering activity, commercial computer software and related documentation legend shall be subject to the following:
   i. Software licenses are by site and by ordering activity. An ordering activity is defined as a cabinet level or independent ordering activity. The software may be used by any subdivision of the ordering activity (service, bureau, division, command, etc.) that has access to the site the software is placed at, even if the subdivision did not participate in the acquisition of the software. Further, the software may be used on a sharing basis where multiple agencies have joint projects that can be satisfied by the use of the software placed at one ordering activity's site. This would allow other agencies access to one ordering activity's database. For ordering activity public domain databases, user agencies and third parties may use the computer program to enter, retrieve, analyze, and present data. The user ordering activity will take appropriate action by instruction, agreement, or otherwise, to protect the Contractor's proprietary property with any third parties that are permitted access to the computer programs and documentation in connection with the user ordering activity's permitted use of the computer programs and documentation. For purposes of this section, all such permitted third parties shall be deemed agents of the user ordering activity.
   ii. Except as is provided above, the ordering activity shall not provide or otherwise make available the software or documentation, or any portion thereof, in any form, to any third party without the prior written approval of the Contractor. Third parties do not include prime Contractors, subcontractors and agents of the ordering activity who have the ordering activity's permission to use the licensed software and documentation at the facility, and who have agreed to use the licensed software and documentation only in accordance with these restrictions. This provision does not limit the right of the ordering activity to use software, documentation, or information therein, which the ordering activity may already have or obtain without restrictions.

iii. The ordering activity shall have the right to use the computer software and documentation with the computer for which it is acquired at any other facility to which that computer may be transferred, or in cases of Disaster Recovery, the ordering activity has the right to transfer the software to another site if the ordering activity site for which it is acquired is deemed to be unsafe for ordering activity personnel; to use the computer software and documentation with a backup computer when the primary computer is inoperative; to copy computer programs for safekeeping (archives) or backup purposes; to transfer a copy of the software to another site for purposes of benchmarking new hardware and/or software; and to modify the software and documentation or combine it with other software, provided that the unmodified portions shall remain subject to these restrictions.

iv. "Commercial Computer Software" may be marked with the Contractor's standard commercial restricted rights legend, but the schedule contract and schedule pricelist, including this clause, "Utilization Limitations" are the only governing terms and conditions and shall take precedence and supersede any different or additional terms and conditions included in the standard commercial legend.

4. Right-To-Copy Pricing

Discounted pricing for right-to-copy licenses is not available for the offerings provided.

WSO2 INFORMATION

WSO2, LLC (WSO2) is well-known by professional developers who take advantage of software-oriented architecture (SOA). WSO2 has developed open-source applications and is an enterprise platform that, in addition to offering total integration, allows consumers to use it to create, integrate, manage, protect, and analyze their APIs, applications and web services. WSO2 also offers IoT and Cloud solutions tailored to every need. WSO2 products are designed to provide the necessary innovation and agility for the network of systems of any customer or environment to be efficient. All products have been designed with the purpose of accompanying the digital transformation and are 100% open source. Furthermore, they stand out due to their compatibility with other components thanks to the extensive use of open communication standards and work perfectly well with each other as a single platform. The most important sets of products are as follows:

5. API Manager

WSO2's API Manager (APIM) is the home of security and governance components, protecting your people, data, and systems. WSO2 APIM is an open-source solution, providing customers all the freedom needed to change direction and scope. At the same time, the product fully supports API publishing, lifecycle management, application development, access control, rate limiting, monetization, and analytics. WSO2 APIM is the home of security and governance components, protecting users, data, and systems. WSO2 APIM is an all-in-one solution that provides:

- Design, compose and publish APIs through the API publisher
- Share APIs with customers and partners in the API store
- Create a proxy for backend services and controls functions such as security and analytics
- Speed up the response time to service API calls

- Monitor the way APIs are used at operation and business levels and monitor system behavior
- Allow APIs to be used by different applications in the safest way possible

6. Identity Manager

WSO2 Identity Server (IS) adds a security layer to existing IT infrastructure, making customer processes run smoothly. Combine safety with usability to connect to new applications whenever it's needed. WSO2 IS guards dataflows so that only the users with the correct credentials gain access to the right systems. This provides a fast, flexible and trustworthy IdAM/ICAM all-in-one solution that provides:

- Provide a unified SSO experience through multiple SSO protocols
- Strengthen authentication by combining multiple identification methods
- Deploy role-based (RBAC) and attribute-based access control (ABAC) to secure access to APIs
- Combine monitoring, reporting and auditing tools in one solution
- Connect to any other system with the IS connectors

7. Enterprise Integrator

Enterprise Integration (EI) isn't only about ESBs.. The WSO2 Enterprise Integrator (EI) brings power and speed through an open-source integration platform to align all systems and applications within a customer's organization with an Enterprise Service Bus (ESB) and microservices. It enables customers to connect and transform data between legacy systems, SaaS applications, services, and APIs, providing customers with all the capabilities of a connected digital architecture. The EI package includes runtime for data and service integration, messaging, and business process execution, microservices, and analytics. The WSO2 EI is an all-in-one solution that provides:

- Connect and expose any data store as a service
- World-class systems, services, and protocol support
- Use for messaging, service, and as a security gateway
- Route, mediate, and transform data
- Achieve high performance, high availability, scalability, and stability
- Ensure lightweight, developer-friendly, and easy deployment
- Manage, deploy, view, and execute business processes
- Manage, monitor, and analyze

SIN 518210C CLOUD COMPUTING & RELATED IT SERVICES

ID NUMBER	LCAT DESCRIPTION	YEAR 2 *04/2025*	YEAR 3 *04/2026*	YEAR 4 *04/2027*	YEAR 5 *04/2028*
03011094	Cloud Administrator I	$85.40	$88.82	$92.37	$96.06
03011095	Cloud Administrator II	$97.85	$101.76	$105.83	$110.06
03011096	Cloud Administrator III	$127.40	$132.50	$137.80	$143.31
03011097	Cloud Administrator IV	$161.11	$167.55	$174.25	$181.22
03011098	Cloud Analyst I	$79.98	$83.18	$86.51	$89.97
03011099	Cloud Analyst II	$100.45	$104.47	$108.65	$113.00
03011100	Cloud Analyst III	$122.10	$126.98	$132.06	$137.34
03011101	Cloud Analyst IV	$149.99	$155.99	$162.23	$168.72
03011102	Cloud Architect I	$99.50	$103.48	$107.62	$111.92
03011103	Cloud Architect II	$118.43	$123.17	$128.10	$133.22
03011104	Cloud Architect III	$146.72	$152.59	$158.69	$165.04
03011105	Cloud Architect IV	$178.88	$186.04	$193.48	$201.22
03011106	Cloud Developer I	$93.98	$97.74	$101.65	$105.72
03011107	Cloud Developer II	$114.56	$119.14	$123.91	$128.87
03011108	Cloud Developer III	$141.97	$147.65	$153.56	$159.70
03011109	Cloud Developer IV	$170.68	$177.51	$184.61	$191.99
03011110	Cloud DevOps Engineer I	$95.32	$99.13	$103.10	$107.22
03011111	Cloud DevOps Engineer II	$119.08	$123.84	$128.79	$133.94
03011112	Cloud DevOps Engineer III	$145.75	$151.58	$157.64	$163.95
03011113	Cloud DevOps Engineer IV	$174.26	$181.23	$188.48	$196.02
03011114	Cloud Engineer I	$98.90	$102.86	$106.97	$111.25
03011115	Cloud Engineer II	$117.73	$122.44	$127.34	$132.43
03011116	Cloud Engineer III	$145.93	$151.77	$157.84	$164.15
03011117	Cloud Engineer IV	$169.22	$175.99	$183.03	$190.35
03011118	Cloud Migration Specialist I	$90.88	$94.52	$98.30	$102.23

ID NUMBER	LCAT DESCRIPTION	YEAR 2 *04/2025*	YEAR 3 *04/2026*	YEAR 4 *04/2027*	YEAR 5 *04/2028*
03011119	Cloud Migration Specialist II	$107.52	$111.82	$116.29	$120.94
03011120	Cloud Migration Specialist III	$136.77	$142.24	$147.93	$153.85
03011121	Cloud Migration Specialist IV	$167.68	$174.39	$181.37	$188.62
03011122	Cloud Project Manager I	$94.67	$98.46	$102.40	$106.50
03011123	Cloud Project Manager II	$114.37	$118.94	$123.70	$128.65
03011124	Cloud Project Manager III	$137.74	$143.25	$148.98	$154.94
03011125	Cloud Project Manager IV	$165.84	$172.47	$179.37	$186.54
03011126	Cloud Security Specialist I	$86.74	$90.21	$93.82	$97.57
03011127	Cloud Security Specialist II	$103.65	$107.80	$112.11	$116.59
03011128	Cloud Security Specialist III	$132.13	$137.42	$142.92	$148.64
03011129	Cloud Security Specialist IV	$165.93	$172.57	$179.47	$186.65
03011130	Cloud Subject Matter Expert I	$168.25	$174.98	$181.98	$189.26
03011131	Cloud Subject Matter Expert II	$187.88	$195.40	$203.22	$211.35
03011132	Cloud Subject Matter Expert III	$220.70	$229.53	$238.71	$248.26
03011133	Cloud Subject Matter Expert IV	$227.46	$236.56	$246.02	$255.86
03011134	Cloud Subject Matter Expert V	$261.94	$272.42	$283.32	$294.65
03011135	Cloud Support Specialist I	$59.02	$61.38	$63.84	$66.39
03011136	Cloud Support Specialist II	$71.09	$73.93	$76.89	$79.97
03011137	Cloud Support Specialist III	$80.94	$84.18	$87.55	$91.05
03011138	Cloud Support Specialist IV	$91.95	$95.63	$99.46	$103.44

SIN 512180C LABOR CATEGORY INFORMATION

Experience and Education

The following labor category minimum technical experience tables correspond to the prices offered in this submission.

All SIN 518210C Labor Categories		
Level I	Junior	Bachelor's degree and 0 to 1 year of experience
Level II	Associate	Bachelor's degree and 2 to 4 years of experience
Level III	Senior	Bachelor's degree and 3 to 5 years of experience
Level IV	Master	Master's degree and 5 to 7 years of experience
Level V	Director	Master's degree and 7+ years of experience

Degree Substitution

This serves as a guide to the experience and educational background of personnel typically found in each labor category. However, the experience of a resource is often a valid substitute for education. With this noted, the following information indicates where experience might be substituted for a degree as accepted by the customer.

All SIN 518210C Labor Categories	
Equivalent to Bachelor's (Level I)	Associates degree + 2 or more years of relevant technical experience
	High School diploma + 4 or more years relevant technical experience
Equivalent to Bachelor's (Level II)	Associates degree + 3 or more years of relevant technical experience
	High School diploma + 6 or more years relevant technical experience
Equivalent to Bachelor's (Level III)	Associates degree + 5 or more years of relevant technical experience
	High School diploma + 7 or more years relevant technical experience
Equivalent to Master's (Level IV)	Bachelor's degree + 7 years of relevant technical experience
	Associates degree + 9 or more years of relevant technical experience
	High School diploma + 11 or more years relevant technical experience
Equivalent to Master's (Level V)	Bachelor's degree + 9 or more years of relevant technical experience
	Associates degree + 11 or more years of relevant technical experience

Experience & Degree Substitution Equivalencies

*Experience exceeding the minimum shown may be substituted for education. Likewise, education exceeding the minimum shown may be substituted for experience.

LABOR CATEGORY	STANDARD QUALS		SUBSTITUTIONS				
	Min Education	Min Exp	PhD	Masters	Bachelors	Associates	High School
Cloud Administrator I	Bachelors	0	0	0	0	2	4
Cloud Administrator II	Bachelors	2	0	0	2	3	6
Cloud Administrator III	Bachelors	3	0	1	3	5	7
Cloud Administrator IV	Masters	5	3	5	7	9	11
Cloud Analyst I	Bachelors	0	0	0	0	2	4

LABOR CATEGORY	STANDARD QUALS		SUBSTITUTIONS				
	Min Education	Min Exp	PhD	Masters	Bachelors	Associates	High School
Cloud Analyst II	Bachelors	2	0	0	2	3	6
Cloud Analyst III	Bachelors	3	0	1	3	5	7
Cloud Analyst IV	Masters	5	3	5	7	9	11
Cloud Architect I	Bachelors	0	0	0	0	2	4
Cloud Architect II	Bachelors	2	0	0	2	3	6
Cloud Architect III	Bachelors	3	0	1	3	5	7
Cloud Architect IV	Masters	5	3	5	7	9	11
Cloud Developer I	Bachelors	0	0	0	0	2	4
Cloud Developer II	Bachelors	2	0	0	2	3	6
Cloud Developer III	Bachelors	3	0	1	3	5	7
Cloud Developer IV	Masters	5	3	5	7	9	11
Cloud DevOps Engineer I	Bachelors	0	0	0	0	2	4
Cloud DevOps Engineer II	Bachelors	2	0	0	2	3	6
Cloud DevOps Engineer III	Bachelors	3	0	1	3	5	7
Cloud DevOps Engineer IV	Masters	5	3	5	7	9	11
Cloud Engineer I	Bachelors	0	0	0	0	2	4
Cloud Engineer II	Bachelors	2	0	0	2	3	6
Cloud Engineer III	Bachelors	3	0	1	3	5	7
Cloud Engineer IV	Masters	5	3	5	7	9	11
Cloud Migration Specialist I	Bachelors	0	0	0	0	2	4
Cloud Migration Specialist II	Bachelors	2	0	0	2	3	6
Cloud Migration Specialist III	Bachelors	3	0	1	3	5	7
Cloud Migration Specialist IV	Masters	5	3	5	7	9	11
Cloud Project Manager I	Bachelors	0	0	0	0	2	4
Cloud Project Manager II	Bachelors	2	0	0	2	3	6
Cloud Project Manager III	Bachelors	3	0	1	3	5	7
Cloud Project Manager IV	Masters	5	3	5	7	9	11
Cloud Security Specialist I	Bachelors	0	0	0	0	2	4
Cloud Security Specialist II	Bachelors	2	0	0	2	3	6
Cloud Security Specialist III	Bachelors	3	0	1	3	5	7
Cloud Security Specialist IV	Masters	5	3	5	7	9	11
Cloud SME I	Bachelors	0	0	0	0	2	4
Cloud SME II	Bachelors	2	0	0	2	3	6
Cloud SME III	Bachelors	3	0	1	3	5	7
Cloud SME IV	Masters	5	3	5	7	9	11
Cloud SME V	Masters	7	5	7	9	11	N/A

LABOR CATEGORY	STANDARD QUALS		SUBSTITUTIONS				
	Min Education	Min Exp	PhD	Masters	Bachelors	Associates	High School
Cloud Support Specialist I	Bachelors	0	0	0	0	2	4
Cloud Support Specialist II	Bachelors	2	0	0	2	3	6
Cloud Support Specialist III	Bachelors	3	0	1	3	5	7
Cloud Support Specialist IV	Masters	5	3	5	7	9	11

Place of Performance

The labor categories provided are for both Contractor and Customer facilities.

Clearance

The labor categories provided are for a Secret and below clearance.

Labor Category Descriptions

The descriptions provided describe the functional responsibilities, education, and experience requirements for each labor category.

CLOUD ADMINISTRATOR I

Functional Responsibility: Performs basic administrative tasks in cloud environments under close supervision. Supports the setup of user accounts, service permissions, and resource configurations following established procedures. Monitors system status and documents activities in accordance with standard policies. Escalates anomalies or failures to senior staff for resolution. Builds initial familiarity with cloud service delivery models and develops fundamental operational skills.

CLOUD ADMINISTRATOR II

Functional Responsibility: Carries out a wider range of administrative functions across assigned cloud environments. Configures services, applies standard security and access policies, and manages scheduled maintenance routines such as backups and updates. Reviews monitoring data to identify potential issues, providing recommendations to prevent disruption. Resolves moderately complex incidents while coordinating with technical teams as needed. Maintains documentation and contributes to process improvements. Provides informal guidance to junior administrators and begins to demonstrate independent judgment in daily operations.

CLOUD ADMINISTRATOR III

Functional Responsibility: Leads the administration of multiple cloud platforms or environments with a focus on reliability and compliance. Establishes configuration standards, coordinates incident response, and develops recovery and continuity practices. Analyzes operational trends, prepares reports, and recommends changes to improve performance and efficiency. Partners with architects and engineers to ensure that administration aligns with organizational objectives.

Mentors and trains junior staff, ensuring consistency and accuracy in operations. Plays a key role in developing and enforcing policies for secure and resilient administration practices.

CLOUD ADMINISTRATOR IV

Functional Responsibility: Directs enterprise-wide cloud administration strategies, providing leadership and oversight across complex hybrid and multi-cloud environments. Defines and enforces governance frameworks, access policies, and lifecycle management practices. Oversee mission-critical operations, ensuring high availability, performance, and cost effectiveness. Advises executives on risks, strategic investments, and operational readiness for new or evolving services. Leads cross-functional collaboration with architecture, engineering, and security teams to establish long-term operational standards. Coaches administrators at all levels, ensuring that organizational knowledge, skills, and practices continually advance to meet emerging cloud service requirements.

CLOUD ANALYST I

Functional Responsibility: Supports the monitoring and reporting of assigned cloud environments while working under close supervision. Observes cloud monitoring processes to develop baseline analytical skills. Collects usage data and organizes reports under senior guidance. Learn to interpret dashboards that track system health and performance. Contributes to compliance documentation by compiling technical evidence. Assists in preparing resource inventories for audits and assessments. Participate in cost reviews to understand billing models. Gains early exposure to workload optimization concepts and develops reporting proficiency.

CLOUD ANALYST II

Functional Responsibility: Analyzes cloud performance metrics and prepares recurring reports for leadership. Identifies anomalies in system behavior and escalates findings to engineers. Reviews cost data and develop recommendations for workload right-sizing. Participate in compliance reviews by verifying configuration and reporting accuracy. Coordinates with administrators to validate usage patterns against billing records. Documents all findings and recommendations to support organizational transparency. Develop custom queries to extract relevant data from monitoring tools. Provides informal guidance to entry-level analysts in data collection techniques.

CLOUD ANALYST III

Functional Responsibility: Performs advanced analysis across multiple cloud platforms, identifying trends that inform enterprise planning. Develop dashboards and analytic tools that track usage, performance, and compliance. Coordinates with engineers to validate optimization opportunities and document savings. Reviews workload configurations to assess alignment with governance requirements. Mentors analysts by reviewing reports and teaching analytic methods. Collaborates with project managers to ensure analysis supports deliverable schedules. Presents findings in technical briefings to leadership. Improves data collection processes by integrating automation. Supports audit readiness by ensuring documentation accuracy.

CLOUD ANALYST IV

Functional Responsibility: Directs enterprise-level analysis efforts across hybrid and multi-cloud environments. Establishes analytic frameworks and reporting standards for consistency across teams. Advises executives on investment strategies, capacity planning, and optimization priorities. Oversees creation of predictive models that anticipate future demand. Coordinates analysis during migration planning to validate resource requirements. Develops training programs that advance analytic maturity across the organization. Engage in strategic planning by presenting risk assessments to leadership. Represents the organization in external forums discussing cloud metrics and governance. Evaluates analytic tools and guides adoption of advanced platforms. Ensure reporting practices evolve with industry standards.

CLOUD ARCHITECT I

Functional Responsibility: Assists senior architects in developing design diagrams and documenting configuration baselines. Prepares inventories of resources to validate against project requirements. Observes design review sessions to understand architectural decision-making. Contributes to migration documentation by preparing checklists and dependencies. Research reference architectures to strengthen understanding of cloud patterns. Participates in pilot projects to apply design principles in controlled settings. Gains exposure to governance frameworks and best practices for scalability.

CLOUD ARCHITECT II

Functional Responsibility: Designs small-scale cloud solutions by applying reference architectures and organizational templates. Prepares implementation plans and validates them with engineers. Reviews designs for compliance with cost, performance, and security requirements. Coordinates with developers to ensure integration requirements are captured. Documents design rationales to maintain transparency during reviews. Participates in modernization initiatives by recommending cloud-native services. Provides input into migration strategies for simple workloads. Offers support to entry-level architects by reviewing draft diagrams.

CLOUD ARCHITECT III

Functional Responsibility: Develops architecture for hybrid and multi-cloud systems supporting mission workloads. Defines governance models that enforce scalability, performance, and compliance standards. Coordinates with program managers and engineers to ensure designs align with organizational goals. Prepares detailed migration roadmaps and reviews cutover plans. Mentors junior architects by conducting technical workshops and providing structured feedback. Evaluates new services and incorporates them into design patterns when appropriate. Leads design reviews to ensure enterprise alignment. Documents integrate frameworks to support interoperability across services. Provides architecture briefings to stakeholders during planning sessions.

CLOUD ARCHITECT IV

Functional Responsibility: Shapes enterprise-level cloud architecture strategies across distributed environments. Establishes standards for scalability, cost optimization, and resilience. Advises executives on long-term modernization roadmaps and adoption strategies. Coordinates

with security leaders to integrate defense-in-depth principles into architecture. Oversees creation of enterprise reference architectures that can be reused across programs. Represents the organization in industry forums on cloud adoption. Develop training pathways for architects to strengthen organizational expertise. Reviews technology evaluations and makes adoption recommendations. Facilitates collaboration across multiple programs to ensure alignment. Ensures architecture decisions directly support mission readiness.

CLOUD DEVELOPER I

Functional Responsibility: Assists in coding, testing, and documenting applications that run in cloud environments. Writes small code modules and integrates them into larger applications under supervision. Executes unit tests to validate functionality and records results. Participate in debugging sessions to identify issues in simple scripts. Reviews secure coding practices to build foundational knowledge. Contributes to documentation by updating design notes and technical records. Observes deployment activities to understand CI/CD pipelines. Gains early experience with cloud-native frameworks and development environments.

CLOUD DEVELOPER II

Functional Responsibility: Develops cloud-based applications using approved frameworks and languages. Conducts code reviews with peers to ensure quality and consistency. Integrates services using APIs and validates interoperability. Applies secure coding practices during development activities. Participates in system testing and validates performance benchmarks. Maintains repositories and ensures adherence to version control standards. Coordinates with DevOps engineers to align development with release schedules. Provides informal mentoring to entry-level developers in coding practices.

CLOUD DEVELOPER III

Functional Responsibility: Leads and implements scalable cloud-native services that integrate across enterprise systems. Oversee development tasks for multiple projects and ensure alignment with design patterns. Evaluates performance metrics to validate scalability and reliability. Coordinates with architects to confirm compliance with governance requirements. Mentors junior developers by reviewing code and providing technical training. Develops technical reports that document application designs and decisions. Prepares leadership briefings on progress and risks. Collaborates with DevOps engineers to streamline deployments. Investigates new frameworks and tools for potential adoption.

CLOUD DEVELOPER IV

Functional Responsibility: Defines enterprise development strategies and coding standards for cloud applications. Oversee design reviews to ensure technical integrity and architectural alignment. Advises executives on modernization priorities and resource investments. Coordinates with program managers to align development activities with organizational goals. Facilitates collaboration between development, DevOps, and architecture teams. Coaches developers across all levels to advance skills and ensure consistency. Represents the organization in external technical communities. Evaluates emerging frameworks and tools for enterprise adoption. Develop guidelines that integrate security and compliance into coding standards. Ensures development outcomes support long-term mission readiness.

CLOUD DEVOPS ENGINEER I

Functional Responsibility: Supports automation activities within established CI/CD pipelines. Configure scripts under supervision to assist with deployments. Monitors logs and reports anomalies for senior review. Documents pipeline changes and maintain internal records. Participates in container deployment exercises to learn orchestration concepts. Contributes to troubleshooting sessions by gathering data. Gains familiarity with DevOps principles, tools, and workflows.

CLOUD DEVOPS ENGINEER II

Functional Responsibility: Builds and maintains pipelines to support development and operations teams. Creates automation scripts for common administrative tasks. Coordinates with engineers and developers to resolve pipeline issues. Validates that compliance checks are integrated into deployment workflows. Documents technical changes and updates operational guides. Participate in governance reviews by presenting pipeline performance. Supports adoption of container orchestration tools. Provides informal mentoring to entry-level engineers.

CLOUD DEVOPS ENGINEER III

Functional Responsibility: Designs and manages pipelines across multiple efforts. Establishes monitoring dashboards and performance baselines for automated deployments. Coordinates release schedules with program managers and ensure operational readiness. Reviews pipeline code from junior engineers and provide technical coaching. Collaborates with architects to integrate governance requirements. Implements observability features such as logging and alerts. Prepares leadership reports on DevOps performance. Facilitates lessons learned sessions after major releases. Evaluates automation tools for enterprise adoption.

CLOUD DEVOPS ENGINEER IV

Functional Responsibility: Directs enterprise DevOps strategies across multi-cloud environments. Establishes organizational standards for automation and monitoring practices. Advises executives on release readiness and operational risk. Coordinates cross-team deployments to ensure stability and compliance. Oversees integration of governance and security requirements into pipelines. Coaches staff across all levels on advanced DevOps practices. Represents the organization in industry forums to share best practices. Reviews emerging technologies and provides adoption recommendations. Develop enterprise metrics that measure DevOps maturity. Ensures DevOps strategies remain aligned with mission requirements.

CLOUD ENGINEER I

Functional Responsibility: Monitors assigned workloads and records performance data for review by senior staff. Configures virtual machines, storage, and networking resources under supervision. Executes patching cycles to gain experience in lifecycle management. Documents configurations and updates internal records. Responds to low-priority alerts by gathering data for incident reports. Participates in recovery exercises to understand continuity requirements. Gains exposure to engineering standards for cloud environments.

CLOUD ENGINEER II

Functional Responsibility: Configures workloads independently and validates resource baselines. Coordinates with developers to troubleshoot application performance issues. Implements routine automation scripts for provisioning and monitoring. Documents engineering changes for compliance and operational transparency. Participates in migration activities by validating dependencies and cutover readiness. Tracks incident trends and communicates findings to leadership. Provides feedback on engineering standards to improve efficiency. Mentors junior staff informally by sharing best practices.

CLOUD ENGINEER III

Functional Responsibility: Designs engineering solutions that optimize performance and scalability across workloads. Implements advanced automation to improve provisioning, monitoring, and recovery processes. Coordinates incident resolution for major outages and prepares root cause analyses. Collaborates with architects to align designs with enterprise strategies. Prepare technical reports that document engineering metrics. Mentors junior engineers by reviewing work products and coaching technical growth. Participates in governance activities by contributing engineering data. Evaluates emerging tools to improve efficiency. Facilitate workshops to improve engineering practices.

CLOUD ENGINEER IV

Functional Responsibility: Defines engineering strategies across enterprise workloads and ensures compliance with governance standards. Oversees automation adoption to streamline lifecycle management. Advises executives on engineering risks and modernization priorities. Coordinates cross-team incident response to ensure rapid recovery. Coaches engineers across all levels to strengthen organizational expertise. Represents the organization in industry discussions on cloud engineering. Reviews technical evaluations and makes adoption recommendations. Develops enterprise roadmaps that align engineering with mission goals. Facilitates collaboration across engineering and architecture teams. Ensure systems remain resilient and cost effective.

CLOUD MIGRATION SPECIALIST I

Functional Responsibility: Assists in planning and executing migrations under senior guidance. Collects workload inventories and documents system dependencies. Participates in migration rehearsals to practice transition steps. Supports cutover activities by validating transfers and reporting outcomes. Updates documentation after each migration cycle. Prepare rollback procedures with assistance from senior staff. Gains familiarity with migration methodologies and tools.

CLOUD MIGRATION SPECIALIST II

Functional Responsibility: Plans migrations for small workloads and validates readiness with stakeholders. Coordinates with engineers to ensure dependencies are addressed. Documents migration procedures and provide reports after execution. Track cutover issues and communicate risks to project managers. Validates that rollback procedures are tested and available. Supports compliance documentation by recording migration evidence. Provides input into workload prioritization decisions. Mentors entry-level staff by reviewing inventories and schedules.

CLOUD MIGRATION SPECIALIST III

Functional Responsibility: Develops migration plans for large or complex workloads. Prepares risk assessments, schedules, and validation reports. Oversees cutover execution to ensure continuity of operations. Collaborate with architects to align migration approaches with enterprise strategies. Facilitates lessons learned sessions to improve methodologies. Mentors migration staff by providing technical training and structured guidance. Reviews documentation to confirm accuracy and completeness. Provides leadership with progress reports and recommendations. Evaluates migration tools for efficiency and suitability.

CLOUD MIGRATION SPECIALIST IV

Functional Responsibility: Defines enterprise migration strategies across multi-cloud environments. Oversees planning and execution for mission-critical transitions. Advises executives on risks, opportunities, and resource requirements. Coordinates cross-functional teams to ensure migration success. Coaches staff across all levels in advanced migration methods. Represents the organization in external forums on migration practices. Reviews technology assessments and adoption proposals. Develops roadmaps that integrate migration with modernization initiatives. Facilitates collaboration between architects and engineers. Ensures organizational readiness for large-scale migrations.

CLOUD PROJECT MANAGER I

Functional Responsibility: Assists in planning activities and maintains project documentation. Tracks schedules and updates task lists under senior direction. Coordinates meeting logistics and records action items. Prepare basic reports to summarize project status. Observes risk review sessions to understand mitigation practices. Learns to use project management tools for scheduling and reporting. Gains foundational experience in managing cloud-focused initiatives.

CLOUD PROJECT MANAGER II

Functional Responsibility: Manages small cloud projects or specific workstreams. Defines schedules, tracks progress and maintains deliverable quality. Coordinates with engineers and developers to ensure tasks remain on track. Monitors risks and escalate concerns to leadership. Documents lessons learned and updates project records. Prepare status briefings for stakeholders. Provides informal mentoring to entry-level staff on project tracking. Reviews budgets to confirm alignment with project activities.

CLOUD PROJECT MANAGER III

Functional Responsibility: Coordinates multiple project efforts simultaneously and ensures alignment with program goals. Develops detailed project plans that include schedules, risks, and resource allocations. Oversees cross-team collaboration to resolve issues quickly. Mentors junior project managers through reviews and coaching sessions. Prepares leadership reports that summarize project risks and performance. Collaborate with architects to align projects with enterprise strategies. Facilitates lessons learned sessions after major deliveries. Reviews project management tools for efficiency. Provides recommendations to improve governance practices.

CLOUD PROJECT MANAGER IV

Functional Responsibility: Directs enterprise cloud program management functions across distributed environments. Establishes governance frameworks to standardize project execution. Advises executives on risk, performance, and investment priorities. Coordinates project portfolios to align with modernization strategies. Coaches project managers across all levels to strengthen delivery practices. Represents the organization in industry groups on cloud program management. Develop training resources to improve project execution. Reviews program-level performance metrics and prepares executive briefings. Facilitate collaboration across programs to ensure consistency. Ensures enterprise strategies are achieved through disciplined execution.

CLOUD SECURITY SPECIALIST I

Functional Responsibility: Assists in monitoring cloud systems for potential security issues. Records alert and gathers data for senior review. Applies basic configuration updates to maintain security baselines. Participates in vulnerability scans and documents results. Contributes to compliance documentation for audits. Observes incident response activities to understand escalation paths. Gains exposure to security tools and reporting methods.

CLOUD SECURITY SPECIALIST II

Functional Responsibility: Implements workload security settings such as encryption and logging. Responds to alerts and performs initial triage for incidents. Documents findings and prepare evidence for remediation. Reviews compliance requirements and ensures configurations are aligned. Participates in risk assessments and provides technical input. Coordinate with engineers to strengthen workload security. Tracks vulnerability management activities to confirm closure. Provides informal coaching to entry-level staff on basic practices.

CLOUD SECURITY SPECIALIST III

Functional Responsibility: Oversees security operations across multiple workloads. Designs monitoring dashboards and configures advanced detection tools. Coordinates incident response activities and prepares root cause analyses. Reviews compliance documentation and validates evidence for audits. Mentors junior staff by reviewing reports and conducting training. Collaborate with architects to align security with enterprise strategies. Facilitates lessons learned sessions after major incidents. Prepare leadership briefings on security posture. Evaluates new tools for adoption in security programs.

CLOUD SECURITY SPECIALIST IV

Functional Responsibility: Shapes enterprise security strategies for multi-cloud environments. Defines standards for monitoring, detection, and remediation. Advises executives on risks, threats, and investment needs. Oversees vulnerability management across workloads and providers. Coordinates with architects to integrate security into all designs. Coaches security specialists at all levels through structured programs. Represents the organization in security industry forums. Reviews and approves major security initiatives. Develop long-term road maps for improving security posture. Ensure enterprise systems remain compliant and resilient.

CLOUD SUBJECT MATTER EXPERT I

Functional Responsibility: Provides technical expertise on specific cloud technologies under the guidance of senior staff. Participates in design reviews and validates limited aspects of solutions. Responds to technical questions from project teams. Reviews documentation for accuracy and clarity. Supports troubleshooting activities by applying specialized knowledge. Contributes to training materials to share knowledge. Gains familiarity with broader enterprise cloud strategies.

CLOUD SUBJECT MATTER EXPERT II

Functional Responsibility: Advises teams on best practices for cloud adoption and usage. Participates in design reviews to validate approaches. Documents recommendations and provide technical input during planning. Assists with complex troubleshooting by applying specialized knowledge. Provides informal mentoring to staff on advanced techniques. Develops technical guides that capture lessons learned. Collaborate with engineers to validate solutions. Reviews pilot projects to assess alignment with standards.

CLOUD SUBJECT MATTER EXPERT III

Functional Responsibility: Guides multiple projects by providing advanced technical expertise. Defines best practices for integration, scalability, and modernization. Mentors staff through structured training and performance reviews. Reviews architectural designs to confirm alignment with standards. Prepare reports summarizing risks and opportunities. Advises leadership on adoption of new services. Facilitates workshops to share knowledge across teams. Evaluates new technologies and provides recommendations. Coordinate with project managers to support complex initiatives.

CLOUD SUBJECT MATTER EXPERT IV

Functional Responsibility: Provides enterprise-level guidance on cloud adoption strategies. Develops reference architectures and integration frameworks. Advises executives on modernization roadmaps and industry trends. Oversee technical evaluations and provide adoption recommendations. Coaches architects and engineers on advanced practices. Represents the organization in industry forums on cloud modernization. Prepares training programs to expand organizational expertise. Reviews enterprise-wide strategies to ensure alignment. Facilitates collaboration across programs to promote consistency. Ensures cloud adoption supports long-term mission success.

CLOUD SUBJECT MATTER EXPERT V

Functional Responsibility: Serves as the top-level technical authority on enterprise cloud services. Defines organizational vision for adoption, integration, and modernization. Advises executive leadership on strategic investments. Represents the organization in government and industry working groups. Coaches technical leaders across programs. Oversees evaluation and adoption of emerging technologies. Develop long-term roadmaps for modernization and resilience. Prepares executive briefings on risks, opportunities, and readiness. Establishes standards that shape the enterprise cloud future. Ensures strategies remain aligned with evolving mission requirements.

CLOUD SUPPORT SPECIALIST I

Functional Responsibility: Provides initial support for cloud services and applications. Responds to user requests, resolves common issues, and documents resolutions for reuse. Monitors help desk queues, record detailed troubleshooting notes, and escalate complex problems to higher-level staff. Gains exposure to ticketing systems, service catalog items, and standard troubleshooting procedures. Develop communication skills by assisting end users and delivering consistent customer service.

CLOUD SUPPORT SPECIALIST II

Functional Responsibility: Delivers intermediate-level support for cloud systems and environments. Troubleshoots recurring user issues, supports account and service access requests, and coordinates with administrators to address system-related problems. Maintains knowledge articles, updates user guides, and contributes to process improvements. Provides clear communication with users during incidents, ensuring they understand impacts, workarounds, and timelines for resolution. Guides junior support personnel in troubleshooting methods and service-level expectations, strengthening overall team performance.

CLOUD SUPPORT SPECIALIST III

Functional Responsibility: Leads advanced support activities across multiple services and organizational environments. Manages escalated incidents that involve complex integrations or cross-platform issues. Coordinates with engineering teams to validate fixes and improve diagnostic tools. Reviews support performance metrics, identify systemic issues, and recommend long-term improvements to reduce incident frequency. Develops training materials, conducts workshops, and mentors staff to improve problem resolution skills. Prepares reports for leadership summarizing support trends, risks, and user satisfaction. Plays a key role in ensuring readiness for new service deployments and major system changes.

CLOUD SUPPORT SPECIALIST IV

Functional Responsibility: Oversees enterprise-level support functions for mission-critical cloud services. Defines support strategies, escalation protocols, and knowledge management frameworks. Establishes performance metrics, analyzes support data, and implements continuous improvement programs to enhance service delivery. Directs communications during major incidents, ensuring timely updates to leadership and end users. Collaborates with technical and business leaders to ensure support readiness for migrations, platform upgrades, and new service rollouts. Resolves the most complex support challenges, balancing user experience with operational stability. Coaches and develops support staff at all levels, fostering a culture of accountability, professionalism, and continuous learning across the support function.

SIN 54151 SOFTWARE MAINTENANCE SERVICES

ID NUMBER	OEM	MFR ID	DESCRIPTION	PRICE
03013001	WSO2	S-AC	Architecture Checkpoint	$2,854.41
03013002	WSO2	S-AC-O	Architecture Checkpoint (Remote)	$572.83
03013003	WSO2	S-AR	Architecture Exchange	$10,550.71
03013004	WSO2	S-AR-O	Architecture Exchange (Remote)	$3,427.42
03013005	WSO2	S-CR	Configuration Review	$8,552.60
03013006	WSO2	S-CR-O	Configuration Review (Remote)	$2,281.50
03013007	WSO2	S-QR	Quarterly Architecture Exchange Package	$34,211.18
03013008	WSO2	S-QR-O	Quarterly Architecture Exchange Package (Remote)	$9,545.20
03013009	WSO2	S-QSP	WSO2 QuickStart	$25,574.12
03013010	WSO2	S-QSP-O	WSO2 QuickStart (Remote)	$13,708.02





SIN 54151 SOFTWARE MAINTENANCE SERVICES INFORMATION

1. Architecture and Configuration Reviews

WSO2 customers can benefit from the challenges and solutions other enterprises have implemented by reviewing their business goals and translation to architecture requirements, apply best practices for architectural patterns, and adjust projects as new requirements or environmental factors come to light. A basic Architecture Review teams you with a WSO2 Platform Architect for two working days to discuss, review, generate and document plans, to ensure your project avoids costly pitfalls. Remote architecture reviews are conducted as a series of 4-hour videoconference sessions over four days.

For ongoing collaboration, customers should consider a Quarterly Review Package consisting of 4 two-day on-site reviews, to be scheduled approximately quarterly.

A Configuration Review consists of two days with one of our Operational Specialists to review configurations, deployment environments and practices, security features, and monitoring, to ensure every aspect of a reliable and secure production deployment is achieved. A remote configuration review is conducted as a series of 4-hour videoconference sessions over four days.

2. Architecture Checkpoints

Architecture checkpoints are carried out by WSO2 Platform Architects or Solution Architects. This one-day session reviews the current project, its business, solution and deployment architectures to ensure that the project is on-track from an architectural, deployment and roadmap perspective. The session is also used to address any challenges and bottlenecks, align with best practices, and answer technical questions.

3. QuickStart

Jumpstarting an evaluation, proof of concept, or project is effectively accomplished through a QuickStart, which places two expert consultants at your site for a week of agile activity to get your team and your project efficiently off the ground. The scope of the QuickStart is carefully laid out in advance, encompassing goals such as:

- Increasing awareness of product capabilities
- Help defining the solution architecture
- Help defining the deployment architecture
- Help defining the implementation plan
- Preparing the project team to begin implementation
- Jointly develop prototype or proof-of-concept code for customer scenarios

QuickStart can be delivered onsite or remotely. An onsite engagements places two WSO2 consultants at your location for a week (five consecutive days) of intensive work. Remote engagements are a 10-day collaboration, with daily 4-hour videoconference sessions and chat activity throughout for resource sharing and maintaining momentum with clarifications and follow-up between sessions. Each QuickStart includes follow-up with 10 hours of query support tickets.

SIN 54151HACS HIGHLY ADAPTIVE CYBERSECURITY SERVICES

ID NUMBER	LCAT DESCRIPTION	YEAR 3 *04/2026*	YEAR 4 *04/2027*	YEAR 5 *04/2028*
03011204	Cybersecurity Analyst I	$88.96	$92.52	$96.22
03011205	Cybersecurity Analyst II	$108.55	$112.89	$117.41
03011206	Cybersecurity Analyst III	$139.48	$145.06	$150.86
03011207	Cybersecurity Analyst IV	$175.41	$182.43	$189.73
03011208	Cybersecurity Architect I	$136.97	$142.45	$148.15
03011209	Cybersecurity Architect II	$165.76	$172.39	$179.29
03011210	Cybersecurity Architect III	$194.63	$202.42	$210.52
03011211	Cybersecurity Architect IV	$233.27	$242.60	$252.30
03011212	Cybersecurity Database Specialist I	$112.83	$117.34	$122.03
03011213	Cybersecurity Database Specialist II	$136.66	$142.13	$147.82
03011214	Cybersecurity Database Specialist III	$173.36	$180.29	$187.50
03011215	Cybersecurity Database Specialist IV	$216.85	$225.52	$234.54
03011216	Cybersecurity Engineer I	$106.06	$110.30	$114.71
03011217	Cybersecurity Engineer II	$134.93	$140.33	$145.94
03011218	Cybersecurity Engineer III	$165.46	$172.08	$178.96
03011219	Cybersecurity Engineer IV	$214.14	$222.71	$231.62
03011220	Cybersecurity Help Desk Specialist I	$65.11	$67.71	$70.42
03011221	Cybersecurity Help Desk Specialist II	$77.47	$80.57	$83.79
03011222	Cybersecurity Help Desk Specialist III	$88.17	$91.70	$95.37
03011223	Cybersecurity Help Desk Specialist IV	$97.85	$101.76	$105.83
03011224	Cybersecurity IA/Security Specialist I	$92.05	$95.73	$99.56
03011225	Cybersecurity IA/Security Specialist II	$110.88	$115.32	$119.93
03011226	Cybersecurity IA/Security Specialist III	$141.50	$147.16	$153.05
03011227	Cybersecurity IA/Security Specialist IV	$174.15	$181.12	$188.36
03011228	Cybersecurity Network Engineer I	$86.26	$89.71	$93.30
03011229	Cybersecurity Network Engineer II	$101.52	$105.58	$109.80

ID NUMBER	LCAT DESCRIPTION	YEAR 3 *04/2026*	YEAR 4 *04/2027*	YEAR 5 *04/2028*
03011230	Cybersecurity Network Engineer III	$125.37	$130.38	$135.60
03011231	Cybersecurity Network Engineer IV	$149.52	$155.50	$161.72
03011232	Cybersecurity Network Specialist I	$93.39	$97.13	$101.02
03011233	Cybersecurity Network Specialist II	$112.52	$117.02	$121.70
03011234	Cybersecurity Network Specialist III	$144.11	$149.87	$155.86
03011235	Cybersecurity Network Specialist IV	$182.55	$189.85	$197.44
03011236	Cybersecurity Project Manager I	$91.66	$95.33	$99.14
03011237	Cybersecurity Project Manager II	$111.37	$115.82	$120.45
03011238	Cybersecurity Project Manager III	$135.52	$140.94	$146.58
03011239	Cybersecurity Project Manager IV	$160.54	$166.96	$173.64
03011240	Cybersecurity Software Engineer I	$90.79	$94.42	$98.20
03011241	Cybersecurity Software Engineer II	$112.62	$117.12	$121.80
03011242	Cybersecurity Software Engineer III	$140.45	$146.07	$151.91
03011243	Cybersecurity Software Engineer IV	$165.76	$172.39	$179.29
03011244	Cybersecurity Subject Matter Expert I	$126.25	$131.30	$136.55
03011245	Cybersecurity Subject Matter Expert II	$154.34	$160.51	$166.93
03011246	Cybersecurity Subject Matter Expert III	$170.48	$177.30	$184.39
03011247	Cybersecurity Subject Matter Expert IV	$211.13	$219.58	$228.36
03011248	Cybersecurity Subject Matter Expert V	$235.58	$245.00	$254.80
03011249	Cybersecurity Systems Administrator I	$75.72	$78.75	$81.90
03011250	Cybersecurity Systems Administrator II	$92.91	$96.63	$100.50
03011251	Cybersecurity Systems Administrator III	$114.56	$119.14	$123.91
03011252	Cybersecurity Systems Administrator IV	$143.23	$148.96	$154.92
03011253	Cybersecurity Systems Engineer I	$92.52	$96.22	$100.07
03011254	Cybersecurity Systems Engineer II	$102.86	$106.97	$111.25
03011255	Cybersecurity Systems Engineer III	$131.15	$136.40	$141.86
03011256	Cybersecurity Systems Engineer IV	$163.14	$169.67	$176.46
03011257	Cybersecurity Test Engineer I	$88.96	$92.52	$96.22

ID NUMBER	LCAT DESCRIPTION	YEAR 3 *04/2026*	YEAR 4 *04/2027*	YEAR 5 *04/2028*
03011258	Cybersecurity Test Engineer II	$108.55	$112.89	$117.41
03011259	Cybersecurity Test Engineer III	$139.48	$145.06	$150.86
03011260	Cybersecurity Test Engineer IV	$172.71	$179.62	$186.80

SIN 54151HACS LABOR CATEGORY INFORMATION

Experience and Education

The following labor category minimum technical experience tables correspond to the prices offered in this submission.

All SIN 54151HACS Labor Categories		
Level I	Junior	Bachelor's degree and 0 to 1 year of experience
Level II	Associate	Bachelor's degree and 2 to 4 years of experience
Level III	Senior	Bachelor's degree and 3 to 5 years of experience
Level IV	Master	Master's degree and 5 to 7 years of experience
Level V	Director	Master's degree and 7+ years of experience

Degree Substitution

This serves as a guide to the experience and educational background of personnel typically found in each labor category. However, the experience of a resource is often a valid substitute for education. With this noted, the following information indicates where experience might be substituted for a degree as accepted by the customer.

All SIN 54151HACS Labor Categories Except Program Manager	
Equivalent to Bachelor's (Level I)	Associates degree + 2 or more years of relevant technical experience
	High School diploma + 4 or more years relevant technical experience
Equivalent to Bachelor's (Level II)	Associates degree + 3 or more years of relevant technical experience
	High School diploma + 6 or more years relevant technical experience
Equivalent to Bachelor's (Level III)	Associates degree + 5 or more years of relevant technical experience
	High School diploma + 7 or more years relevant technical experience
Equivalent to Master's (Level IV)	Bachelor's degree + 7 years of relevant technical experience
	Associates degree + 9 or more years of relevant technical experience
	High School diploma + 11 or more years relevant technical experience
Equivalent to Master's (Level V)	Bachelor's degree + 9 or more years of relevant technical experience
	Associates degree + 11 or more years of relevant technical experience

Experience & Degree Substitution Equivalencies

*Experience exceeding the minimum shown may be substituted for education. Likewise, education exceeding the minimum shown may be substituted for experience.

LABOR CATEGORY	STANDARD QUALS		SUBSTITUTIONS				
	Min Education	Min Exp	PhD	Masters	Bachelors	Associates	High School
Cybersecurity Analyst I	Bachelors	0	0	0	0	2	4
Cybersecurity Analyst II	Bachelors	2	0	0	2	3	6
Cybersecurity Analyst III	Bachelors	3	0	1	3	5	7
Cybersecurity Analyst IV	Masters	5	3	5	7	9	11
Cybersecurity Architect I	Bachelors	0	0	0	0	2	4

LABOR CATEGORY	STANDARD QUALS		SUBSTITUTIONS				
	Min Education	Min Exp	PhD	Masters	Bachelors	Associates	High School
Cybersecurity Architect II	Bachelors	2	0	0	2	3	6
Cybersecurity Architect III	Bachelors	3	0	1	3	5	7
Cybersecurity Architect IV	Masters	5	3	5	7	9	11
Cybersecurity DB Specialist I	Bachelors	0	0	0	0	2	4
Cybersecurity DB Specialist II	Bachelors	2	0	0	2	3	6
Cybersecurity DB Specialist III	Bachelors	3	0	1	3	5	7
Cybersecurity DB Specialist IV	Masters	5	3	5	7	9	11
Cybersecurity Engineer I	Bachelors	0	0	0	0	2	4
Cybersecurity Engineer II	Bachelors	2	0	0	2	3	6
Cybersecurity Engineer III	Bachelors	3	0	1	3	5	7
Cybersecurity Engineer IV	Masters	5	3	5	7	9	11
Cybersecurity Help Desk Specialist I	Bachelors	0	0	0	0	2	4
Cybersecurity Help Desk Specialist II	Bachelors	2	0	0	2	3	6
Cybersecurity Help Desk Specialist III	Bachelors	3	0	1	3	5	7
Cybersecurity Help Desk Specialist IV	Masters	5	3	5	7	9	11
Cybersecurity IA/Security Specialist I	Bachelors	0	0	0	0	2	4
Cybersecurity IA/Security Specialist II	Bachelors	2	0	0	2	3	6
Cybersecurity IA/Security Specialist III	Bachelors	3	0	1	3	5	7
Cybersecurity IA/Security Specialist IV	Masters	5	3	5	7	9	11
Cybersecurity Network Engineer I	Bachelors	0	0	0	0	2	4
Cybersecurity Network Engineer II	Bachelors	2	0	0	2	3	6
Cybersecurity Network Engineer III	Bachelors	3	0	1	3	5	7
Cybersecurity Network Engineer IV	Masters	5	3	5	7	9	11
Cybersecurity Network Specialist I	Bachelors	0	0	0	0	2	4
Cybersecurity Network Specialist II	Bachelors	2	0	0	2	3	6
Cybersecurity Network Specialist III	Bachelors	3	0	1	3	5	7
Cybersecurity Network Specialist IV	Masters	5	3	5	7	9	11
Cybersecurity Project Manager I	Bachelors	0	0	0	0	2	4
Cybersecurity Project Manager II	Bachelors	2	0	0	2	3	6

LABOR CATEGORY	STANDARD QUALS			SUBSTITUTIONS			
	Min Education	Min Exp	PhD	Masters	Bachelors	Associates	High School
Cybersecurity Project Manager III	Bachelors	3	0	1	3	5	7
Cybersecurity Project Manager IV	Masters	5	3	5	7	9	11
Cybersecurity Software Engineer I	Bachelors	0	0	0	0	2	4
Cybersecurity Software Engineer II	Bachelors	2	0	0	2	3	6
Cybersecurity Software Engineer III	Bachelors	3	0	1	3	5	7
Cybersecurity Software Engineer IV	Masters	5	3	5	7	9	11
Cybersecurity SME I	Bachelors	0	0	0	0	2	4
Cybersecurity SME II	Bachelors	2	0	0	2	3	6
Cybersecurity SME III	Bachelors	3	0	1	3	5	7
Cybersecurity SME IV	Masters	5	3	5	7	9	11
Cybersecurity SME V	Masters	7	5	7	9	11	N/A
Cybersecurity Systems Administrator I	Bachelors	0	0	0	0	2	4
Cybersecurity Systems Administrator II	Bachelors	2	0	0	2	3	6
Cybersecurity Systems Administrator III	Bachelors	3	0	1	3	5	7
Cybersecurity Systems Administrator IV	Masters	5	3	5	7	9	11
Cybersecurity Systems Engineer I	Bachelors	0	0	0	0	2	4
Cybersecurity Systems Engineer II	Bachelors	2	0	0	2	3	6
Cybersecurity Systems Engineer III	Bachelors	3	0	1	3	5	7
Cybersecurity Systems Engineer IV	Masters	5	3	5	7	9	11
Cybersecurity Test Engineer I	Bachelors	0	0	0	0	2	4
Cybersecurity Test Engineer II	Bachelors	2	0	0	2	3	6
Cybersecurity Test Engineer III	Bachelors	3	0	1	3	5	7
Cybersecurity Test Engineer IV	Masters	5	3	5	7	9	11

Place of Performance

The labor categories provided are for both Contractor and Customer facilities.

Clearance

The labor categories provided are for a Secret and below clearance.

Labor Category Descriptions

The descriptions provided describe the functional responsibilities, education, and experience requirements for each labor category.

CYBERSECURITY ANALYST I

Functional Responsibility: Performs entry-level cybersecurity monitoring and analysis in support of defensive cyber operations. Reviews alerts, event logs, and network traffic to identify potential threats or anomalies under direct supervision. Applies basic knowledge of intrusion detection systems, vulnerability scanners, and endpoint protection tools to assist with triage and documentation of security incidents. Supports the maintenance of security baselines and system hardening in accordance with DoD and NIST guidance. Develops foundational understanding of RMF processes and the principles of confidentiality, integrity, and availability.

CYBERSECURITY ANALYST II

Functional Responsibility: Conducts intermediate-level cybersecurity assessments and incident analysis activities. Analyzes system vulnerabilities, evaluates security events, and assists in implementing mitigation strategies. Utilizes SIEM tools, IDS/IPS, and endpoint monitoring utilities to detect and report threats. Coordinates with network and system administrators to validate incident containment and eradication. Prepares technical reports, risk assessments, and remediation documentation following NIST SP 800-61 incident handling and SP 800-53 control guidelines. Demonstrates growing proficiency in enterprise security technologies, including zero trust and identity management solutions.

CYBERSECURITY ANALYST III

Functional Responsibility: Leads complex threat analysis, vulnerability management, and cyber defense operations. Performs correlation and fusion of intelligence from multiple sources to identify advanced persistent threats and network intrusions. Designs and executes red/blue team exercises to assess system resilience and validate defensive postures. Applies NIST SP 800-37 and SP 800-53 methodologies to assess and authorize systems under RMF. Mentors junior analysts in technical procedures, forensic analysis, and security tool configuration. Develops SOPs for incident response and contributes to the development of organizational cybersecurity policy and training programs. Serves as a senior advisor in the identification, protection, detection, response, and recovery lifecycle activities.

CYBERSECURITY ANALYST IV

Functional Responsibility: Oversees enterprise-wide cybersecurity operations and provides technical and managerial leadership to multidisciplinary teams. Directs the planning, execution, and sustainment of SOC activities across networks, cloud environments, and mission systems. Defines cybersecurity strategies, establishes risk management priorities, and ensures compliance with FISMA and NIST standards. Supervises and evaluates personnel performance, manages staffing and training plans, and ensures team readiness for incident response and threat hunting operations. Coordinates with executive leadership and stakeholders to align cybersecurity initiatives with mission objectives, leading the continual improvement of organizational resilience and zero trust architecture implementation.

CYBERSECURITY ARCHITECT I

Functional Responsibility: Supports the development and maintenance of secure data frameworks used in cybersecurity operations. Assists in mapping data flows, documenting interfaces, and validating data structures for vulnerability and threat management systems. Follows established design patterns to ensure that security controls and privacy protections are applied consistently across repositories. Works closely with engineers and analysts to maintain data accuracy and traceability in compliance with agency security standards and RMF documentation requirements.

CYBERSECURITY ARCHITECT II

Functional Responsibility: Designs and implements secure data models and pipelines that enable correlation of cyber event data from multiple enterprise systems. Defines data relationships and storage mechanisms to ensure accuracy, scalability, and compliance with information assurance requirements. Collaborates with analysts, engineers, and SOC personnel to integrate automated feeds from vulnerability scanners, configuration management databases, and cloud monitoring tools. Evaluates new data management technologies and recommends improvements to enhance data availability and security. Operates with limited supervision and contributes to the development of enterprise data architecture standards supporting the organization's cybersecurity mission.

CYBERSECURITY ARCHITECT III

Functional Responsibility: Leads complex data architecture initiatives supporting agency-wide cybersecurity programs and zero trust initiatives. Integrates structured, semi-structured, and unstructured data from numerous sources into unified schemas to improve visibility and enable advanced analytics. Establishes automated quality controls, metadata management, and access control mechanisms to ensure integrity and traceability across the data lifecycle. Partners with engineering and operations teams to optimize the performance of security analytics platforms, dashboards, and risk scoring models. Mentors junior staff, provides architectural guidance, and conducts peer reviews to ensure consistency and compliance with federal cybersecurity and data governance standards. Serves as a subject-matter resource to program leadership on matters involving secure data design and analytic enablement.

CYBERSECURITY ARCHITECT IV

Functional Responsibility: Provides enterprise-level leadership in the planning, design, and governance of secure data architectures that underpin large-scale cybersecurity and risk management operations. Defines the overarching vision for data integration and sharing across hybrid, cloud, and on-premises environments while ensuring alignment with zero trust data principles, FISMA, and NIST frameworks. Directs multi-disciplinary teams in architecting resilient data ecosystems that support proactive cyber defense, continuous monitoring, and mission analytics. Establishes policies for data classification, protection, and stewardship; oversees implementation of advanced encryption and access management solutions; and ensures architecture compliance across all operational enclaves. Coordinates with senior executives, mission owners, and federal stakeholders to align technical capabilities with enterprise cyber objectives. Supervises subordinate architects and engineers, manages staffing and priorities, and provides authoritative approval for all cybersecurity data architecture deliverables.

CYBERSECURITY DATABASE SPECIALIST I

Functional Responsibility: Assists in the configuration and maintenance of secure databases supporting cybersecurity operations, vulnerability management, and monitoring systems. Performs data validation, indexing, and basic query optimization to ensure integrity and performance under supervision. Applies standard security controls for user access, encryption, and backup procedures in accordance with federal information security policies. Participates in database patching and change management activities to support mission availability and compliance.

CYBERSECURITY DATABASE SPECIALIST II

Functional Responsibility: Implements and maintains secure database environments that store and process cybersecurity event, asset, and risk information. Develops stored procedures, views, and access controls to enforce least privilege and ensure data confidentiality. Conducts audits, monitors performance, and tunes configurations to support analytics and continuous monitoring tools. Collaborates with system administrators and cybersecurity engineers to implement secure data flows across on-premises and cloud platforms. Maintains documentation for RMF accreditation and ensures database baselines align with applicable DISA STIGs and federal standards.

CYBERSECURITY DATABASE SPECIALIST III

Functional Responsibility: Designs and manages complex database infrastructures that support enterprise-scale cybersecurity, vulnerability, and incident response systems. Integrates multiple data sources, ensuring consistency, redundancy, and high availability across mission-critical applications. Implements advanced security features such as data masking, transparent encryption, and auditing to protect sensitive cyber threat and incident data. Coordinates with developers and analysts to optimize schema design and improve query performance for investigative and reporting tools. Guides junior team members in best practices for secure database administration and contributes to the development of enterprise data retention and disaster recovery strategies.

CYBERSECURITY DATABASE SPECIALIST IV

Functional Responsibility: Directs the planning, implementation, and governance of database systems supporting large-scale cybersecurity and risk management operations. Defines enterprise database architectures and data protection strategies that align with zero trust and NIST SP 800-53 control families. Oversees backup, replication, and failover mechanisms to ensure resilience and mission continuity across hybrid cloud and classified environments. Establishes policies for credential management, auditing, and encryption key lifecycle operations to safeguard sensitive data repositories. Leads cross-functional teams in assessing new technologies, resolving high-impact incidents, and developing enterprise migration roadmaps. Supervises database personnel, manages workload distribution, and ensures consistent adherence to cybersecurity and data integrity standards across all programs.

CYBERSECURITY ENGINEER I

Functional Responsibility: Supports the design and implementation of secure information systems under the guidance of senior engineers. Assists in configuring and maintaining firewalls, endpoint protection, and encryption technologies in compliance with DoD and NIST security controls. Reviews vulnerability scan results and participates in patch management activities. Applies foundational knowledge of system security engineering principles to integrate security features during system setup and testing. Documents technical configurations and contributes to risk assessments following the RMF Prepare and Categorize

steps. Develops basic scripts and automation tools to improve system monitoring and compliance verification.

CYBERSECURITY ENGINEER II

Functional Responsibility: Implements and manages cybersecurity technologies and architectures to protect enterprise networks and applications. Designs secure configurations for servers, workstations, and virtual environments while supporting continuous monitoring and system accreditation efforts. Analyzes system security plans to ensure alignment with NIST SP 800-53 control baselines and validates control implementation through testing. Collaborates with system administrators and developers to incorporate security into DevSecOps pipelines and cloud-based deployments. Troubleshoots and mitigates vulnerabilities, supports contingency planning, and ensures system recovery procedures meet mission availability requirements. Applies intermediate knowledge of zero trust principles, identity federation, and encryption key management.

CYBERSECURITY ENGINEER III

Functional Responsibility: Leads system security engineering and risk mitigation activities across multiple enterprise or mission systems. Develops and enforces security architectures, standards, and technical policies to ensure systems are designed and operated securely from inception through sustainment. Conducts detailed RMF assessment and authorization activities, producing artifacts such as Security Assessment Reports, POA&Ms, and continuous monitoring strategies. Integrates advanced solutions for intrusion detection, endpoint protection, and data loss prevention across hybrid and cloud environments. Mentors junior engineers in cybersecurity design practices, tool configuration, and compliance documentation. Coordinates with program managers and ISSOs to verify that all security engineering deliverables meet mission and regulatory requirements.

CYBERSECURITY ENGINEER IV

Functional Responsibility: Directs enterprise cybersecurity engineering strategy and serves as the senior technical authority for secure architecture design and risk management. Oversees system design reviews, vulnerability remediation programs, and accreditation activities for complex networks and cloud infrastructures. Defines organization-wide standards for security control inheritance, container hardening, and encryption architecture in accordance with zero trust and NIST SP 800-207 guidance. Manages a team of cybersecurity engineers, assigning project priorities, conducting performance evaluations, and ensuring continuous professional development. Advises senior leadership on cybersecurity investments, emerging threats, and compliance posture. Leads the development of enterprise security blueprints that integrate threat intelligence, automation, and continuous monitoring into the organization's defense-in-depth architecture.

CYBERSECURITY HELP DESK SPECIALIST I

Functional Responsibility: Provides entry-level cybersecurity service desk support for user accounts, secure configurations, and incident reporting. Receives and documents incoming service requests through approved ticketing systems, categorizing them by severity and aligning them with established service-level agreements. Follows standard operating procedures to assist users with password resets, account provisioning, endpoint protection updates, and encrypted communications. Maintains detailed call records and escalation logs to ensure traceability and audit compliance. Works under close supervision to apply agency policies related to user access, authentication, and endpoint security, contributing to overall

incident prevention and early detection efforts within the organization's cybersecurity operations framework.

CYBERSECURITY HELP DESK SPECIALIST II

Functional Responsibility: Delivers intermediate-level technical support for cybersecurity incidents, access control, and endpoint security services. Diagnoses and resolves recurring issues associated with authentication failures, certificate expirations, email security, and workstation configuration compliance. Monitors alerts generated by antivirus and SIEM tools, validating and escalating suspicious activity to analysts or the SOC for further review. Coordinates with network engineers and system administrators to isolate compromised systems, implement containment measures, and verify restoration integrity. Assists in drafting user guidance and FAQs that promote adherence to security policies, reducing the frequency of preventable incidents. Operates independently on routine assignments and ensures that all help desk activities maintain compliance with NIST SP 800-53 and agency-specific cybersecurity baselines.

CYBERSECURITY HELP DESK SPECIALIST III

Functional Responsibility: Leads day-to-day cybersecurity service desk operations, handling advanced escalations and ensuring timely incident resolution across enterprise systems. Investigates and resolves complex user and system issues involving secure remote access, privilege escalation, and endpoint compliance within classified and unclassified network environments. Analyzes incident patterns to identify root causes and recommends long-term corrective actions to strengthen cybersecurity posture. Coordinates closely with SOC analysts to validate threat indicators and communicate relevant findings to operations teams. Maintains documentation of all actions taken in accordance with incident response playbooks and RMF control evidence requirements. Mentors junior specialists by conducting quality reviews of tickets, delivering hands-on training sessions, and developing improved triage workflows that enhance efficiency and accuracy. Functions with a high degree of autonomy and acts as the primary liaison between user support teams and enterprise cybersecurity operations.

CYBERSECURITY HELP DESK SPECIALIST IV

Functional Responsibility: Directs and oversees enterprise cybersecurity help desk functions that support thousands of users across geographically distributed environments. Establishes and enforces policies for incident triage, escalation, and reporting in accordance with NIST SP 800-61 and agency response frameworks. Designs performance metrics, key performance indicators, and training programs to ensure help desk personnel meet or exceed service-level agreements for response and resolution. Coordinates with senior cybersecurity leadership, SOC managers, and IT operations teams to address systemic vulnerabilities, recurring incidents, and major outage events. Develops strategies for proactive issue detection through automation, analytics, and threat intelligence integration. Leads after-action reviews to refine playbooks and maintain a culture of continuous improvement. Supervises multiple shifts or regional teams, manages staffing and performance evaluations, and provides regular updates to senior leadership on service health, incident trends, and resource needs.

CYBERSECURITY INFORMATION ASSURANCE / SECURITY SPECIALIST I

Functional Responsibility: Supports the implementation and maintenance of cybersecurity policies, procedures, and security controls across systems and applications. Performs routine security audits to verify adherence to established standards and assists with documenting control evidence for RMF packages. Reviews user access lists, validates account permissions, and reports deviations for corrective

action. Monitors logs and security tools to identify anomalies and assists senior personnel in analyzing potential incidents. Ensures that security configurations follow DISA STIGs and baseline hardening requirements. Operates under guidance, contributing to a culture of compliance and continuous security improvement.

CYBERSECURITY INFORMATION ASSURANCE / SECURITY SPECIALIST II

Functional Responsibility: Executes information assurance activities that protect enterprise systems from unauthorized access, misuse, and data loss. Conducts vulnerability scans, evaluates results, and coordinates remediation with system owners to maintain compliance with NIST SP 800-53 and agency risk management requirements. Reviews security documentation, supports POA&M tracking, and updates system security plans to reflect current configurations. Collaborates with system engineers to integrate security controls into system development and sustainment lifecycles. Participates in assessments and audits, providing findings and evidence to authorizing officials. Works independently on assigned systems while consulting senior specialists for risk acceptance and mitigation decisions.

CYBERSECURITY INFORMATION ASSURANCE / SECURITY SPECIALIST III

Functional Responsibility: Manages complex information assurance initiatives that span multiple systems and environments. Leads security control assessments, interprets audit findings, and recommends mitigation strategies to reduce organizational risk. Develops and enforces processes for continuous monitoring, data protection, and configuration management. Partners with network and cloud engineers to integrate automated compliance validation and reporting mechanisms. Reviews security artifacts for accuracy and completeness before submission to accreditation authorities. Coaches and mentors junior specialists, providing feedback on documentation quality and technical accuracy. Engages with incident response teams to ensure lessons learned translate into updated control baselines and security policies.

CYBERSECURITY INFORMATION ASSURANCE / SECURITY SPECIALIST IV

Functional Responsibility: Oversees enterprise-wide information assurance and cybersecurity compliance programs across hybrid and multi-cloud environments. Defines policy frameworks, governance models, and control strategies aligned with FISMA, NIST SP 800-37, and zero trust principles. Directs risk assessment and authorization activities, ensuring all systems maintain ATO in accordance with federal requirements. Coordinates enterprise audits, manages RMF documentation repositories, and ensures all POA&M actions are tracked to closure. Leads collaboration with system owners, program managers, and executives to align cybersecurity objectives with mission priorities. Evaluates the effectiveness of control implementations and guides architecture improvements to strengthen protection and resilience. Supervises information assurance teams, manages workload allocation, and establishes professional development paths to build organizational capability in cybersecurity compliance and governance.

CYBERSECURITY NETWORK ENGINEER I

Functional Responsibility: Assists in maintaining secure network infrastructure components supporting cybersecurity operations and mission systems. Configures switches, routers, and firewalls under supervision to enforce approved access control policies. Performs basic network monitoring, packet capture analysis, and device health checks to identify irregular activity. Implements security patches and firmware updates as directed by senior engineers. Documents configurations and topology changes to

maintain traceability for RMF and audit requirements. Learns to apply security principles such as segmentation, least privilege, and encryption in support of a defense-in-depth architecture.

CYBERSECURITY NETWORK ENGINEER II

Functional Responsibility: Implements and sustains secure network architectures that protect enterprise systems from unauthorized access and disruption. Deploys and manages security devices including firewalls, intrusion prevention systems, and virtual private networks across on-premises and cloud environments. Conducts configuration reviews and access control validations to ensure compliance with established cybersecurity policies. Monitors traffic patterns to detect anomalies and collaborates with SOC analysts to investigate potential incidents. Participates in vulnerability remediation by applying patches and reconfiguring devices in coordination with system administrators. Develops network diagrams, standard operating procedures, and security control documentation supporting continuous monitoring and accreditation activities.

CYBERSECURITY NETWORK ENGINEER III

Functional Responsibility: Designs and optimizes secure enterprise networks that integrate cloud, on-premises, and hybrid infrastructures. Configures advanced routing, segmentation, and encryption solutions to safeguard data-in-transit and maintain mission assurance under all operational conditions. Evaluates and deploys emerging technologies such as software-defined networking, zero trust segmentation, and network behavior analytics to improve visibility and resiliency. Conducts detailed forensic analysis of network incidents and implements corrective measures to prevent recurrence. Collaborates with cross-functional teams to ensure alignment between cybersecurity requirements, system performance, and operational needs. Provides mentorship to junior engineers, reviews design packages for accuracy, and supports the development of enterprise security baselines and policies.

CYBERSECURITY NETWORK ENGINEER IV

Functional Responsibility: Leads the design, implementation, and governance of secure network architectures across enterprise and mission-critical environments. Establishes strategy for network defense, segmentation, and monitoring that aligns with zero trust and NIST SP 800-207 principles. Directs teams in deploying scalable, resilient, and compliant connectivity solutions across classified and unclassified networks. Oversees the integration of continuous diagnostics, network access control, and threat intelligence feeds to enhance situational awareness. Coordinates network modernization efforts, evaluating technologies and defining standards that reduce attack surfaces and improve automation. Manages subordinate engineers, sets priorities, and allocates resources to ensure uninterrupted mission support. Provides senior technical guidance to leadership, develops enterprise architecture documentation, and validates that all network configurations maintain compliance with FISMA, DISA STIGs, and organizational security policies.

CYBERSECURITY NETWORK SPECIALIST I

Functional Responsibility: Monitors and supports daily network operations to ensure secure connectivity across mission environments. Performs device inventory validation, cable and port management, and basic configuration of security appliances under the direction of senior specialists. Reviews alerts from network monitoring tools, identifies routine performance issues, and reports findings for further analysis. Assists with documentation of diagrams, patch schedules, and device baselines to maintain compliance with

organizational and RMF requirements. Applies foundational cybersecurity concepts such as confidentiality, integrity, and availability to preserve secure data exchange throughout the enterprise.

CYBERSECURITY NETWORK SPECIALIST II

Functional Responsibility: Administers network components that enable secure communications and continuous operations across enterprise and tactical systems. Conducts configuration audits, implements access control lists, and applies encryption standards to protect sensitive information in transit. Tracks network utilization trends to forecast capacity needs and ensure efficient bandwidth allocation. Collaborates with cybersecurity engineers to apply system updates, resolve vulnerability findings, and verify remediation effectiveness. Prepares technical documentation supporting ATO packages and participates in functional testing of disaster recovery and continuity-of-operations plans. Operates independently within assigned areas and contributes to strengthening the organization's network security posture.

CYBERSECURITY NETWORK SPECIALIST III

Functional Responsibility: Coordinates the implementation and sustainment of complex network security solutions supporting hybrid and multi-cloud environments. Validates routing, firewall, and VPN configurations to maintain compliance with security policies and zero trust segmentation principles. Conducts packet-level analysis to isolate anomalies and supports the investigation of potential intrusions or data exfiltration events. Develops automation scripts to streamline configuration management and compliance reporting. Works closely with system owners to integrate network-level protections with endpoint and identity solutions. Provides guidance and training to junior specialists, reviews network documentation for accuracy, and recommends design improvements that enhance efficiency and threat resilience.

CYBERSECURITY NETWORK SPECIALIST IV

Functional Responsibility: Directs enterprise network security operations and leads initiatives that strengthen situational awareness, performance, and defense-in-depth capabilities. Defines policies for configuration management, access enforcement, and device monitoring across all enclaves. Oversees the deployment of advanced network analytics and continuous diagnostic systems that detect and respond to emerging threats in real time. Coordinates modernization projects that align infrastructure with zero trust and cloud-native networking frameworks. Partners with leadership to plan technology investments, ensuring that network operations support both mission assurance and compliance with federal cybersecurity mandates. Supervises subordinate specialists, establishes performance goals, and ensures that all network activities adhere to FISMA, DISA STIG, and NIST SP 800-53 requirements.

CYBERSECURITY PROJECT MANAGER I

Functional Responsibility: Coordinates assigned cybersecurity projects by organizing tasks, tracking milestones, and maintaining communication between technical teams and leadership. Assists with the preparation of project schedules, resource allocations, and risk logs. Monitors task completion, identifies potential delays, and reports status updates to senior managers. Supports the collection of deliverables and ensures documentation aligns with project standards and client expectations. Collaborates with engineers, analysts, and administrative staff to ensure all project activities comply with established security policies and quality guidelines. Demonstrates an understanding of project management methodologies and

cybersecurity fundamentals while gaining practical experience in coordinating small-scale technical efforts.

CYBERSECURITY PROJECT MANAGER II

Functional Responsibility: Manages the daily execution of cybersecurity initiatives, ensuring all deliverables meet technical, financial, and schedule goals. Develops and maintains project plans, manages risk registers, and coordinates task assignments across interdisciplinary teams. Tracks progress through performance metrics, conducts variance analyses, and ensures corrective actions are implemented in a timely manner. Facilitates meetings with government stakeholders, communicates project status, and documents key decisions to maintain transparency and accountability. Oversees compliance with cybersecurity frameworks such as NIST SP 800-37 and validates that deliverables align with organizational quality assurance processes. Anticipates resource needs, prioritizes work, and adjusts plans to sustain project momentum and mission relevance.

CYBERSECURITY PROJECT MANAGER III

Functional Responsibility: Leads complex cybersecurity projects encompassing multiple technical domains, workstreams, or task orders. Establishes integrated management plans that address scope, cost, schedule, and technical performance. Defines objectives, coordinates cross-functional activities, and ensures alignment between cybersecurity operations and mission outcomes. Implements governance frameworks to monitor earned value, manage risks, and maintain compliance with RMF and Zero Trust security requirements. Directs team activities, evaluates performance, and resolves issues that could affect delivery timelines or technical quality. Interfaces with contracting officers, program executives, and client leadership to communicate progress and adjust strategies to meet evolving needs. Mentors junior project managers and refines project management practices that enhance consistency and accountability across the organization.

CYBERSECURITY PROJECT MANAGER IV

Functional Responsibility: Oversees enterprise cybersecurity programs that integrate multiple projects, contracts, and geographically distributed teams. Defines strategic priorities, program governance structures, and long-term performance goals to ensure mission success and compliance with federal cybersecurity mandates. Manages program budgets, resource allocation, and staffing to achieve efficient and effective project delivery. Coordinates program-level reviews, risk assessments, and progress reporting for senior leadership and government stakeholders. Guides technical teams in applying RMF, NIST SP 800-53, and Zero Trust principles across systems and environments. Leads executive briefings and ensures consistent communication between project teams, customers, and decision makers. Supervises project managers, sets organizational priorities, and drives continuous improvement to strengthen delivery capability, accountability, and cybersecurity program maturity.

CYBERSECURITY SOFTWARE ENGINEER I

Functional Responsibility: Assists in developing and maintaining secure software components that support cybersecurity operations and system monitoring. Writes and tests basic scripts and application modules using approved coding standards and secure development practices. Reviews static analysis results under supervision, remediating vulnerabilities as directed by senior engineers. Supports configuration control processes to ensure code integrity and traceability throughout the development lifecycle. Contributes to documentation of release notes, build procedures, and change records. Gains

familiarity with DevSecOps principles, version control tools, and automated testing environments. Participates in sprint reviews and code walkthroughs, reinforcing an understanding of secure coding guidelines and federal software assurance requirements.

CYBERSECURITY SOFTWARE ENGINEER II

Functional Responsibility: Develops, integrates, and maintains secure applications that enable defensive cyber operations, incident response, and vulnerability management functions. Designs functional modules, implements APIs, and applies encryption or authentication mechanisms to protect data and enforce access control. Conducts secure code reviews, dynamic analysis, and remediation of findings from automated testing tools. Implements logging and error handling techniques that enhance auditability and forensic readiness. Collaborates with system administrators and cybersecurity analysts to ensure software aligns with mission objectives and agency cybersecurity policies. Prepares and updates technical documentation, including design specifications and deployment instructions. Works independently on assigned development tasks and contributes to the refinement of the organization's secure software engineering standards.

CYBERSECURITY SOFTWARE ENGINEER III

Functional Responsibility: Architects and sustains complex, security-focused software solutions supporting large-scale federal or defense cybersecurity programs. Leads the design and integration of modular, reusable codebases using microservices and containerized architectures. Implements advanced security controls such as token-based authentication, secure session management, and cryptographic validation of code integrity. Automates software testing and deployment pipelines to enforce continuous security throughout the DevSecOps lifecycle. Collaborates closely with risk management and quality assurance teams to verify RMF control implementation and maintain traceability of evidence. Analyzes application vulnerabilities and designs systemic corrections that enhance overall resiliency. Mentors junior engineers by conducting peer reviews, leading sprint retrospectives, and guiding adherence to secure development frameworks such as NIST SP 800-218 and OWASP. Contributes to modernization roadmaps that improve maintainability, scalability, and mission alignment.

CYBERSECURITY SOFTWARE ENGINEER IV

Functional Responsibility: Leads enterprise software security engineering efforts and defines the organization's approach to secure software development across multiple projects. Establishes strategies for secure design, coding, and deployment consistent with zero trust and supply chain risk management principles. Oversees implementation of CI/CD pipelines, ensuring security validation gates are embedded into every stage of the development process. Directs development of custom applications supporting vulnerability management, automation of RMF documentation, and advanced analytics. Evaluates emerging programming frameworks, libraries, and cloud-native tools for security compliance and operational suitability. Coordinates with stakeholders to align application architectures with broader enterprise cybersecurity objectives. Conducts technical risk assessments, defines security requirements for procurements, and validates contractor deliverables for compliance. Supervises software engineering teams, manages resources and timelines, and ensures all developed applications meet federal cybersecurity, FISMA, and NIST 800-series standards for confidentiality, integrity, and availability.

CYBERSECURITY SUBJECT MATTER EXPERT I

Functional Responsibility: Supports cybersecurity project teams by providing research, analysis, and technical input on specialized subjects such as network defense, risk management, and incident response. Assists in interpreting cybersecurity standards and applying control requirements to system configurations. Reviews technical documentation, contributes to security assessments, and helps ensure system compliance with organizational and federal requirements. Participates in meetings, captures technical notes, and assists senior staff in developing recommendations for system enhancements or process improvements. Demonstrates a foundational understanding of cybersecurity principles, methodologies, and technologies while gaining practical experience in applying expertise within project-specific environments.

CYBERSECURITY SUBJECT MATTER EXPERT II

Functional Responsibility: Provides targeted expertise in specific cybersecurity domains to enhance the performance, compliance, and resilience of mission systems. Conducts analysis of security controls, technical configurations, and risk indicators to identify areas for improvement. Advises teams on the practical implementation of cybersecurity best practices and supports integration of defensive technologies into enterprise environments. Drafts reports, policy recommendations, and procedures to ensure consistent application of cybersecurity standards. Collaborates with engineers, analysts, and administrators to align mission objectives with regulatory and technical requirements. Functions as a trusted technical resource capable of resolving moderate complexity issues and contributing to long-term security enhancements.

CYBERSECURITY SUBJECT MATTER EXPERT III

Functional Responsibility: Serves as a recognized advisor providing deep technical insight and advanced analytical support in specialized areas such as RMF compliance, cyber defense automation, or cloud security integration. Leads evaluations of security architectures and control implementations to ensure alignment with federal frameworks and mission objectives. Develops tailored mitigation strategies and implementation roadmaps for complex systems and operational environments. Conducts technical briefings, develops guidance materials, and facilitates workshops to enhance organizational knowledge and readiness. Partners with leadership to assess and prioritize cybersecurity initiatives, ensuring efficient allocation of resources to reduce organizational risk. Mentors mid-level professionals and contributes to the refinement of cybersecurity policies and methodologies across projects.

CYBERSECURITY SUBJECT MATTER EXPERT IV

Functional Responsibility: Functions as a principal consultant providing enterprise-level guidance on cybersecurity policy, governance, and architecture. Defines standards and frameworks that integrate risk management, zero trust, and continuous monitoring principles across multiple programs. Oversees high-impact assessments, develops enterprise risk strategies, and provides authoritative recommendations to leadership on compliance with FISMA, NIST, and DoD directives. Engages with external stakeholders, auditors, and interagency representatives to coordinate security initiatives and share best practices. Leads complex investigations and readiness assessments, ensuring systemic vulnerabilities are identified and remediated efficiently. Shapes enterprise cybersecurity policies and directs the creation of training programs that elevate organizational expertise and preparedness.

CYBERSECURITY SUBJECT MATTER EXPERT V

Functional Responsibility: Serves as the senior-most authority on cybersecurity strategy, policy, and technical innovation across the enterprise. Defines the overarching cybersecurity vision and ensures its integration into mission execution, IT modernization, and organizational governance. Advises executives and authorizing officials on strategic risk posture, compliance initiatives, and technology adoption. Establishes enterprise-wide standards for architecture, data protection, and zero trust implementation across multiple operational domains. Directs large-scale R&D efforts focused on emerging threats, automation, and AI-enabled defense capabilities. Represents the organization at national and interagency levels, influencing policy development and contributing to governmentwide cybersecurity advancements. Manages cross-functional teams, allocates resources, and oversees enterprise cybersecurity program execution to ensure all activities align with federal mandates and mission-critical objectives.

CYBERSECURITY SYSTEMS ADMINISTRATOR I

Functional Responsibility: Monitors and maintains secure computing environments supporting enterprise cybersecurity operations. Applies standard procedures for account provisioning, group policy updates, and system patching to preserve baseline compliance. Performs daily log reviews and verifies that antivirus definitions, operating system updates, and configuration standards remain current. Assists in resolving user issues related to authentication, permissions, and endpoint security. Documents maintenance actions, configuration changes, and incident tickets in accordance with established processes. Works closely with senior administrators to gain proficiency in security tools, vulnerability scanning utilities, and RMF control evidence collection.

CYBERSECURITY SYSTEMS ADMINISTRATOR II

Functional Responsibility: Administers secure server and workstation environments that support mission-critical cybersecurity functions. Implements and validates configuration baselines using automation tools and centralized management consoles. Conducts vulnerability remediation, access control maintenance, and patch deployment across both on-premises and cloud-based systems. Analyzes event logs, identifies system-level anomalies, and coordinates remediation with engineering and network teams. Creates and maintains scripts to automate backup, monitoring, and compliance reporting. Verifies that all changes are documented in accordance with configuration management and RMF requirements. Provides input on policy updates and technical procedures to improve system availability and security. Operates with limited supervision and participates in audits and control assessments to ensure ongoing adherence to federal cybersecurity standards.

CYBERSECURITY SYSTEMS ADMINISTRATOR III

Functional Responsibility: Oversees administration of complex, hybrid systems supporting enterprise cybersecurity and risk management missions. Plans and executes maintenance schedules, disaster recovery exercises, and configuration rollouts across multiple environments. Hardens systems through registry edits, secure service configurations, and advanced access control implementations that reinforce zero trust principles. Investigates elevated incidents involving unauthorized activity or malware detection, ensuring timely remediation and documentation. Integrates host-based intrusion detection, vulnerability management, and asset inventory tools to enhance situational awareness. Partners with cybersecurity engineers to validate compliance with DISA STIGs, NIST SP 800-53 controls, and organizational security policies. Provides mentorship to junior administrators, performs quality assurance checks, and contributes to optimization of incident response workflows and system baselining processes.

CYBERSECURITY SYSTEMS ADMINISTRATOR IV

Functional Responsibility: Directs enterprise system administration activities across distributed networks and mission systems, ensuring continuous compliance, resilience, and performance. Establishes governance frameworks for configuration management, patch validation, and access enforcement aligned with federal cybersecurity requirements and zero trust architecture. Designs procedures for system hardening, monitoring, and auditing to maintain consistent security postures across all enclaves. Coordinates multi-tier remediation campaigns, ensuring vulnerabilities and noncompliance items are resolved within defined SLAs. Oversees the integration of cloud and virtualization technologies into enterprise operations while maintaining secure baselines and RMF traceability. Engages senior leadership, authorizing officials, and auditors to communicate security status and corrective action progress. Leads a team of administrators and specialists, prioritizing workloads, defining key performance indicators, and cultivating professional growth within the cybersecurity operations workforce.

CYBERSECURITY SYSTEMS ENGINEER I

Functional Responsibility: Assists in the implementation and sustainment of secure information systems supporting cybersecurity and mission operations. Configures system components under guidance to ensure compliance with established baselines and technical standards. Participates in hardware and software installation, basic troubleshooting, and performance verification across local and virtual environments. Conducts initial testing of security patches, system updates, and configuration changes prior to deployment. Collects operational metrics and prepares reports to support RMF documentation. Collaborates with senior engineers to gain familiarity with security control integration, automation tools, and change management practices used in federal environments.

CYBERSECURITY SYSTEMS ENGINEER II

Functional Responsibility: Builds, configures, and optimizes systems that meet cybersecurity performance and compliance requirements across on-premises and cloud infrastructures. Integrates security tools such as endpoint protection, vulnerability scanning, and configuration enforcement platforms. Performs impact assessments of new updates, analyzes system logs to detect potential irregularities, and validates corrective actions. Designs scripts to automate administrative tasks, increase efficiency, and reduce configuration drift. Coordinates closely with administrators, developers, and network staff to ensure system interoperability and adherence to zero trust security principles. Prepares and maintains technical documentation including design diagrams, implementation plans, and risk mitigation strategies. Operates independently within assigned domains while ensuring systems remain aligned with mission objectives and cybersecurity mandates.

CYBERSECURITY SYSTEMS ENGINEER III

Functional Responsibility: Develops and maintains complex systems architectures that integrate advanced security controls, analytics, and automation capabilities. Leads planning and execution of system upgrades, migrations, and optimization efforts that enhance performance and resilience. Implements continuous monitoring, access control enforcement, and data protection mechanisms aligned with NIST and DoD cybersecurity policies. Evaluates new technologies for potential inclusion into enterprise environments and coordinates pilot testing to validate security effectiveness. Diagnoses and resolves high-impact incidents, documenting findings for root cause analysis and long-term remediation. Collaborates with accreditation authorities to ensure systems maintain valid authorizations and meet

evolving compliance requirements. Guides and trains junior engineers, provides peer review of technical deliverables, and contributes to standard operating procedures for secure system lifecycle management.

CYBERSECURITY SYSTEMS ENGINEER IV

Functional Responsibility: Directs the engineering, integration, and governance of enterprise systems supporting mission-critical cybersecurity capabilities. Defines the technical vision for secure infrastructure development, ensuring all configurations align with zero trust and resilience objectives. Oversees large-scale modernization initiatives that incorporate cloud, virtualization, and containerization technologies while maintaining RMF accreditation and system integrity. Establishes enterprise standards for automation, baseline enforcement, and secure configuration management across multiple enclaves. Leads technical risk assessments, evaluates interoperability between cybersecurity solutions, and coordinates complex problem resolution involving cross-domain systems. Advises senior leadership on system readiness, emerging threats, and compliance strategies that strengthen organizational resilience. Manages a team of engineers, sets technical priorities, allocates resources, and ensures all engineering activities maintain alignment with FISMA, NIST SP 800-53, and DISA STIG compliance frameworks.

CYBERSECURITY TEST ENGINEER I

Functional Responsibility: Performs foundational testing activities to verify the integrity, security, and performance of systems supporting cybersecurity operations. Executes predefined test scripts and procedures to evaluate compliance with functional and non-functional requirements. Records test results, identifies deviations, and assists with defect documentation for further review by senior testers. Supports setup and configuration of test environments, ensuring that hardware, software, and network settings align with approved baselines. Applies fundamental cybersecurity concepts such as least privilege, encryption, and authentication when validating configurations. Works under supervision to learn federal test methodologies, automated scanning tools, and RMF verification procedures.

CYBERSECURITY TEST ENGINEER II

Functional Responsibility: Conducts comprehensive security and functional testing of systems and applications to identify vulnerabilities, control deficiencies, and performance bottlenecks. Designs test cases that simulate real-world cyber threats and evaluates system responses to confirm resilience. Uses automated tools to perform static and dynamic analysis, penetration testing, and compliance validation. Analyzes results to determine root causes of issues and collaborates with developers and system engineers to implement corrective actions. Prepares detailed test reports, validation matrices, and evidence for RMF documentation. Participates in readiness assessments and configuration audits to ensure systems meet operational and security acceptance criteria. Operates with moderate independence and provides recommendations to enhance testing efficiency and coverage.

CYBERSECURITY TEST ENGINEER III

Functional Responsibility: Leads testing efforts for complex enterprise systems and cybersecurity platforms, ensuring comprehensive validation of security controls, reliability, and interoperability. Develops and manages test strategies, plans, and automation frameworks to improve consistency and repeatability of testing processes. Conducts risk-based assessments, vulnerability exploit validation, and boundary testing to verify system protection levels under simulated attack conditions. Coordinates cross-team collaboration to verify that test findings translate into measurable risk reductions. Evaluates test tool effectiveness, implements improvements, and aligns methodologies with evolving federal and agency

testing standards. Mentors junior test engineers by reviewing test artifacts, providing targeted training, and promoting adherence to cybersecurity testing best practices. Documents lessons learned to refine enterprise validation frameworks and enhance continuous monitoring activities.

CYBERSECURITY TEST ENGINEER IV

Functional Responsibility: Oversees enterprise-level cybersecurity testing and evaluation programs, defining organizational standards for validation, verification, and accreditation support. Establishes comprehensive test architectures integrating automation, analytics, and threat emulation capabilities that ensure consistent evaluation of system resilience across hybrid and cloud environments. Directs large-scale test campaigns that assess compliance with NIST SP 800-53, NIST SP 800-115, and agency-specific security control frameworks. Reviews and approves risk mitigation plans and test result summaries prior to submission to authorizing officials. Collaborates with senior leadership to shape enterprise testing strategy, ensuring that validation activities align with zero trust, DevSecOps, and continuous monitoring objectives. Supervises test engineering teams, manages resource allocation, and provides technical oversight for penetration testing, performance evaluation, and certification efforts. Ensures that all testing outcomes drive tangible security improvements and maintain compliance with federal cybersecurity mandates.

SIN 54151S PROFESSIONAL IT SERVICES

ID NUMBER	LCAT DESCRIPTION	YEAR 1 *04/2024*	YEAR 2 *04/2025*	YEAR 3 *04/2026*	YEAR 4 *04/2027*	YEAR 5 *04/2028*
03011001	Applications Developer I	$82.52	$85.82	$89.25	$92.82	$96.53
03011002	Applications Developer II	$106.36	$110.61	$115.03	$119.63	$124.42
03011003	Applications Developer III	$113.69	$118.24	$122.97	$127.89	$133.01
03011004	Applications Developer IV	$154.04	$160.20	$166.61	$173.27	$180.20
03011005	Applications Systems Analyst I	$81.60	$84.86	$88.25	$91.78	$95.45
03011006	Applications Systems Analyst II	$98.11	$102.03	$106.11	$110.35	$114.76
03011007	Applications Systems Analyst III	$124.70	$129.69	$134.88	$140.28	$145.89
03011008	Applications Systems Analyst IV	$154.95	$161.15	$167.60	$174.30	$181.27
03011009	Business Systems Analyst I	$97.19	$101.08	$105.12	$109.32	$113.69
03011010	Business Systems Analyst II	$108.19	$112.52	$117.02	$121.70	$126.57
03011011	Business Systems Analyst III	$120.11	$124.91	$129.91	$135.11	$140.51
03011012	Business Systems Analyst IV	$134.78	$140.17	$145.78	$151.61	$157.67
03011013	Configuration Management Specialist I	$84.35	$87.72	$91.23	$94.88	$98.68
03011014	Configuration Management Specialist II	$101.77	$105.84	$110.07	$114.47	$119.05
03011015	Configuration Management Specialist III	$122.86	$127.77	$132.88	$138.20	$143.73
03011016	Configuration Management Specialist IV	$152.20	$158.29	$164.62	$171.20	$178.05
03011017	Data Architect I	$90.77	$94.40	$98.18	$102.11	$106.19
03011018	Data Architect II	$129.28	$134.45	$139.83	$145.42	$151.24
03011019	Data Architect III	$139.37	$144.94	$150.74	$156.77	$163.04
03011020	Data Architect IV	$173.29	$180.22	$187.43	$194.93	$202.73
03011021	Database Specialist I	$91.69	$95.36	$99.17	$103.14	$107.27
03011022	Database Specialist II	$122.86	$127.77	$132.88	$138.20	$143.73
03011023	Database Specialist III	$152.20	$158.29	$164.62	$171.20	$178.05
03011024	Database Specialist IV	$165.04	$171.64	$178.51	$185.65	$193.08
03011025	Enterprise Architect I	$108.19	$112.52	$117.02	$121.70	$126.57
03011026	Enterprise Architect II	$132.03	$137.31	$142.80	$148.51	$154.45

ID NUMBER	LCAT DESCRIPTION	YEAR 1 *04/2024*	YEAR 2 *04/2025*	YEAR 3 *04/2026*	YEAR 4 *04/2027*	YEAR 5 *04/2028*
03011027	Enterprise Architect III	$154.95	$161.15	$167.60	$174.30	$181.27
03011028	Enterprise Architect IV	$189.79	$197.38	$205.28	$213.49	$222.03
03011029	Hardware Engineer I	$80.69	$83.92	$87.28	$90.77	$94.40
03011030	Hardware Engineer II	$99.02	$102.98	$107.10	$111.38	$115.84
03011031	Hardware Engineer III	$120.11	$124.91	$129.91	$135.11	$140.51
03011032	Hardware Engineer IV	$150.37	$156.38	$162.64	$169.15	$175.92
03011033	Helpdesk Specialist I	$59.60	$61.98	$64.46	$67.04	$69.72
03011034	Helpdesk Specialist II	$72.43	$75.33	$78.34	$81.47	$84.73
03011035	Helpdesk Specialist III	$92.60	$96.30	$100.15	$104.16	$108.33
03011036	Helpdesk Specialist IV	$110.03	$114.43	$119.01	$123.77	$128.72
03011037	Information Assurance/Security Specialist I	$101.77	$105.84	$110.07	$114.47	$119.05
03011038	Information Assurance/Security Specialist II	$118.28	$123.01	$127.93	$133.05	$138.37
03011039	Information Assurance/Security Specialist III	$134.78	$140.17	$145.78	$151.61	$157.67
03011040	Information Assurance/Security Specialist IV	$155.87	$162.10	$168.58	$175.32	$182.33
03011041	Network Engineer I	$110.03	$114.43	$119.01	$123.77	$128.72
03011042	Network Engineer II	$123.78	$128.73	$133.88	$139.24	$144.81
03011043	Network Engineer III	$165.04	$171.64	$178.51	$185.65	$193.08
03011044	Network Engineer IV	$189.79	$197.38	$205.28	$213.49	$222.03
03011045	Network Specialist I	$84.35	$87.72	$91.23	$94.88	$98.68
03011046	Network Specialist II	$114.61	$119.19	$123.96	$128.92	$134.08
03011047	Network Specialist III	$131.11	$136.35	$141.80	$147.47	$153.37
03011048	Network Specialist IV	$175.12	$182.12	$189.40	$196.98	$204.86
03011049	Program Manager I	$128.36	$133.49	$138.83	$144.38	$150.16
03011050	Program Manager II	$139.37	$144.94	$150.74	$156.77	$163.04
03011051	Program Manager III	$165.04	$171.64	$178.51	$185.65	$193.08
03011052	Program Manager IV	$189.79	$197.38	$205.28	$213.49	$222.03
03011053	Project Manager I	$105.44	$109.66	$114.05	$118.61	$123.35
03011054	Project Manager II	$122.86	$127.77	$132.88	$138.20	$143.73

ID NUMBER	LCAT DESCRIPTION	YEAR 1 *04/2024*	YEAR 2 *04/2025*	YEAR 3 *04/2026*	YEAR 4 *04/2027*	YEAR 5 *04/2028*
03011055	Project Manager III	$143.95	$149.71	$155.70	$161.93	$168.41
03011056	Project Manager IV	$165.04	$171.64	$178.51	$185.65	$193.08
03011057	Quality Assurance Specialist I	$88.94	$92.50	$96.20	$100.05	$104.05
03011058	Quality Assurance Specialist II	$101.77	$105.84	$110.07	$114.47	$119.05
03011059	Quality Assurance Specialist III	$122.86	$127.77	$132.88	$138.20	$143.73
03011060	Quality Assurance Specialist IV	$168.71	$175.46	$182.48	$189.78	$197.37
03011061	Software Engineer I	$94.44	$98.22	$102.15	$106.24	$110.49
03011062	Software Engineer II	$111.86	$116.33	$120.98	$125.82	$130.85
03011063	Software Engineer III	$134.78	$140.17	$145.78	$151.61	$157.67
03011064	Software Engineer IV	$148.53	$154.47	$160.65	$167.08	$173.76
03011065	Subject Matter Expert I	$92.60	$96.30	$100.15	$104.16	$108.33
03011066	Subject Matter Expert II	$134.78	$140.17	$145.78	$151.61	$157.67
03011067	Subject Matter Expert III	$176.96	$184.04	$191.40	$199.06	$207.02
03011068	Subject Matter Expert IV	$202.63	$210.74	$219.17	$227.94	$237.06
03011069	Subject Matter Expert V	$219.13	$227.90	$237.02	$246.50	$256.36
03011070	Systems Administrator I	$80.69	$83.92	$87.28	$90.77	$94.40
03011071	Systems Administrator II	$98.11	$102.03	$106.11	$110.35	$114.76
03011072	Systems Administrator III	$119.19	$123.96	$128.92	$134.08	$139.44
03011073	Systems Administrator IV	$137.53	$143.03	$148.75	$154.70	$160.89
03011074	Systems Engineer I	$94.44	$98.22	$102.15	$106.24	$110.49
03011075	Systems Engineer II	$111.86	$116.33	$120.98	$125.82	$130.85
03011076	Systems Engineer III	$128.36	$133.49	$138.83	$144.38	$150.16
03011077	Systems Engineer IV	$144.87	$150.66	$156.69	$162.96	$169.48
03011078	Technical Writer I	$66.93	$69.61	$72.39	$75.29	$78.30
03011079	Technical Writer II	$80.69	$83.92	$87.28	$90.77	$94.40
03011080	Technical Writer III	$100.86	$104.89	$109.09	$113.45	$117.99
03011081	Technical Writer IV	$123.78	$128.73	$133.88	$139.24	$144.81
03011082	Technology Engineer I	$120.11	$124.91	$129.91	$135.11	$140.51

ID NUMBER	LCAT DESCRIPTION	YEAR 1 *04/2024*	YEAR 2 *04/2025*	YEAR 3 *04/2026*	YEAR 4 *04/2027*	YEAR 5 *04/2028*
03011083	Technology Engineer II	$143.95	$149.71	$155.70	$161.93	$168.41
03011084	Technology Engineer III	$162.29	$168.78	$175.53	$182.55	$189.85
03011085	Technology Engineer IV	$176.96	$184.04	$191.40	$199.06	$207.02
03011086	Test Engineer I	$91.69	$95.36	$99.17	$103.14	$107.27
03011087	Test Engineer II	$113.69	$118.24	$122.97	$127.89	$133.01
03011088	Test Engineer III	$134.78	$140.17	$145.78	$151.61	$157.67
03011089	Test Engineer IV	$155.87	$162.10	$168.58	$175.32	$182.33
03011090	Voice/Data Communications Engineer I	$86.19	$89.64	$93.23	$96.96	$100.84
03011091	Voice/Data Communications Engineer II	$101.77	$105.84	$110.07	$114.47	$119.05
03011092	Voice/Data Communications Engineer III	$126.53	$131.59	$136.85	$142.32	$148.01
03011093	Voice/Data Communications Engineer IV	$165.04	$171.64	$178.51	$185.65	$193.08

SIN 54151S LABOR CATEGORY INFORMATION

Experience and Education

The following labor category minimum technical experience tables correspond to the prices offered in this submission.

All SIN 54151S Labor Categories Except Program Manager		
Level I	Junior	Bachelor's degree and 0 to 1 year of experience
Level II	Associate	Bachelor's degree and 2 to 4 years of experience
Level III	Senior	Bachelor's degree and 3 to 5 years of experience
Level IV	Master	Master's degree and 5 to 7 years of experience
Level V	Director	Master's degree and 7+ years of experience
SIN 54151S Program Manager		
Level I	Deputy	Bachelor's degree and 2 to 4 years of experience
Level II	Deputy	Bachelor's degree and 3 to 5 years of experience
Level III	Deputy	Master's degree and 5+ years of experience
Level IV	Deputy	Master's degree and 7+ years of experience

Degree Substitution

This serves as a guide to the experience and educational background of personnel typically found in each labor category. However, the experience of a resource is often a valid substitute for education. With this noted, the following information indicates where experience might be substituted for a degree as accepted by the customer.

All SIN 54151S Labor Categories Except Program Manager	
Equivalent to Bachelor's (Level I)	Associates degree + 2 or more years of relevant technical experience
	High School diploma + 4 or more years relevant technical experience
Equivalent to Bachelor's (Level II)	Associates degree + 3 or more years of relevant technical experience
	High School diploma + 6 or more years relevant technical experience
Equivalent to Bachelor's (Level III)	Associates degree + 5 or more years of relevant technical experience
	High School diploma + 7 or more years relevant technical experience
Equivalent to Master's (Level IV)	Bachelor's degree + 7 years of relevant technical experience
	Associates degree + 9 or more years of relevant technical experience
	High School diploma + 11 or more years relevant technical experience
Equivalent to Master's (Level V)	Bachelor's degree + 9 or more years of relevant technical experience
	Associates degree + 11 or more years of relevant technical experience
SIN 54151S Program Manager	
Equivalent to Bachelor's (Level I)	Associates degree + 5 or more years of relevant technical experience
	High School diploma + 7 or more years relevant technical experience
Equivalent to Bachelor's (Level II)	Associates degree + 7 or more years of relevant technical experience
	High School diploma + 9 or more years relevant technical experience
Equivalent to Master's (Level III)	Bachelor's degree + 9 years of relevant technical experience
	Associates degree + 11 or more years relevant technical experience
Equivalent to Master's (Level IV)	Bachelor's degree + 11 years of relevant technical experience
	Associates degree + 13 or more years relevant technical experience

Experience & Degree Substitution Equivalencies

*Experience exceeding the minimum shown may be substituted for education. Likewise, education exceeding the minimum shown may be substituted for experience.

LABOR CATEGORY	STANDARD QUALS		SUBSTITUTIONS				
	Min Education	Min Exp	PhD	Masters	Bachelors	Associates	High School
Applications Developer I	Bachelors	0	0	0	0	2	4
Applications Developer II	Bachelors	2	0	0	2	3	6
Applications Developer III	Bachelors	3	0	1	3	5	7
Applications Developer IV	Masters	5	3	5	7	9	11
Applications Systems Analyst I	Bachelors	0	0	0	0	2	4
Applications Systems Analyst II	Bachelors	2	0	0	2	3	6
Applications Systems Analyst III	Bachelors	3	0	1	3	5	7
Applications Systems Analyst IV	Masters	5	3	5	7	9	11
Business Systems Analyst I	Bachelors	0	0	0	0	2	4
Business Systems Analyst II	Bachelors	2	0	0	2	3	6
Business Systems Analyst III	Bachelors	3	0	1	3	5	7
Business Systems Analyst IV	Masters	5	3	5	7	9	11
Configuration Management Specialist I	Bachelors	0	0	0	0	2	4
Configuration Management Specialist II	Bachelors	2	0	0	2	3	6
Configuration Management Specialist III	Bachelors	3	0	1	3	5	7
Configuration Management Specialist IV	Masters	5	3	5	7	9	11
Data Architect I	Bachelors	0	0	0	0	2	4
Data Architect II	Bachelors	2	0	0	2	3	6
Data Architect III	Bachelors	3	0	1	3	5	7
Data Architect IV	Masters	5	3	5	7	9	11
Database Specialist I	Bachelors	0	0	0	0	2	4
Database Specialist II	Bachelors	2	0	0	2	3	6
Database Specialist III	Bachelors	3	0	1	3	5	7
Database Specialist IV	Masters	5	3	5	7	9	11
Enterprise Architect I	Bachelors	0	0	0	0	2	4
Enterprise Architect II	Bachelors	2	0	0	2	3	6
Enterprise Architect III	Bachelors	3	0	1	3	5	7
Enterprise Architect IV	Masters	5	3	5	7	9	11
Hardware Engineer I	Bachelors	0	0	0	0	2	4
Hardware Engineer II	Bachelors	2	0	0	2	3	6

LABOR CATEGORY	STANDARD QUALS	SUBSTITUTIONS					
	Min Education	Min Exp	PhD	Masters	Bachelors	Associates	High School
Hardware Engineer III	Bachelors	3	0	1	3	5	7
Hardware Engineer IV	Masters	5	3	5	7	9	11
Helpdesk Specialist I	Bachelors	0	0	0	0	2	4
Helpdesk Specialist II	Bachelors	2	0	0	2	3	6
Helpdesk Specialist III	Bachelors	3	0	1	3	5	7
Helpdesk Specialist IV	Masters	5	3	5	7	9	11
Information Assurance/ Security Specialist I	Bachelors	0	0	0	0	2	4
Information Assurance/ Security Specialist II	Bachelors	2	0	0	2	3	6
Information Assurance/ Security Specialist III	Bachelors	3	0	1	3	5	7
Information Assurance/ Security Specialist IV	Masters	5	3	5	7	9	11
Network Engineer I	Bachelors	0	0	0	0	2	4
Network Engineer II	Bachelors	2	0	0	2	3	6
Network Engineer III	Bachelors	3	0	1	3	5	7
Network Engineer IV	Masters	5	3	5	7	9	11
Network Specialist I	Bachelors	0	0	0	0	2	4
Network Specialist II	Bachelors	2	0	0	2	3	6
Network Specialist III	Bachelors	3	0	1	3	5	7
Network Specialist IV	Masters	5	3	5	7	9	11
Program Manager I	Bachelors	2	0	0	2	5	7
Program Manager II	Bachelors	3	0	1	3	7	9
Program Manager III	Masters	5	3	5	7	11	N/A
Program Manager IV	Masters	7	5	7	9	13	N/A
Project Manager I	Bachelors	0	0	0	0	2	4
Project Manager II	Bachelors	2	0	0	2	3	6
Project Manager III	Bachelors	3	0	1	3	5	7
Project Manager IV	Masters	5	3	5	7	9	11
Quality Assurance Specialist I	Bachelors	0	0	0	0	2	4
Quality Assurance Specialist II	Bachelors	2	0	0	2	3	6
Quality Assurance Specialist III	Bachelors	3	0	1	3	5	7
Quality Assurance Specialist IV	Masters	5	3	5	7	9	11
Software Engineer I	Bachelors	0	0	0	0	2	4
Software Engineer II	Bachelors	2	0	0	2	3	6
Software Engineer III	Bachelors	3	0	1	3	5	7

LABOR CATEGORY	STANDARD QUALS	SUBSTITUTIONS					
	Min Education	Min Exp	PhD	Masters	Bachelors	Associates	High School
Software Engineer IV	Masters	5	3	5	7	9	11
Subject Matter Expert I	Bachelors	0	0	0	0	2	4
Subject Matter Expert II	Bachelors	2	0	0	2	3	6
Subject Matter Expert III	Bachelors	3	0	1	3	5	7
Subject Matter Expert IV	Masters	5	3	5	7	9	11
Subject Matter Expert V	Masters	7	5	7	9	11	N/A
Systems Administrator I	Bachelors	0	0	0	0	2	4
Systems Administrator II	Bachelors	2	0	0	2	3	6
Systems Administrator III	Bachelors	3	0	1	3	5	7
Systems Administrator IV	Masters	5	3	5	7	9	11
Systems Engineer I	Bachelors	0	0	0	0	2	4
Systems Engineer II	Bachelors	2	0	0	2	3	6
Systems Engineer III	Bachelors	3	0	1	3	5	7
Systems Engineer IV	Masters	5	3	5	7	9	11
Technical Writer I	Bachelors	0	0	0	0	2	4
Technical Writer II	Bachelors	2	0	0	2	3	6
Technical Writer III	Bachelors	3	0	1	3	5	7
Technical Writer IV	Masters	5	3	5	7	9	11
Technology Engineer I	Bachelors	0	0	0	0	2	4
Technology Engineer II	Bachelors	2	0	0	2	3	6
Technology Engineer III	Bachelors	3	0	1	3	5	7
Technology Engineer IV	Masters	5	3	5	7	9	11
Test Engineer I	Bachelors	0	0	0	0	2	4
Test Engineer II	Bachelors	2	0	0	2	3	6
Test Engineer III	Bachelors	3	0	1	3	5	7
Test Engineer IV	Masters	5	3	5	7	9	11
Voice/Data Communications Engineer I	Bachelors	0	0	0	0	2	4
Voice/Data Communications Engineer II	Bachelors	2	0	0	2	3	6
Voice/Data Communications Engineer III	Bachelors	3	0	1	3	5	7
Voice/Data Communications Engineer IV	Masters	5	3	5	7	9	11

Place of Performance

The labor categories provided are for both Contractor and Customer facilities.

Clearance

The labor categories provided are for a Secret and below clearance.

Labor Category Descriptions

The descriptions provided describe the functional responsibilities, education, and experience requirements for each labor category.

APPLICATIONS DEVELOPER I

Functional Responsibility: Designs, develops, enhances, debugs, and implements software. Troubleshoots production problems related to software applications. Research, tests, builds, and coordinates the conversion and/or integration of new products based on client requirements. Designs and develop new software products or major enhancements to existing software. Addresses problems of systems integration, compatibility, and multiple platforms. Consults with project teams and end users to identify application requirements. Performs feasibility analysis on potential future projects to management. Assists in the evaluation and recommendation of application software packages, application integration and testing tools. Resolves problems with software and responds to suggestions for improvements and enhancements. Acts as team leader on projects. Instructs, assigns, directs, and checks the work of other software developers on development team. Participates in development of software user manuals. Applies fundamental concepts, processes, practices, and procedures on technical assignments. Performs work that requires practical experience and training. Work is performed under supervision.

APPLICATIONS DEVELOPER II

Functional Responsibility: Designs, develops, enhances, debugs, and implements software. Troubleshoots production problems related to software applications. Research, tests, builds, and coordinates the conversion and/or integration of new products based on client requirements. Designs and develop new software products or major enhancements to existing software. Addresses problems of systems integration, compatibility, and multiple platforms. Consults with project teams and end users to identify application requirements. Performs feasibility analysis on potential future projects to management. Assists in the evaluation and recommendation of application software packages, application integration and testing tools. Resolves problems with software and responds to suggestions for improvements and enhancements. Acts as team leader on projects. Instructs, assigns, directs, and checks the work of other software developers on development team. Participates in development of software user manuals. Possesses and applies expertise on multiple complex work assignments. Assignments may be broad in nature, requiring originality and innovation in determining how to accomplish tasks. Operates with appreciable latitude in developing methodology and presenting solutions to problems. Contributes to deliverables and performance metrics where applicable. Work is performed under supervision.

APPLICATIONS DEVELOPER III

Functional Responsibility: Design, develop, enhance, debugs, and implement software. Troubleshoots production problems related to software applications. Research, tests, builds, and coordinates the conversion and/or integration of new products based on client requirements. Designs and develop new software products or major enhancements to existing software.

Addresses problems of systems integration, compatibility, and multiple platforms. Consults with project teams and end users to identify application requirements. Performs feasibility analysis on potential future projects to management. Assists in the evaluation and recommendation of application software packages, application integration and testing tools. Resolves problems with software and responds to suggestions for improvements and enhancements. Acts as team leader on projects. Instructs, assigns, directs, and checks the work of other software developers on development team. Participates in development of software user manuals. Possesses and applies a comprehensive knowledge across key tasks and high impact assignments. Plans and leads major technology assignments. Evaluates performance results and recommends major changes affecting short-term project growth and success. Functions as a technical expert across multiple project assignments. May supervise others.

APPLICATIONS DEVELOPER IV

Functional Responsibility: Design, develop, enhance, debugs, and implement software. Troubleshoots production problems related to software applications. Research, tests, builds, and coordinates the conversion and/or integration of new products based on client requirements. Design and develop new software products or major enhancements to existing software. Addresses problems of systems integration, compatibility, and multiple platforms. Consults with project teams and end users to identify application requirements. Performs feasibility analysis on potential future projects to management. Assists in the evaluation and recommendation of application software packages, application integration and testing tools. Resolves problems with software and responds to suggestions for improvements and enhancements. Acts as team leader on projects. Instructs, assigns, directs, and checks the work of other software developers on development team. Participates in development of software user manuals. Provides technical/management leadership on major tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that technical requirements are met. Interactions involve client negotiations and interfacing with senior management. Decision making and domain knowledge may have a critical impact on overall project implementation. May supervise others.

APPLICATIONS SYSTEMS ANALYST I

Functional Responsibility: Formulates/defines system scope and objectives. Devises or modifies procedures to solve complex problems considering computer equipment capacity and limitations, operating time, and form of desired results. Prepares detailed specifications for programs. Assists in the design, development, testing, implementation, and documentation of new software and enhancements of existing applications. Works with project managers, developers, and end users to ensure application designs meet business requirements. Formulates/defines specifications for complex operating software programming applications or modifies/maintains complex existing applications using engineering releases and utilities from the manufacturer. Designs, codes, tests, debugs, and documents those programs. Provides overall operating system, such as sophisticated file maintenance routines, large telecommunications networks, computer accounting, and advanced mathematical/scientific software packages. Assists in all phases of software systems programming applications. Evaluates new and existing software products. Applies fundamental concepts, processes, practices, and procedures on technical assignments. Performs work that requires practical experience and training. Work is performed under supervision.

APPLICATIONS SYSTEMS ANALYST II

Functional Responsibility: Formulates/defines system scope and objectives. Devises or modifies procedures to solve complex problems considering computer equipment capacity and limitations, operating time, and form of desired results. Prepares detailed specifications for programs. Assists in the design, development, testing, implementation, and documentation of new software and enhancements of existing applications. Works with project managers, developers, and end users to ensure application designs meet business requirements. Formulates/defines specifications for complex operating software programming applications or modifies/maintains complex existing applications using engineering releases and utilities from the manufacturer. Designs, codes, tests, debugs, and documents those programs. Provides overall operating system, such as sophisticated file maintenance routines, large telecommunications networks, computer accounting, and advanced mathematical/scientific software packages. Assists in all phases of software systems programming applications. Evaluates new and existing software products. Possesses and applies expertise on multiple complex work assignments. Assignments may be broad in nature, requiring originality and innovation in determining how to accomplish tasks. Operates with appreciable latitude in developing methodology and presenting solutions to problems. Contributes to deliverables and performance metrics where applicable. Work is performed under supervision.

APPLICATIONS SYSTEMS ANALYST III

Functional Responsibility: Formulates/defines system scope and objectives. Devises or modifies procedures to solve complex problems considering computer equipment capacity and limitations, operating time, and form of desired results. Prepares detailed specifications for programs. Assists in the design, development, testing, implementation, and documentation of new software and enhancements of existing applications. Works with project managers, developers, and end users to ensure application designs meet business requirements. Formulates/defines specifications for complex operating software programming applications or modifies/maintains complex existing applications using engineering releases and utilities from the manufacturer. Designs, codes, tests, debugs, and documents those programs. Provides overall operating system, such as sophisticated file maintenance routines, large telecommunications networks, computer accounting, and advanced mathematical/scientific software packages. Assists in all phases of software systems programming applications. Evaluates new and existing software products. Possesses and applies a comprehensive knowledge across key tasks and high impact assignments. Plans and leads major technology assignments. Evaluates performance results and recommends major changes affecting short-term project growth and success. Functions as a technical expert across multiple project assignments. May supervise others.

APPLICATIONS SYSTEMS ANALYST IV

Functional Responsibility: Formulates/defines system scope and objectives. Devises or modifies procedures to solve complex problems considering computer equipment capacity and limitations, operating time, and form of desired results. Prepares detailed specifications for programs. Assists in the design, development, testing, implementation, and documentation of new software and enhancements of existing applications. Works with project managers, developers, and end users to ensure application designs meet business requirements. Formulates/defines specifications for complex operating software programming applications or modifies/maintains complex existing applications using engineering releases and utilities from the manufacturer. Designs, codes, tests,

debugs, and documents those programs. Provides overall operating system, such as sophisticated file maintenance routines, large telecommunications networks, computer accounting, and advanced mathematical/scientific software packages. Assists in all phases of software systems programming applications. Evaluates new and existing software products. Provides technical/management leadership on major tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that technical requirements are met. Interactions involve client negotiations and interfacing with senior management. Decision making and domain knowledge may have a critical impact on overall project implementation. May supervise others.

BUSINESS SYSTEMS ANALYST I

Functional Responsibility: Formulates and defines systems scope and objectives based on both user needs and a thorough understanding of business systems and industry requirements. Devises or modifies procedures to solve complex problems considering computer equipment capacity and limitations, operation time, and form of desired results. Includes analysis of business and user needs, documentation of requirements, and translation into proper system requirements specifications. Work is performed under supervision.

BUSINESS SYSTEMS ANALYST II

Functional Responsibility: Formulates and defines systems scope and objectives based on both user needs and a thorough understanding of business systems and industry requirements. Devises or modifies procedures to solve complex problems considering computer equipment capacity and limitations, operation time, and form of desired results. Includes analysis of business and user needs, documentation of requirements, and translation into proper system requirements specifications. Contributes to deliverables and performance metrics where applicable. Work is performed under supervision.

BUSINESS SYSTEMS ANALYST III

Functional Responsibility: Formulates and defines systems scope and objectives based on both user needs and a thorough understanding of business systems and industry requirements. Devises or modifies procedures to solve complex problems considering computer equipment capacity and limitations, operation time, and form of desired results. Includes analysis of business and user needs, documentation of requirements, and translation into proper system requirements specifications. Contributes to deliverables and performance metrics where applicable. Possesses and applies a comprehensive knowledge across key tasks and high impact assignments. Plans and leads major technology assignments. Evaluates performance results and recommends major changes affecting short-term project growth and success. Functions as a technical expert across multiple project assignments. May supervise others.

BUSINESS SYSTEMS ANALYST IV

Functional Responsibility: Formulates and defines systems scope and objectives based on both user needs and a thorough understanding of business systems and industry requirements. Devises or modifies procedures to solve complex problems considering computer equipment capacity and limitations, operation time, and form of desired results. Includes analysis of business and user

needs, documentation of requirements, and translation into proper system requirements specifications. Provides consultation on complex projects and is considered the top-level contributor/specialist of most phases of systems analysis, while considering the business implications of the application of technology to the current and future business environment. Provides technical/management leadership on major tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that technical requirements are met. Interactions involve client negotiations and interfacing with senior management. Decision making and domain knowledge may have a critical impact on overall project implementation. May supervise others.

CONFIGURATION MANAGEMENT SPECIALIST I

Functional Responsibility: Provides configuration management planning. Describes provisions for configuration identification, change control, configuration status accounting, and configuration audits. Regulates the change process so that only approved and validated changes are incorporated into product documents and related software. Possesses and applies expertise on multiple complex work assignments. Assignments may be broad in nature, requiring originality and innovation in determining how to accomplish tasks. Operates with guidance in developing methodology and presenting solutions to problems. Work is performed under supervision.

CONFIGURATION MANAGEMENT SPECIALIST II

Functional Responsibility: Provides configuration management planning. Describes provisions for configuration identification, change control, configuration status accounting, and configuration audits. Regulates the change process so that only approved and validated changes are incorporated into product documents and related software. Possesses and applies expertise on multiple complex work assignments. Assignments may be broad in nature, requiring originality and innovation in determining how to accomplish tasks. Operates with appreciable latitude in developing methodology and presenting solutions to problems. Contributes to deliverables and performance metrics where applicable. Work is performed under supervision.

CONFIGURATION MANAGEMENT SPECIALIST III

Functional Responsibility: Provides configuration management planning. Describes provisions for configuration identification, change control, configuration status accounting, and configuration audits. Regulates the change process so that only approved and validated changes are incorporated into product documents and related software. Possesses and applies a comprehensive knowledge across key tasks and high impact assignments. Plans and leads major technology assignments. Evaluates performance results and recommends major changes affecting short-term project growth and success. Functions as a technical expert across multiple project assignments. May supervise others.

CONFIGURATION MANAGEMENT SPECIALIST IV

Functional Responsibility: Provides configuration management planning. Describes provisions for configuration identification, change control, configuration status accounting, and configuration audits. Regulates the change process so that only approved and validated changes are incorporated into product documents and related software. Provides technical/management leadership on major

tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that technical requirements are met. Interactions involve client negotiations and interfacing with senior management. Decision making and domain knowledge may have a critical impact on overall project implementation. May supervise others.

DATA ARCHITECT I

Functional Responsibility: Designs and builds relational databases. Performs data access analysis design, and archive/recovery design and implementation. Develop strategies for data acquisitions, archive recovery, and implementation of a database. Works in a data warehouse environment, which includes data design, database architecture, and metadata repository creation. Translates business needs into long- term architecture solutions. Defines, designs, and builds dimensional databases. Develops data warehousing blueprints, evaluating hardware and software platforms, and integrating systems. Reviews and develops object and data models and the metadata repository to structure the data for better management and quicker access. Work is performed under supervision.

DATA ARCHITECT II

Functional Responsibility: Designs and builds relational databases. Performs data access analysis design, and archive/recovery design and implementation. Develop strategies for data acquisitions, archive recovery, and implementation of a database. Works in a data warehouse environment, which includes data design, database architecture, and metadata repository creation. Translates business needs into long- term architecture solutions. Defines, designs, and builds dimensional databases. Develops data warehousing blueprints, evaluating hardware and software platforms, and integrating systems. Reviews and develops object and data models and the metadata repository to structure the data for better management and quicker access. Contributes to deliverables and performance metrics where applicable. Work is performed under supervision.

DATA ARCHITECT III

Functional Responsibility: Designs and builds relational databases. Performs data access analysis design, and archive/recovery design and implementation. Develop strategies for data acquisitions, archive recovery, and implementation of a database. Works in a data warehouse environment, which includes data design, database architecture, and metadata repository creation. Translates business needs into long- term architecture solutions. Defines, designs, and builds dimensional databases. Develops data warehousing blueprints, evaluating hardware and software platforms, and integrating systems. Reviews and develops object and data models and the metadata repository to structure the data for better management and quicker access. Contributes to deliverables and performance metrics where applicable. Possesses and applies a comprehensive knowledge across key tasks and high impact assignments. Plans and leads major technology assignments. Evaluates performance results and recommends major changes affecting short-term project growth and success. Functions as a technical expert across multiple project assignments. May supervise others.

DATA ARCHITECT IV

Functional Responsibility: Designs and builds relational databases. Performs data access analysis design, and archive/recovery design and implementation. Develop strategies for data acquisitions, archive recovery, and implementation of a database. Works in a data warehouse environment, which includes data design, database architecture, and metadata repository creation. Translates business needs into long- term architecture solutions. Defines, designs, and builds dimensional databases. Develops data warehousing blueprints, evaluating hardware and software platforms, and integrating systems. Reviews and develops object and data models and the metadata repository to structure the data for better management and quicker access. Provides technical/management leadership on major tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that technical requirements are met. Interactions involve client negotiations and interfacing with senior management. Decision making and domain knowledge may have a critical impact on overall project implementation. May supervise others.

DATABASE SPECIALIST I

Functional Responsibility: Provides all activities related to the administration of computerized databases. Projects long-range requirements for database administration and design in conjunction with other managers in the information systems function. Designs, creates, and maintains databases in a client/server environment. Conducts quality control and auditing of databases in a client/server environment to ensure accurate and appropriate use of data. Advises users on access to various client/server databases. Designs, implements, and maintains complex databases with respect to JCL, access methods, access time, device allocation, validation checks, organization, protection and security, documentation, and statistical methods. Applies knowledge and experience with database technologies, development methodologies, and front-end (e.g., COGNOS)/back-end programming languages (e.g., SQL). Performs database programming and supports systems design. Includes maintenance of database dictionaries, overall monitoring of standards and procedures, file design and storage, and integration of systems through database design. fundamental concepts, processes, practices, and procedures on technical assignments. Performs work that requires practical experience and training. Work is performed under supervision.

DATABASE SPECIALIST II

Functional Responsibility: Provides all activities related to the administration of computerized databases. Projects long-range requirements for database administration and design in conjunction with other managers in the information systems function. Designs, creates, and maintains databases in a client/server environment. Conducts quality control and auditing of databases in a client/server environment to ensure accurate and appropriate use of data. Advises users on access to various client/server databases. Designs, implements, and maintains complex databases with respect to JCL, access methods, access time, device allocation, validation checks, organization, protection and security, documentation, and statistical methods. Applies knowledge and experience with database technologies, development methodologies, and front-end (e.g., COGNOS)/back-end programming languages (e.g., SQL). Performs database programming and supports systems design. Includes maintenance of database dictionaries, overall monitoring of

standards and procedures, file design and storage, and integration of systems through database design. Possesses and applies expertise on multiple complex work assignments. Assignments may be broad in nature, requiring originality and innovation in determining how to accomplish tasks. Operates with appreciable latitude in developing methodology and presenting solutions to problems. Contributes to deliverables and performance metrics where applicable. Work is performed under supervision.

DATABASE SPECIALIST III

Functional Responsibility: Provides all activities related to the administration of computerized databases. Projects long-range requirements for database administration and design in conjunction with other managers in the information systems function. Designs, creates, and maintains databases in a client/server environment. Conducts quality control and auditing of databases in a client/server environment to ensure accurate and appropriate use of data. Advises users on access to various client/server databases. Designs, implements, and maintains complex databases with respect to JCL, access methods, access time, device allocation, validation checks, organization, protection and security, documentation, and statistical methods. Applies knowledge and experience with database technologies, development methodologies, and front-end (e.g., COGNOS)/back-end programming languages (e.g., SQL). Performs database programming and supports systems design. Includes maintenance of database dictionaries, overall monitoring of standards and procedures, file design and storage, and integration of systems through database design. Possesses and applies a comprehensive knowledge across key tasks and high impact assignments. Plans and leads major technology assignments. Evaluates performance results and recommends major changes affecting short-term project growth and success. Functions as a technical expert across multiple project assignments. May supervise others.

DATABASE SPECIALIST IV

Functional Responsibility: Provides all activities related to the administration of computerized databases. Projects long-range requirements for database administration and design in conjunction with other managers in the information systems function. Designs, creates, and maintains databases in a client/server environment. Conducts quality control and auditing of databases in a client/server environment to ensure accurate and appropriate use of data. Advises users on access to various client/server databases. Designs, implements, and maintains complex databases with respect to JCL, access methods, access time, device allocation, validation checks, organization, protection and security, documentation, and statistical methods. Applies knowledge and experience with database technologies, development methodologies, and front-end (e.g., COGNOS)/back-end programming languages (e.g., SQL). Performs database programming and supports systems design. Includes maintenance of database dictionaries, overall monitoring of standards and procedures, file design and storage, and integration of systems through database design. Provides technical/management leadership on major tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that technical requirements are met. Interactions involve client negotiations and interfacing with senior management. Decision making and domain knowledge may have a critical impact on overall project implementation. May supervise others.

ENTERPRISE ARCHITECT I

Functional Responsibility: Design and develops complex business solutions using a variety of computer technologies. Independently performs a variety of system design and engineering tasks, which are broad in nature and are concerned with design and implementation of major enterprise systems development and integration, including supporting personnel, hardware, software, and support facilities and/or equipment. Considered a Subject Matter Expert (SME) in one or more specific areas of computer system design and networking. Applies fundamental concepts, processes, practices, and procedures on technical assignments. Performs work that requires practical experience and training. Work is performed under supervision.

ENTERPRISE ARCHITECT II

Functional Responsibility: Design and develops complex business solutions using a variety of computer technologies. Independently performs a variety of system design and engineering tasks, which are broad in nature and are concerned with design and implementation of major enterprise systems development and integration, including supporting personnel, hardware, software, and support facilities and/or equipment. Considered a Subject Matter Expert (SME) in one or more specific areas of computer system design and networking. Applies knowledge of complex concepts and techniques to develop and implement automated solutions to engineering, scientific, or business data acquisition and management problems. Uses scientific and engineering logic to independently identify conceptual or theoretical solutions to problems of technology systems hardware or software design and operation. Evaluates and recommends optimum solutions balancing specific project needs with economic constraints. Formulates architectural design, functional specification, interfaces, and documentation of computer systems considering system interrelationships, operating modes, and equipment configurations. Responsible for developing project plans, justifications, guidelines, and controls. Possesses and applies expertise on multiple complex work assignments. Assignments may be broad in nature, requiring originality and innovation in determining how to accomplish tasks. Operates with appreciable latitude in developing methodology and presenting solutions to problems. Contributes to deliverables and performance metrics where applicable. Work is performed under supervision.

ENTERPRISE ARCHITECT III

Functional Responsibility: Design and develops complex business solutions using a variety of computer technologies. Independently performs a variety of system design and engineering tasks, which are broad in nature and are concerned with design and implementation of major enterprise systems development and integration, including supporting personnel, hardware, software, and support facilities and/or equipment. Considered a Subject Matter Expert (SME) in one or more specific areas of computer system design and networking. Applies knowledge of complex concepts and techniques to develop and implement automated solutions to engineering, scientific, or business data acquisition and management problems. Uses scientific and engineering logic to independently identify conceptual or theoretical solutions to problems of technology systems hardware or software design and operation. Evaluates and recommends optimum solutions balancing specific project needs with economic constraints. Formulates architectural design, functional specification, interfaces, and documentation of computer systems considering system interrelationships, operating modes, and equipment configurations. Responsible for developing project plans, justifications, guidelines, and controls. Possesses and applies expertise on multiple

complex work assignments. Assignments may be broad in nature, requiring originality and innovation in determining how to accomplish tasks. Operates with appreciable latitude in developing methodology and presenting solutions to problems. Contributes to deliverables and performance metrics where applicable. May supervise others.

ENTERPRISE ARCHITECT IV

Functional Responsibility: Design and develop complex business solutions using a variety of computer technologies. Independently performs a variety of system design and engineering tasks, which are broad in nature and are concerned with design and implementation of major enterprise systems development and integration, including supporting personnel, hardware, software, and support facilities and/or equipment. Considered a Subject Matter Expert (SME) in one or more specific areas of computer system design and networking. Applies knowledge of complex concepts and techniques to develop and implement automated solutions to engineering, scientific, or business data acquisition and management problems. Uses scientific and engineering logic to independently identify conceptual or theoretical solutions to problems of technology systems hardware or software design and operation. Evaluates and recommends optimum solutions balancing specific project needs with economic constraints. Formulates architectural design, functional specification, interfaces, and documentation of computer systems considering system interrelationships, operating modes, and equipment configurations. Responsible for developing project plans, justifications, guidelines, and controls. Provides technical/management leadership on major tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that technical requirements are met. Interactions involve client negotiations and interfacing with senior management. Decision making and domain knowledge may have a critical impact on overall project implementation. May supervise others.

HARDWARE ENGINEER I

Functional Responsibility: Provide analysis related to the design, development, and implementation of hardware for products. Develops test strategies, devices, and systems. Perform stress and performance tests on a variety of computer or network hardware including circuit boards, processors, and wiring. Applies fundamental concepts, processes, practices, and procedures on technical assignments. Performs work that requires practical experience and training. Work is performed under supervision.

HARDWARE ENGINEER II

Functional Responsibility: Provide analysis related to the design, development, and implementation of hardware for products. Develops test strategies, devices, and systems. Perform stress and performance tests on a variety of computer or network hardware including circuit boards, processors, and wiring. Applies fundamental concepts, processes, practices, and procedures on technical assignments. Performs work that requires practical experience and training. Possesses and applies expertise on multiple complex work assignments. Assignments may be broad in nature, requiring originality and innovation in determining how to accomplish tasks. Operates with appreciable latitude in developing methodology and presenting solutions to

problems. Contributes to deliverables and performance metrics where applicable. Work is performed under supervision.

HARDWARE ENGINEER III

Functional Responsibility: Provide analysis related to the design, development, and implementation of hardware for products. Develops test strategies, devices, and systems. Perform stress and performance tests on a variety of computer or network hardware including circuit boards, processors, and wiring. fundamental concepts, processes, practices, and procedures on technical assignments. Performs work that requires practical experience and training. Possesses and applies a comprehensive knowledge across key tasks and high impact assignments. Plans and leads major technology assignments. Evaluates performance results and recommends major changes affecting short-term project growth and success. Functions as a technical expert across multiple project assignments. May supervise others.

HARDWARE ENGINEER IV

Functional Responsibility: Lead analysis related to the design, development, and implementation of hardware for products. Develops test strategies, devices, and systems. Perform stress and performance tests on a variety of computer or network hardware including circuit boards, processors, and wiring. fundamental concepts, processes, practices, and procedures on technical assignments. Performs work that requires practical experience and training. Possesses and applies a comprehensive knowledge across key tasks and high impact assignments. Plans and leads major technology assignments. Evaluates performance results and recommends major changes affecting short-term project growth and success. Functions as a technical expert across multiple project assignments. Decision making and domain knowledge may have a critical impact on overall project implementation. May supervise others.

HELP DESK SPECIALIST I

Functional Responsibility: Respond to and diagnoses problems through discussion with users. Ensures a timely process through which problems are controlled. Includes problem recognition, research, isolation, resolution, and follow-up steps. Supervises operation of help desk and serves as focal point for customer concerns. Provides support to end users on a variety of issues. Identifies, researches, and resolves technical problems. Responds to telephone calls, email, and personnel requests for technical support. Documents, tracks, and monitors the problem to ensure a timely resolution. Provides second-tier support to end users for either PC, server, or mainframe applications or hardware. Interact with network services, software systems engineering, and/or applications development to restore service and/or identify and correct core problems. Simulates or recreates user problems to resolve operating difficulties. Recommend systems modifications to reduce user problems. Applies fundamental concepts, processes, practices, and procedures on technical assignments. Performs work that requires practical experience and training. Work is performed under supervision.

HELP DESK SPECIALIST II

Functional Responsibility: Respond to and diagnoses problems through discussion with users. Ensures a timely process through which problems are controlled. Includes problem recognition, research, isolation, resolution, and follow-up steps. Supervises operation of help desk and serves

as focal point for customer concerns. Provides support to end users on a variety of issues. Identifies, researches, and resolves technical problems. Responds to telephone calls, email, and personnel requests for technical support. Documents, tracks, and monitors the problem to ensure a timely resolution. Provides second-tier support to end users for either PC, server, or mainframe applications or hardware. Interact with network services, software systems engineering, and/or applications development to restore service and/or identify and correct core problems. Simulates or recreates user problems to resolve operating difficulties. Recommend systems modifications to reduce user problems. Possesses and applies expertise on multiple complex work assignments. Assignments may be broad in nature, requiring originality and innovation in determining how to accomplish tasks. Operates with appreciable latitude in developing methodology and presenting solutions to problems. Contributes to deliverables and performance metrics where applicable. Work is performed under supervision.

HELP DESK SPECIALIST III

Functional Responsibility: Respond to and diagnoses problems through discussion with users. Ensures a timely process through which problems are controlled. Includes problem recognition, research, isolation, resolution, and follow-up steps. Supervises operation of help desk and serves as focal point for customer concerns. Provides support to end users on a variety of issues. Identifies, researches, and resolves technical problems. Responds to telephone calls, email, and personnel requests for technical support. Documents, tracks, and monitors the problem to ensure a timely resolution. Provides second-tier support to end users for either PC, server, or mainframe applications or hardware. Interact with network services, software systems engineering, and/or applications development to restore service and/or identify and correct core problems. Simulates or recreates user problems to resolve operating difficulties. Recommend systems modifications to reduce user problems. Possesses and applies a comprehensive knowledge across key tasks and high impact assignments. Plans and leads major technology assignments. Evaluates performance results and recommends major changes affecting short-term project growth and success. Functions as a technical expert across multiple project assignments. May supervise others.

HELP DESK SPECIALIST IV

Functional Responsibility: Respond to and diagnoses problems through discussion with users. Ensures a timely process through which problems are controlled. Includes problem recognition, research, isolation, resolution, and follow-up steps. Supervises operation of help desk and serves as focal point for customer concerns. Provides support to end users on a variety of issues. Identifies, researches, and resolves technical problems. Responds to telephone calls, email, and personnel requests for technical support. Documents, tracks, and monitors the problem to ensure a timely resolution. Provides second-tier support to end users for either PC, server, or mainframe applications or hardware. Interact with network services, software systems engineering, and/or applications development to restore service and/or identify and correct core problems. Simulates or recreates user problems to resolve operating difficulties. Recommend systems modifications to reduce user problems. Provides technical/management leadership on major tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that technical requirements are met. Interactions involve client negotiations and interfacing with senior management. Decision making

and domain knowledge may have a critical impact on overall project implementation. May supervise others.

INFORMATION ASSURANCE/SECURITY SPECIALIST I

Functional Responsibility: Determines enterprise information assurance and security standards. Develops and implements information assurance/security standards and procedures. Coordinates, develops, and evaluates security programs for an organization. Recommend information assurance/security solutions to support customer requirements. Identifies, reports, and resolves security violations. Establishes and satisfies information assurance and security requirements based upon the analysis of user, policy, regulatory, and resource demands. Supports customers at the highest levels in the development and implementation of doctrine and policies. Apply know-how to government and commercial common user systems, as well as to dedicated special purpose systems requiring specialized security features and procedures. Performs analysis, design, and development of security features for system architectures. Analyzes and defines security requirements for computer systems, which may include mainframes, workstations, and personal computers. Designs, develops, engineers, and implements solutions that meet security requirements. Provides integration and implementation of the computer system security solution. Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems. Performs vulnerability/risk analyses of computer systems and applications during all phases of the system development life cycle. Ensures that all information systems are functional and secure. Applies fundamental concepts, processes, practices, and procedures on technical assignments. Performs work that requires practical experience and training. Work is performed under supervision.

INFORMATION ASSURANCE/SECURITY SPECIALIST II

Functional Responsibility: Determines enterprise information assurance and security standards. Develops and implements information assurance/security standards and procedures. Coordinates, develops, and evaluates security programs for an organization. Recommend information assurance/security solutions to support customer requirements. Identifies, reports, and resolves security violations. Establishes and satisfies information assurance and security requirements based upon the analysis of user, policy, regulatory, and resource demands. Supports customers at the highest levels in the development and implementation of doctrine and policies. Apply know-how to government and commercial common user systems, as well as to dedicated special purpose systems requiring specialized security features and procedures. Performs analysis, design, and development of security features for system architectures. Analyzes and defines security requirements for computer systems, which may include mainframes, workstations, and personal computers. Designs, develops, engineers, and implements solutions that meet security requirements. Provides integration and implementation of the computer system security solution. Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems. Performs vulnerability/risk analyses of computer systems and applications during all phases of the system development life cycle. Ensures that all information systems are functional and secure. Possesses and applies expertise on multiple complex work assignments. Assignments may be broad in nature, requiring originality and innovation in determining how to accomplish tasks. Operates with appreciable latitude in developing methodology and presenting solutions to problems. Contributes to deliverables and performance metrics where applicable. Work is performed under supervision.

INFORMATION ASSURANCE/SECURITY SPECIALIST III

Functional Responsibility: Determines enterprise information assurance and security standards. Develops and implements information assurance/security standards and procedures. Coordinates, develops, and evaluates security programs for an organization. Recommend information assurance/security solutions to support customer requirements. Identifies, reports, and resolves security violations. Establishes and satisfies information assurance and security requirements based upon the analysis of user, policy, regulatory, and resource demands. Supports customers at the highest levels in the development and implementation of doctrine and policies. Apply know-how to government and commercial common user systems, as well as to dedicated special purpose systems requiring specialized security features and procedures. Performs analysis, design, and development of security features for system architectures. Analyzes and defines security requirements for computer systems, which may include mainframes, workstations, and personal computers. Designs, develops, engineers, and implements solutions that meet security requirements. Provides integration and implementation of the computer system security solution. (l) Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems. Performs vulnerability/risk analyses of computer systems and applications during all phases of the system development life cycle. Ensures that all information systems are functional and secure. Possesses and applies a comprehensive knowledge across key tasks and high impact assignments. Plans and leads major technology assignments. Evaluates performance results and recommends major changes affecting short-term project growth and success. Functions as a technical expert across multiple project assignments. May supervise others.

INFORMATION ASSURANCE/SECURITY SPECIALIST IV

Functional Responsibility: Determines enterprise information assurance and security standards. Develops and implements information assurance/security standards and procedures. Coordinates, develops, and evaluates security programs for an organization. Recommend information assurance/security solutions to support customer requirements. Identifies, reports, and resolves security violations. Establishes and satisfies information assurance and security requirements based upon the analysis of user, policy, regulatory, and resource demands. Supports customers at the highest levels in the development and implementation of doctrine and policies. Apply know-how to government and commercial common user systems, as well as to dedicated special purpose systems requiring specialized security features and procedures. Performs analysis, design, and development of security features for system architectures. Analyzes and defines security requirements for computer systems, which may include mainframes, workstations, and personal computers. Designs, develops, engineers, and implements solutions that meet security requirements. Provides integration and implementation of the computer system security solution. Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems. Performs vulnerability/risk analyses of computer systems and applications during all phases of the system development life cycle. Ensures that all information systems are functional and secure. Provides technical/management leadership on major tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that technical requirements are met. Interactions involve client negotiations and interfacing with senior

management. Decision making and domain knowledge may have a critical impact on overall project implementation. May supervise others.

NETWORK ENGINEER I

Functional Responsibility: Manages an engineering group responsible for telecommunications, networks, and other IT disciplines. Apply extremely complex networking concepts in the analysis, study, and design of data networks. Analyzes network characteristics (e.g., traffic, connect time, transmission speeds, packet sizes, and throughput) and recommends procurement, removals, and modifications to network components. Designs and optimizes network topologies and site configurations. Plans and supervises installations, transitions, and cutovers of network components and capabilities. Review existing network designs and capabilities with the goal of making refinements, reducing operating overhead, enhancing network throughput, and improving current network topologies. Work is performed under supervision.

NETWORK ENGINEER II

Functional Responsibility: Applies extremely complex networking concepts in the analysis, study, and design of data networks. Analyzes network characteristics (e.g., traffic, connect time, transmission speeds, packet sizes, and throughput) and recommends procurement, removals, and modifications to network components. Designs and optimizes network topologies and site configurations. Plans and supervises installations, transitions, and cutovers of network components and capabilities. Review existing network designs and capabilities with the goal of making refinements, reducing operating overhead, enhancing network throughput, and improving current network topologies. Can perform more complex tasks with minimal supervision. Work is performed under supervision.

NETWORK ENGINEER III

Functional Responsibility: Applies extremely complex networking concepts in the analysis, study, and design of data networks. Analyzes network characteristics (e.g., traffic, connect time, transmission speeds, packet sizes, and throughput) and recommends procurement, removals, and modifications to network components. Designs and optimizes network topologies and site configurations. Plans and supervises installations, transitions, and cutovers of network components and capabilities. Review existing network designs and capabilities with the goal of making refinements, reducing operating overhead, enhancing network throughput, and improving current network topologies. Can perform all tasks with no supervision required. May supervise others.

NETWORK ENGINEER VI

Functional Responsibility: Manages an engineering group responsible for telecommunications, networks, and other IT disciplines. Apply extremely complex networking concepts in the analysis, study, and design of data networks. Analyzes network characteristics (e.g., traffic, connect time, transmission speeds, packet sizes, and throughput) and recommends procurement, removals, and modifications to network components. Designs and optimizes network topologies and site configurations. Plans and supervises installations, transitions, and cutovers of network components and capabilities. Review existing network designs and capabilities with the goal of making refinements, reducing operating overhead, enhancing network throughput, and improving current network topologies. Provides technical/management leadership on major tasks or technology

assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that technical requirements are met. Interactions involve client negotiations and interfacing with senior management. Decision making and domain knowledge may have a critical impact on overall project implementation. May supervise others.

NETWORK SPECIALIST I

Functional Responsibility: Provides technical guidance for directing and monitoring information systems operations. Designs, builds, and implements network systems. Directs compilation of records and reports concerning network operations and maintenance. Troubleshoots network performance issues. Analyzes network traffic and provides capacity-planning solutions. Monitors and responds to complex technical control facility hardware and software problems. Interfaces with vendor support service groups to ensure proper escalation during outages or periods of degraded system performance. Manages the purchase, testing, installation, and support of network communications, including LAN/MAN/WAN systems. Performs system-level design and configuration of products including determination of hardware, OS, and other platform specifications. Plans large-scale systems projects through vendor comparison and cost studies. Performs a variety of systems engineering tasks and activities that are broad in nature and are concerned with major systems design, integration, and implementation, including personnel, hardware, software, budgetary, and support facilities and/or equipment. Provides quality assurance review and the evaluation of new and existing software products. Provide assistance and oversight for all information systems operations activities, including computer and telecommunications/ communications operations, data entry, data control, LAN/MAN/WAN administration and operations support, operating systems programming, system security policy procedures, and/or web strategy and operations. Provides input to policy level discussions regarding standards and budget constraints. Monitors and responds to hardware, software, and network problems. Provides the routine testing and analysis of all elements of the network facilities (including power, software, communications machinery, lines, modems, and terminals). Utilizes software and hardware tools and identifies and diagnoses complex problems and factors affecting network performance. Troubleshoots network systems when necessary and makes improvements to the network Knowledge/Skill Description Applies fundamental concepts, processes, practices, and procedures on technical assignments. Performs work that requires practical experience and training. Work is performed under supervision.

NETWORK SPECIALIST II

Functional Responsibility: Provides technical guidance for directing and monitoring information systems operations. Designs, builds, and implements network systems. Directs compilation of records and reports concerning network operations and maintenance. Troubleshoots network performance issues. Analyzes network traffic and provides capacity-planning solutions. Monitors and responds to complex technical control facility hardware and software problems. Interfaces with vendor support service groups to ensure proper escalation during outages or periods of degraded system performance. Manages the purchase, testing, installation, and support of network communications, including LAN/MAN/WAN systems. Performs system-level design and configuration of products including determination of hardware, OS, and other platform specifications. Plans large-scale systems projects through vendor comparison and cost studies.

Performs a variety of systems engineering tasks and activities that are broad in nature and are concerned with major systems design, integration, and implementation, including personnel, hardware, software, budgetary, and support facilities and/or equipment. Provides quality assurance review and the evaluation of new and existing software products. Provide assistance and oversight for all information systems operations activities, including computer and telecommunications/ communications operations, data entry, data control, LAN/MAN/WAN administration and operations support, operating systems programming, system security policy procedures, and/or web strategy and operations. Provides input to policy level discussions regarding standards and budget constraints. Supervises all personnel engaged in the operation and support of network facilities, including all communications equipment on various platforms in large scale or multi-shift operations. Supervises complex operations that involve two or more additional functions such as, but not limited to, network operations, systems security, systems software support, and production support activities. Monitors and responds to hardware, software, and network problems. Provides the routine testing and analysis of all elements of the network facilities (including power, software, communications machinery, lines, modems, and terminals). Utilizes software and hardware tools and identifies and diagnoses complex problems and factors affecting network performance. Troubleshoots network systems when necessary and makes improvements to the network Possesses and applies expertise on multiple complex work assignments. Assignments may be broad in nature, requiring originality and innovation in determining how to accomplish tasks. Operates with appreciable latitude in developing methodology and presenting solutions to problems. Contributes to deliverables and performance metrics where applicable. Work is performed under supervision.

NETWORK SPECIALIST III

Functional Responsibility: Provides technical guidance for directing and monitoring information systems operations. Designs, builds, and implements network systems. Directs compilation of records and reports concerning network operations and maintenance. Troubleshoots network performance issues. Analyzes network traffic and provides capacity-planning solutions. Monitors and responds to complex technical control facility hardware and software problems. Interfaces with vendor support service groups to ensure proper escalation during outages or periods of degraded system performance. Manages the purchase, testing, installation, and support of network communications, including LAN/MAN/WAN systems. Performs system-level design and configuration of products including determination of hardware, OS, and other platform specifications. Plans large-scale systems projects through vendor comparison and cost studies. Performs a variety of systems engineering tasks and activities that are broad in nature and are concerned with major systems design, integration, and implementation, including personnel, hardware, software, budgetary, and support facilities and/or equipment. Provides quality assurance review and the evaluation of new and existing software products. Provide assistance and oversight for all information systems operations activities, including computer and telecommunications/ communications operations, data entry, data control, LAN/MAN/WAN administration and operations support, operating systems programming, system security policy procedures, and/or web strategy and operations. Provides input to policy level discussions regarding standards and budget constraints. Supervises all personnel engaged in the operation and support of network facilities, including all communications equipment on various platforms in large scale or multi-shift operations. Supervises complex operations that involve two or more additional functions such as, but not limited to, network operations, systems security, systems software support, and

production support activities. Monitors and responds to hardware, software, and network problems. Provides the routine testing and analysis of all elements of the network facilities (including power, software, communications machinery, lines, modems, and terminals). Utilizes software and hardware tools and identifies and diagnoses complex problems and factors affecting network performance. Troubleshoots network systems when necessary and makes improvements to the network. Possesses and applies expertise on multiple complex work assignments. Assignments may be broad in nature, requiring originality and innovation in determining how to accomplish tasks. Operates with appreciable latitude in developing methodology and presenting solutions to problems. Contributes to deliverables and performance metrics where applicable. May supervise others.

NETWORK SPECIALIST IV

Functional Responsibility: Provides technical guidance for directing and monitoring information systems operations. Designs, builds, and implements network systems. Directs compilation of records and reports concerning network operations and maintenance. Troubleshoots network performance issues. Analyzes network traffic and provides capacity planning solutions. Monitors and responds to complex technical control facility hardware and software problems. Interfaces with vendor support service groups to ensure proper escalation during outages or periods of degraded system performance. Manages the purchase, testing, installation, and support of network communications, including LAN/MAN/WAN systems. Performs system-level design and configuration of products including determination of hardware, OS, and other platform specifications. Plans large-scale systems projects through vendor comparison and cost studies. Performs a variety of systems engineering tasks and activities that are broad in nature and are concerned with major systems design, integration, and implementation, including personnel, hardware, software, budgetary, and support facilities and/or equipment. Provides quality assurance review and the evaluation of new and existing software products. Provide assistance and oversight for all information systems operations activities, including computer and telecommunications/ communications operations, data entry, data control, LAN/MAN/WAN administration and operations support, operating systems programming, system security policy procedures, and/or web strategy and operations. Provides input to policy level discussions regarding standards and budget constraints. Supervises all personnel engaged in the operation and support of network facilities, including all communications equipment on various platforms in large-scale or multi-shift operations. Supervises complex operations that involve two or more additional functions such as, but not limited to, network operations, systems security, systems software support, and production support activities. Monitors and responds to hardware, software, and network problems. Provides the routine testing and analysis of all elements of the network facilities (including power, software, communications machinery, lines, modems, and terminals). Utilizes software and hardware tools and identifies and diagnoses complex problems and factors affecting network performance. Troubleshoots network systems when necessary and makes improvements to the network. Provides technical/management leadership on major tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that technical requirements are met. Interactions involve client negotiations and interfacing with senior management. Decision making and domain knowledge may have a critical impact on overall project implementation. May supervise others.

PROGRAM MANAGER I

Functional Responsibility: Provides program management for multiple projects. Prepares project implementation plan, coordinates project activities, monitors project milestones, and provides progress reports. Responsible for all aspects of performance (i.e., technical, contractual, administrative, financial). Consults with the customer to ensure adherence to contractual obligations establishes and maintains technical and financial reports to show progress of projects to management and customers, organizes and assigns responsibilities to subordinates, and oversees the completion of all assigned tasks. Performs overall management of contract support operations, possibly involving multiple projects and groups of personnel at multiple locations. Organizes, directs, and coordinates the planning and production of all contract support activities. Able to manage smaller programs with minimal supervision. May supervise others.

PROGRAM MANAGER II

Functional Responsibility: Provides program management for multiple projects. Prepares project implementation plan, coordinates project activities, monitors project milestones, and provides progress reports. Responsible for all aspects of performance (i.e., technical, contractual, administrative, financial). Consults with the customer to ensure adherence to contractual obligations establishes and maintains technical and financial reports to show progress of projects to management and customers, organizes and assigns responsibilities to subordinates, and oversees the completion of all assigned tasks Performs overall management of contract support operations, possibly involving multiple projects and groups of personnel at multiple locations. Organizes, directs, and coordinates the planning and production of all contract support activities. Possesses and applies a comprehensive knowledge across key tasks and high impact assignments. Plans and leads major technology assignments. Evaluates performance results and recommends major changes affecting short-term project growth and success. Able to manage all programs with no supervision required. May supervise others.

PROGRAM MANAGER III

Functional Responsibility: Provides program management for multiple projects. Prepares project implementation plan, coordinates project activities, monitors project milestones, and provides progress reports. Responsible for all aspects of performance (i.e., technical, contractual, administrative, financial). Consults with the customer to ensure adherence to contractual obligations establishes and maintains technical and financial reports to show progress of projects to management and customers, organizes and assigns responsibilities to subordinates, and oversees the completion of all assigned tasks Performs overall management of contract support operations, possibly involving multiple projects and groups of personnel at multiple locations. Organizes, directs, and coordinates the planning and production of all contract support activities. Provides technical/management leadership on major tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that technical requirements are met. Interactions involve client negotiations and interfacing with senior management. Decision making and domain knowledge may have a critical impact on overall project implementation. May supervise others.

PROGRAM MANAGER IV

Functional Responsibility: Provides program management for multiple projects. Prepares project implementation plan, coordinates project activities, monitors project milestones, and provides progress reports. Responsible for all aspects of performance (i.e., technical, contractual, administrative, financial). Consults with the customer to ensure adherence to contractual obligations establishes and maintains technical and financial reports to show progress of projects to management and customers, organizes and assigns responsibilities to subordinates, and oversees the completion of all assigned tasks Performs overall management of contract support operations, possibly involving multiple projects and groups of personnel at multiple locations. Organizes, directs, and coordinates the planning and production of all contract support activities. Provides technical/management leadership on major tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that technical requirements are met. Interactions involve client negotiations and interfacing with senior management. Decision making and domain knowledge may have a critical impact on overall project implementation. May supervise others.

PROJECT MANAGER I

Functional Responsibility: Responsible for assisting the management of small to med- sized projects. Assists in preparing implementation plan, coordinates activities, monitors milestones, and provides progress reports. Creation and management of project information related to contractual requirements and cost for submittal to the program manager for review and approval. Must have rudimentary understanding of accounting, management, and contract principles. Performs day-to-day management of assigned delivery order projects that involve teams of data processing and other information system and management professionals who have previously been involved in analyzing, designing, integrating, testing, documenting, converting, extending, and implementing automated information and telecommunications systems. Demonstrates proven skills in those technical areas addressed by the delivery order to be managed. Organizes, directs, and coordinates the planning and production of all activities Associated with assigned delivery order projects. Demonstrates writing and oral communication skills. May defer more complex problems to more senior project managers. Work is performed under supervision.

PROJECT MANAGER II

Functional Responsibility: Responsible for assisting the management of small to medium sized projects. Assists in preparing implementation plan, coordinates activities, monitors milestones, and provides progress reports. Creation and management of project information related to contractual requirements and cost for submittal to the program manager for review and approval. Must have rudimentary understanding of accounting, management, and contract principles. Performs day-to-day management of assigned delivery order projects that involve teams of data processing and other information system and management professionals who have previously been involved in analyzing, designing, integrating, testing, documenting, converting, extending, and implementing automated information and telecommunications systems. Demonstrates proven skills in those technical areas addressed by the delivery order to be managed. Organizes, directs, and coordinates the planning and production of all activities associated with assigned delivery order projects.

Demonstrates writing and oral communication skills. Able to manage more complex projects with no supervision required. May supervise others.

PROJECT MANAGER III

Functional Responsibility: Responsible for leading the management of medium to large sized projects. Assists in preparing implementation plan, coordinates activities, monitors milestones, and provides progress reports. Creation and management of project information related to contractual requirements and cost for submittal to the program manager for review and approval. Must have rudimentary understanding of accounting, management, and contract principles. Performs day-to-day management of assigned delivery order projects that involve teams of data processing and other information system and management professionals who have previously been involved in analyzing, designing, integrating, testing, documenting, converting, extending, and implementing automated information and telecommunications systems. Demonstrates proven skills in those technical areas addressed by the delivery order to be managed. Organizes, directs, and coordinates the planning and production of all activities associated with assigned delivery order projects. Demonstrates writing and oral communication skills. Able to manage more complex projects with no supervision required. and applies a comprehensive knowledge across key tasks and high impact assignments. Plans and leads major technology assignments. Evaluates performance results and recommends major changes affecting short-term project growth and success. Functions as a technical expert across multiple project assignments. May supervise others.

PROJECT MANAGER IV

Functional Responsibility: Responsible for leading the management of medium to large sized projects. Assists in preparing implementation plan, coordinates activities, monitors milestones, and provides progress reports. Creation and management of project information related to contractual requirements and cost for submittal to the program manager for review and approval. Must have rudimentary understanding of accounting, management, and contract principles. Performs day-to-day management of assigned delivery order projects that involve teams of data processing and other information system and management professionals who have previously been involved in analyzing, designing, integrating, testing, documenting, converting, extending, and implementing automated information and telecommunications systems. Demonstrates proven skills in those technical areas addressed by the delivery order to be managed. Organizes, directs, and coordinates the planning and production of all activities associated with assigned delivery order projects. Demonstrates writing and oral communication skills. Provides technical/management leadership on major tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that technical requirements are met. Interactions involve client negotiations and interfacing with senior management. Decision making and domain knowledge may have a critical impact on overall project implementation. May supervise others.

QUALITY ASSURANCE SPECIALIST I

Functional Responsibility: Provides development of project Software Quality Assurance Plan and the implementation of procedures that conform to the requirements of the contract. Provides an independent assessment of how the project's software development process is being

implemented relative to the defined process and recommends methods to optimize the organization's process. May be responsible for all activities involving quality assurance and compliance with applicable regulatory requirements. Conducts audits and reviews/analyzes data and documentation. Develops and implements procedures and test plans for assuring quality in a system development environment which supports large databases and applications. Applies fundamental concepts, processes, practices, and procedures on technical assignments. Performs work that requires practical experience and training. Work is performed under supervision.

QUALITY ASSURANCE SPECIALIST II

Functional Responsibility: Provides development of project Software Quality Assurance Plan and the implementation of procedures that conform to the requirements of the contract. Provides an independent assessment of how the project's software development process is being implemented relative to the defined process and recommends methods to optimize the organization's process. May be responsible for all activities involving quality assurance and compliance with applicable regulatory requirements. Conducts audits and reviews/analyzes data and documentation. Develops and implements procedures and test plans for assuring quality in a system development environment which supports large databases and applications. Possesses and applies expertise on multiple complex work assignments. Assignments may be broad in nature, requiring originality and innovation in determining how to accomplish tasks. Operates with appreciable latitude in developing methodology and presenting solutions to problems. Contributes to deliverables and performance metrics where applicable. Work is performed under supervision.

QUALITY ASSURANCE SPECIALIST III

Functional Responsibility: Provides development of project Software Quality Assurance Plan and the implementation of procedures that conform to the requirements of the contract. Provides an independent assessment of how the project's software development process is being implemented relative to the defined process and recommends methods to optimize the organization's process. May be responsible for all activities involving quality assurance and compliance with applicable regulatory requirements. Conducts audits and reviews/analyzes data and documentation. Develops and implements procedures and test plans for assuring quality in a system development environment which supports large databases and applications. Possesses and applies a comprehensive knowledge across key tasks and high impact assignments. Plans and leads major technology assignments. Evaluates performance results and recommends major changes affecting short-term project growth and success. Functions as a technical expert across multiple project assignments. May supervise others.

QUALITY ASSURANCE SPECIALIST IV

Functional Responsibility: Provides development of project Software Quality Assurance Plan and the implementation of procedures that conform to the requirements of the contract. Provides an independent assessment of how the project's software development process is being implemented relative to the defined process and recommends methods to optimize the organization's process. May be responsible for all activities involving quality assurance and compliance with applicable regulatory requirements. Conducts audits and reviews/analyzes data and documentation. Develops and implements procedures and test plans for assuring quality in a system development environment which supports large databases and applications. Provides

technical/management leadership on major tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that technical requirements are met. Interactions involve client negotiations and interfacing with senior management. Decision making and domain knowledge may have a critical impact on overall project implementation. May supervise others.

SOFTWARE ENGINEER I

Functional Responsibility: Develops and customizes application servers and toolsets to enhance business processes, including workflow development, knowledge, and data management. Research, test and report capabilities of technology products, application servers and toolsets, with business analysts to map business and functional requirements. Develops and applies departmental and organization- wide business modernization and process improvements models for use in designing and customizing integrated, shared application servers and knowledge and data management systems. Analyzes and resolves application software and toolset issues. Rely on experience and judgment to plan and accomplish goals. Work is performed under supervision.

SOFTWARE ENGINEER II

Functional Responsibility: Develops and customizes application servers and toolsets to enhance business processes, including workflow development, knowledge, and data management. Research, test and report capabilities of technology products, application servers and toolsets, with business analysts to map business and functional requirements. Develops and applies departmental and organization-wide business modernization and process improvements models for use in designing and customizing integrated, shared application servers and knowledge and data management systems. Analyzes and resolves application software and toolset issues. Rely on experience and judgment to plan and accomplish goals. Can complete tasks of intermediate complexity alone and may only require supervision provided by more experienced personnel for more complex problems. Contributes to deliverables and performance metrics where applicable. Work is performed under supervision.

SOFTWARE ENGINEER III

Functional Responsibility: Develops and customizes application servers and toolsets to enhance business processes, including workflow development, knowledge, and data management. Research, test and report capabilities of technology products, application servers and toolsets, with business analysts to map business and functional requirements. Develops and applies departmental and organization-wide business modernization and process improvements models for use in designing and customizing integrated, shared application servers and knowledge and data management systems. Analyzes and resolves application software and toolset issues. Rely on experience and judgment to plan and accomplish goals. May supervise others.

SOFTWARE ENGINEER IV

Functional Responsibility: Develops and customizes application servers and toolsets to enhance business processes, including workflow development, knowledge, and data management. Research, test and report capabilities of technology products, application servers and toolsets, with business analysts to map business and functional requirements. Develops and applies departmental

and organization-wide business modernization and process improvements models for use in designing and customizing integrated, shared application servers and knowledge and data management systems. Analyzes and resolves application software and toolset issues. Provides technical/management leadership on major tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that technical requirements are met. Interactions involve client negotiations and interfacing with senior management. Decision making and domain knowledge may have a critical impact on overall project implementation. May supervise others.

SUBJECT MATTER EXPERT I

Functional Responsibility: Has advanced understanding of area of expertise related to IT disciplines and principles. Advises team members of implication of approaches during solution development. Serves as facilitator for Integrated Product Team meetings. Provides expert consultative support to a functional IT technical area of the project. Develop solutions to complex problems. Works closely with the information technologists to identify the best technological solution to technical issues. Familiar with a specific field's concepts, practices, and procedures. Rely on extensive experience and judgment to plan and accomplish goals. Work is performed under supervision.

SUBJECT MATTER EXPERT II

Functional Responsibility: Has advanced understanding of area of expertise related to IT disciplines and principles. Advises team members of implication of approaches during solution development. Serves as facilitator for Integrated Product Team meetings. Provides expert consultative support to a functional IT technical area of the project. Develop solutions to complex problems. Works closely with the information technologists to identify the best technological solution to technical issues. Familiar with a specific field's concepts, practices, and procedures. Rely on extensive experience and judgment to plan and accomplish goals. Contributes to deliverables and performance metrics where applicable. Work is performed under supervision.

SUBJECT MATTER EXPERT III

Functional Responsibility: Has advanced understanding of area of expertise related to IT disciplines and principles. Advises team members of implication of approaches during solution development. Serves as facilitator for Integrated Product Team meetings. Provides expert consultative support to a functional IT technical area of the project. Develop solutions to complex problems. Works closely with the information technologists to identify the best technological solution to technical issues. Familiar with a specific field's concepts, practices, and procedures. Rely on extensive experience and judgment to plan and accomplish goals. Contributes to deliverables and performance metrics where applicable. This position may perform limited management duties. May supervise others.

SUBJECT MATTER EXPERT IV

Functional Responsibility: Has advanced understanding of area of expertise related to IT disciplines and principles. Advises team members of implication of approaches during solution development. Serves as facilitator for Integrated Product Team meetings. Provides expert

consultative support to a functional IT technical area of the project. Develop solutions to complex problems. Works closely with the information technologists to identify the best technological solution to technical issues. Familiar with a specific field's concepts, practices, and procedures. Rely on extensive experience and judgment to plan and accomplish goals. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that technical requirements are met. Interactions involve client negotiations and interfacing with senior management. Decision making and domain knowledge may have a critical impact on overall project implementation. This position will perform managerial duties as requested with minimal support from more experienced personnel. May supervise others.

SUBJECT MATTER EXPERT V

Functional Responsibility: Has advanced understanding of area of expertise related to IT disciplines and principles. Advises team members of implication of approaches during solution development. Serves as facilitator for Integrated Product Team meetings. Provides expert consultative support to a functional IT technical area of the project. Develop solutions to complex problems. Works closely with the information technologists to identify the best technological solution to technical issues. Familiar with a specific field's concepts, practices, and procedures. Rely on extensive experience and judgment to plan and accomplish goals Responsible for developing project plans, justifications, guidelines, and controls. Provides technical/ management leadership on major tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that technical requirements are met. Interactions involve client negotiations and interfacing with senior management. Decision making and domain knowledge may have a critical impact on overall project implementation. May supervise others.

SYSTEMS ADMINISTRATOR I

Functional Responsibility: Responsible for the installing, managing, maintaining, and troubleshooting hardware and software on systems, to maintain the on-going operational performance of programs (software) and the hardware on which the programs run within the Mainframe, Mid-Range, or PC environments. Implements and supports local area network (LAN) and Wide area network (WAN) hardware and software. Analyzes customer workflow and procedures to recommend operational support tools and technologies to satisfy customer needs. Acts as a liaison between the customer, suppliers, and other technical groups to resolve network and hardware problems. Analyzes performance problems and recommends solutions to enhance functionality, reliability and/or usability. Implements operational support standards and procedures relating to change management, performance management, and security. Recommend changes and improvements to existing standards. Provides support for the overall IT system administration activities such as user access, backup and recovery procedures, patches and upgrades, tuning, and performance. Work is performed under supervision.

SYSTEMS ADMINISTRATOR II

Functional Responsibility: Responsible for the installing, managing, maintaining, and troubleshooting hardware and software on systems, to maintain the on-going operational

performance of programs (software) and the hardware on which the programs run within the Mainframe, Mid-Range, or PC environments. Implements and supports local area network (LAN) and Wide area network (WAN) hardware and software. Analyzes customer workflow and procedures to recommend operational support tools and technologies to satisfy customer needs. Acts as a liaison between the customer, suppliers, and other technical groups to resolve network and hardware problems. Analyzes performance problems and recommends solutions to enhance functionality, reliability and/or usability. Implements operational support standards and procedures relating to change management, performance management, and security. Recommend changes and improvements to existing standards. Provides support for the overall IT system administration activities such as user access, backup and recovery procedures, patches and upgrades, tuning, and performance. Can perform more complex tasks with minimal supervision. Contributes to deliverables and performance metrics where applicable. Work is performed under supervision.

SYSTEMS ADMINISTRATOR III

Functional Responsibility: Responsible for the installing, managing, maintaining, and troubleshooting hardware and software on systems, to maintain the on-going operational performance of programs (software) and the hardware on which the programs run within the Mainframe, Mid-Range, or PC environments. Implements and supports local area network (LAN) and Wide area network (WAN) hardware and software. Analyzes customer workflow and procedures to recommend operational support tools and technologies to satisfy customer needs. Acts as a liaison between the customer, suppliers, and other technical groups to resolve network and hardware problems. Analyzes performance problems and recommends solutions to enhance functionality, reliability and/or usability. Implements operational support standards and procedures relating to change management, performance management, and security. Recommend changes and improvements to existing standards. Provides support for the overall IT system administration activities such as user access, backup and recovery procedures, patches and upgrades, tuning, and performance. Possesses and applies a comprehensive knowledge across key tasks and high impact assignments. Plans and leads major technology assignments. Evaluates performance results and recommends major changes affecting short-term project growth and success. Functions as a technical expert across multiple project assignments. May supervise others.

SYSTEMS ADMINISTRATOR IV

Functional Responsibility: Responsible for the installing, managing, maintaining, and troubleshooting hardware and software on systems, to maintain the on-going operational performance of programs (software) and the hardware on which the programs run within the Mainframe, Mid-Range, or PC environments. Implements and supports local area network (LAN) and Wide area network (WAN) hardware and software. Analyzes customer workflow and procedures to recommend operational support tools and technologies to satisfy customer needs. Acts as a liaison between the customer, suppliers, and other technical groups to resolve network and hardware problems. Analyzes performance problems and recommends solutions to enhance functionality, reliability and/or usability. Implements operational support standards and procedures relating to change management, performance management, and security. Recommend changes and improvements to existing standards. Provides support for the overall IT system administration activities such as user access, backup and recovery procedures, patches and upgrades, tuning, and performance. Provides technical/management leadership on major tasks or

technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that technical requirements are met. Interactions involve client negotiations and interfacing with senior management. Decision making and domain knowledge may have a critical impact on overall project implementation. This position will perform managerial duties as requested with minimal support from more experienced personnel. May supervise others.

SYSTEMS ENGINEER I

Functional Responsibility: Provides analysis related to the design, development, and integration of hardware, software, machine interfaces, and all system level requirements to provide an integrated IT solution. Develops integrated system test requirements, strategies, devices, and systems. Directs overall system level testing. Work is performed under supervision.

SYSTEMS ENGINEER II

Functional Responsibility: Provides analysis related to the design, development, and integration of hardware, software, machine interfaces, and all system level requirements to provide an integrated IT solution. Develops integrated system test requirements, strategies, devices, and systems. Directs overall system level testing. Can perform more complex tasks with minimal supervision. Contributes to deliverables and performance metrics where applicable. Work is performed under supervision.

SYSTEMS ENGINEER III

Functional Responsibility: Provides analysis related to the design, development, and integration of hardware, software, machine interfaces, and all system level requirements to provide an integrated IT solution. Develops integrated system test requirements, strategies, devices, and systems. Possesses and applies a comprehensive knowledge across key tasks and high impact assignments. Plans and leads major technology assignments. Evaluates performance results and recommends major changes affecting short-term project growth and success. Directs overall system level testing. Can perform more complex tasks with minimal supervision. Contributes to deliverables and performance metrics where applicable. May supervise others.

SYSTEMS ENGINEER IV

Functional Responsibility: Provides analysis related to the design, development, and integration of hardware, software, machine interfaces, and all system level requirements to provide an integrated IT solution. Develops integrated system test requirements, strategies, devices, and systems. Directs overall system level testing. Provides technical/management leadership on major tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that technical requirements are met. Interactions involve client negotiations and interfacing with senior management. Decision making and domain knowledge may have a critical impact on overall project implementation. This position will perform managerial duties as requested with minimal support from more experienced personnel. May supervise others.

TECHNICAL WRITER I

Functional Responsibility: Writes a variety of technical articles, reports, brochures, and/or manuals for documentation for a wide range of uses. Coordinates the display of graphics and the production of the document. Ensures content is of high quality and conforms with standards. Work is performed under supervision.

TECHNICAL WRITER II

Functional Responsibility: Writes a variety of technical articles, reports, brochures, and/or manuals for documentation for a wide range of uses. Coordinates the display of graphics and the production of the document. Ensures content is of high quality and conforms with standards. Can perform more complex tasks with minimal supervision. Contributes to deliverables and performance metrics where applicable. Work is performed under supervision.

TECHNICAL WRITER III

Functional Responsibility: Writes a variety of technical articles, reports, brochures, and/or manuals for documentation for a wide range of uses. Coordinates the display of graphics and the production of the document. Ensures content is of high quality and conforms with standards. Possesses and applies a comprehensive knowledge across key tasks and high impact assignments. Plans and leads major technology assignments. Evaluates performance results and recommends major changes affecting short-term project growth and success. Functions as a technical expert across multiple project assignments. May supervise others.

TECHNICAL WRITER IV

Functional Responsibility: Writes a variety of technical articles, reports, brochures, and/or manuals for documentation for a wide range of uses. Coordinates the display of graphics and the production of the document. Ensures content is of high quality and conforms with standards. Provides technical/management leadership on major tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that technical requirements are met. Interactions involve client negotiations and interfacing with senior management. Decision making and domain knowledge may have a critical impact on overall project implementation. This position will perform managerial duties as requested with minimal support from more experienced personnel. May supervise others.

TECHNOLOGY ENGINEER I

Functional Responsibility: Performs computer engineering and software development. Analyzes business processes, functions, and procedures to develop the best software. Establishes systems specifications and objectives. Participates in systems development and design, including software programming and user interface design. Formulates test plans, coordinates, and performs software testing. Has application knowledge of commonly used concepts, practices and procedures with the information technology fields. Analyzes engineering problems and develops solutions. Makes recommendation after performing system analysis. Work is performed under supervision.

TECHNOLOGY ENGINEER II

Functional Responsibility: Performs computer engineering and software development. Leads engineers in the activities of solving computer problems and enabling computer technology to meet the needs of the organization. Assigns, coordinates, and reviews work of engineering personnel. Responsible for applying concepts or modernization, innovation, consolidation, and cost reduction to assigned tasks. A certain degree of creativity and latitude is expected. Contributes to deliverables and performance metrics where applicable. Work is performed under supervision.

TECHNOLOGY ENGINEER III

Functional Responsibility: Performs computer engineering and software development. Applies full understanding of computer engineering discipline and industry best practices plus innovation to effectively design, implement, and support software products. Gives technical guidance to other engineers in the team. Analyzes engineering problems and develops innovative solutions. Leads engineers in performing system trade studies to maximize investments in equipment, personnel, and business processes. Evaluates performance results and recommends major changes affecting short-term project growth and success. Functions as a technical expert across multiple project assignments. May supervise others.

TECHNOLOGY ENGINEER IV

Functional Responsibility: Performs computer engineering and software development. Applies full understanding of computer engineering discipline and industry best practices plus innovation to effectively design, implement, and support software products. Gives technical guidance to other engineers in the team. Analyzes engineering problems and develops innovative solutions. Leads engineers in performing system trade studies to maximize investments in equipment, personnel, and business processes. Evaluates performance results and recommends major changes affecting short-term project growth and success. Functions as a technical expert across multiple project assignments. Provides technical/management leadership on major tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that technical requirements are met. Interactions involve client negotiations and interfacing with senior management. Decision making and domain knowledge may have a critical impact on overall project implementation. This position will perform managerial duties as requested with minimal support from more experienced personnel. May supervise others.

TEST ENGINEER I

Functional Responsibility: Evaluates, recommends, and implements automated test tools and strategies. Designs, implements, and conducts test and evaluation procedures to ensure system requirements are met. Develops, maintains, and upgrades automated test scripts and architectures for application products. Also writes, implements, and reports status for system test cases for testing. Analyzes test cases and provides regular progress reports. Serves as subject matter specialist providing testing knowledge/experience for the support of user requirements of complex to highly complex software/hardware applications. Directs and/or participates in all phases of risk management assessments and software/hardware development with emphasis on analysis of user requirements, test design and test tools selection. Applies fundamental concepts, processes,

practices, and procedures on technical assignments. Performs work that requires practical experience and training. Work is performed under supervision.

TEST ENGINEER II

Functional Responsibility: Evaluates, recommends, and implements automated test tools and strategies. Designs, implements, and conducts test and evaluation procedures to ensure system requirements are met. Develops, maintains, and upgrades automated test scripts and architectures for application products. Also writes, implements, and reports status for system test cases for testing. Analyzes test cases and provides regular progress reports. Serves as subject matter specialist providing testing knowledge/experience for the support of user requirements of complex to highly complex software/hardware applications. Directs and/or participate in all phases of risk management assessments and software/hardware development with emphasis on analysis of user requirements, test design and test tools selection. Possesses and applies expertise on multiple complex work assignments. Assignments may be broad in nature, requiring originality and innovation in determining how to accomplish tasks. Operates with appreciable latitude in developing methodology and presenting solutions to problems. Contributes to deliverables and performance metrics where applicable. Work is performed under supervision.

TEST ENGINEER III

Functional Responsibility: Evaluates, recommends, and implements automated test tools and strategies. Designs, implements, and conducts test and evaluation procedures to ensure system requirements are met. Develops, maintains, and upgrades automated test scripts and architectures for application products. Also writes, implements, and reports status for system test cases for testing. Analyzes test cases and provides regular progress reports. Serves as subject matter specialist providing testing knowledge/experience for the support of user requirements of complex to highly complex software/hardware applications. Directs and/or participate in all phases of risk management assessments and software/hardware development with emphasis on analysis of user requirements, test design and test tools selection. Possesses and applies a comprehensive knowledge across key tasks and high impact assignments. Plans and leads major technology assignments. Evaluates performance results and recommends major changes affecting short-term project growth and success. Functions as a technical expert across multiple project assignments. May supervise others.

TEST ENGINEER IV

Functional Responsibility: Evaluates, recommends, and implements automated test tools and strategies. Designs, implements, and conducts test and evaluation procedures to ensure system requirements are met. Develops, maintains, and upgrades automated test scripts and architectures for application products. Also writes, implements, and reports status for system test cases for testing. Analyzes test cases and provides regular progress reports. Serves as subject matter specialist providing testing knowledge/experience for the support of user requirements of complex to highly complex software/hardware applications. Directs and/or participate in all phases of risk management assessments and software/hardware development with emphasis on analysis of user requirements, test design and test tools selection. Possesses and applies a comprehensive knowledge across key tasks and high impact assignments. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that

technical requirements are met. Interactions involve client negotiations and interfacing with senior management. Decision making and domain knowledge may have a critical impact on overall project implementation. May supervise others.

VOICE/DATA COMMUNICATIONS ENGINEER I

Functional Responsibility: Provides technical direction and engineering knowledge for communications activities including planning, designing, developing, testing, installing, and maintaining large communications networks. Ensures that adequate and appropriate planning is provided to direct building architects and planners in building communications spaces and media pathways meet industry standards. Develops, operates, and maintains voice, wireless, video, and data communications systems. Provides complex engineering or analytical tasks and activities associated with one or more technical areas within the communications function. Applies fundamental concepts, processes, practices, and procedures on technical assignments. Performs work that requires practical experience and training. Work is performed under supervision.

VOICE/DATA COMMUNICATIONS ENGINEER II

Functional Responsibility: Provides technical direction and engineering knowledge for communications activities including planning, designing, developing, testing, installing, and maintaining large communications networks. Ensures that adequate and appropriate planning is provided to direct building architects and planners in building communications spaces and media pathways meet industry standards. Develops, operates, and maintains voice, wireless, video, and data communications systems. Provides complex engineering or analytical tasks and activities associated with one or more technical areas within the communications function. Possesses and applies expertise on multiple complex work assignments. Assignments may be broad in nature, requiring originality and innovation in determining how to accomplish tasks. Operates with appreciable latitude in developing methodology and presenting solutions to problems. Contributes to deliverables and performance metrics where applicable. Work is performed under supervision.

VOICE/DATA COMMUNICATIONS ENGINEER III

Functional Responsibility: Provides technical direction and engineering knowledge for communications activities including planning, designing, developing, testing, installing, and maintaining large communications networks. Ensures that adequate and appropriate planning is provided to direct building architects and planners in building communications spaces and media pathways meet industry standards. Develops, operates, and maintains voice, wireless, video, and data communications systems. Provides complex engineering or analytical tasks and activities associated with one or more technical areas within the communications function. Possesses and applies a comprehensive knowledge across key tasks and high impact assignments. Plans and leads major technology assignments. Evaluates performance results and recommends major changes affecting short-term project growth and success. Functions as a technical expert across multiple project assignments. May supervise others.

VOICE/DATA COMMUNICATIONS ENGINEER IV

Functional Responsibility: Provides technical direction and engineering knowledge for communications activities including planning, designing, developing, testing, installing, and maintaining large communications networks. Ensures that adequate and appropriate planning is

provided to direct building architects and planners in building communications spaces and media pathways meet industry standards. Develops, operates, and maintains voice, wireless, video, and data communications systems. Provides complex engineering or analytical tasks and activities associated with one or more technical areas within the communications function. Provides technical/management leadership on major tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that technical requirements are met. Interactions involve client negotiations and interfacing with senior management. Decision making and domain knowledge may have a critical impact on overall project implementation. May supervise others.

SIN 541519ICAM IDENTITY, CREDENTIALING & ACCESS MANAGEMENT

ID NUMBER	LCAT DESCRIPTION	YEAR 2 *04/2025*	YEAR 3 *04/2026*	YEAR 4 *04/2027*	YEAR 5 *04/2028*
03011139	IAM Applications Developer I	$85.82	$89.25	$92.82	$96.53
03011140	IAM Applications Developer II	$110.61	$115.03	$119.63	$124.42
03011141	IAM Applications Developer III	$118.24	$122.97	$127.89	$133.01
03011142	IAM Applications Developer IV	$160.20	$166.61	$173.27	$180.20
03011143	IAM Architect I	$112.52	$117.02	$121.70	$126.57
03011144	IAM Architect II	$137.31	$142.80	$148.51	$154.45
03011145	IAM Architect III	$161.15	$167.60	$174.30	$181.27
03011146	IAM Architect IV	$197.38	$205.28	$213.49	$222.03
03011147	IAM Data Architect I	$94.40	$98.18	$102.11	$106.19
03011148	IAM Data Architect II	$134.45	$139.83	$145.42	$151.24
03011149	IAM Data Architect III	$144.94	$150.74	$156.77	$163.04
03011150	IAM Data Architect IV	$180.22	$187.43	$194.93	$202.73
03011151	IAM Database Specialist I	$95.36	$99.17	$103.14	$107.27
03011152	IAM Database Specialist II	$127.78	$132.89	$138.21	$143.74
03011153	IAM Database Specialist III	$158.29	$164.62	$171.20	$178.05
03011154	IAM Database Specialist IV	$171.64	$178.51	$185.65	$193.08
03011155	IAM Help Desk Specialist I	$61.98	$64.46	$67.04	$69.72
03011156	IAM Help Desk Specialist II	$75.34	$78.35	$81.48	$84.74
03011157	IAM Help Desk Specialist III	$96.31	$100.16	$104.17	$108.34
03011158	IAM Help Desk Specialist IV	$114.43	$119.01	$123.77	$128.72
03011159	IAM Identity Specialist I	$84.87	$88.26	$91.79	$95.46
03011160	IAM Identity Specialist I	$102.03	$106.11	$110.35	$114.76
03011161	IAM Identity Specialist I	$129.68	$134.87	$140.26	$145.87
03011162	IAM Identity Specialist I	$161.15	$167.60	$174.30	$181.27
03011163	IAM Information Assurance/Security Specialist I	$105.84	$110.07	$114.47	$119.05

ID NUMBER	LCAT DESCRIPTION	YEAR 2 *04/2025*	YEAR 3 *04/2026*	YEAR 4 *04/2027*	YEAR 5 *04/2028*
03011164	IAM Information Assurance/Security Specialist II	$123.01	$127.93	$133.05	$138.37
03011165	IAM Information Assurance/Security Specialist III	$140.17	$145.78	$151.61	$157.67
03011166	IAM Information Assurance/Security Specialist IV	$162.11	$168.59	$175.33	$182.34
03011167	IAM Network Engineer I	$114.43	$119.01	$123.77	$128.72
03011168	IAM Network Engineer II	$128.73	$133.88	$139.24	$144.81
03011169	IAM Network Engineer III	$171.64	$178.51	$185.65	$193.08
03011170	IAM Network Engineer IV	$197.38	$205.28	$213.49	$222.03
03011171	IAM Network Specialist I	$87.73	$91.24	$94.89	$98.69
03011172	IAM Network Specialist II	$119.19	$123.96	$128.92	$134.08
03011173	IAM Network Specialist III	$136.36	$141.81	$147.48	$153.38
03011174	IAM Network Specialist IV	$182.13	$189.42	$197.00	$204.88
03011175	IAM Project Manager I	$109.66	$114.05	$118.61	$123.35
03011176	IAM Project Manager II	$127.78	$132.89	$138.21	$143.74
03011177	IAM Project Manager III	$149.70	$155.69	$161.92	$168.40
03011178	IAM Project Manager IV	$171.64	$178.51	$185.65	$193.08
03011179	IAM Quality Assurance Specialist I	$92.49	$96.19	$100.04	$104.04
03011180	IAM Quality Assurance Specialist II	$105.84	$110.07	$114.47	$119.05
03011181	IAM Quality Assurance Specialist III	$127.78	$132.89	$138.21	$143.74
03011182	IAM Quality Assurance Specialist IV	$175.46	$182.48	$189.78	$197.37
03011183	IAM Software Engineer I	$98.22	$102.15	$106.24	$110.49
03011184	IAM Software Engineer II	$116.33	$120.98	$125.82	$130.85
03011185	IAM Software Engineer III	$140.17	$145.78	$151.61	$157.67
03011186	IAM Software Engineer IV	$154.48	$160.66	$167.09	$173.77
03011187	IAM Subject Matter Expert I	$96.31	$100.16	$104.17	$108.34
03011188	IAM Subject Matter Expert II	$140.17	$145.78	$151.61	$157.67
03011189	IAM Subject Matter Expert III	$184.04	$191.40	$199.06	$207.02
03011190	IAM Subject Matter Expert IV	$210.73	$219.16	$227.93	$237.05

ID NUMBER	LCAT DESCRIPTION	YEAR 2 *04/2025*	YEAR 3 *04/2026*	YEAR 4 *04/2027*	YEAR 5 *04/2028*
03011191	IAM Subject Matter Expert V	$227.90	$237.02	$246.50	$256.36
03011192	IAM Systems Administrator I	$83.91	$87.27	$90.76	$94.39
03011193	IAM Systems Administrator II	$102.03	$106.11	$110.35	$114.76
03011194	IAM Systems Administrator III	$123.96	$128.92	$134.08	$139.44
03011195	IAM Systems Administrator IV	$143.03	$148.75	$154.70	$160.89
03011196	IAM Systems Engineer I	$98.22	$102.15	$106.24	$110.49
03011197	IAM Systems Engineer II	$116.33	$120.98	$125.82	$130.85
03011198	IAM Systems Engineer III	$133.50	$138.84	$144.39	$150.17
03011199	IAM Systems Engineer IV	$150.66	$156.69	$162.96	$169.48
03011200	IAM Test Engineer I	$95.36	$99.17	$103.14	$107.27
03011201	IAM Test Engineer II	$118.24	$122.97	$127.89	$133.01
03011202	IAM Test Engineer III	$140.17	$145.78	$151.61	$157.67
03011203	IAM Test Engineer IV	$162.11	$168.59	$175.33	$182.34

SIN 541519ICAM LABOR CATEGORY INFORMATION

Experience and Education

The following labor category minimum technical experience tables correspond to the prices offered in this submission.

All SIN 541519ICAM Labor Categories		
Level I	Junior	Bachelor's degree and 0 to 1 year of experience
Level II	Associate	Bachelor's degree and 2 to 4 years of experience
Level III	Senior	Bachelor's degree and 3 to 5 years of experience
Level IV	Master	Master's degree and 5 to 7 years of experience
Level V	Director	Master's degree and 7+ years of experience

Degree Substitution

This serves as a guide to the experience and educational background of personnel typically found in each labor category. However, the experience of a resource is often a valid substitute for education. With this noted, the following information indicates where experience might be substituted for a degree as accepted by the customer.

All SIN 541519ICAM Labor Categories	
Equivalent to Bachelor's (Level I)	Associates degree + 2 or more years of relevant technical experience
	High School diploma + 4 or more years relevant technical experience
Equivalent to Bachelor's (Level II)	Associates degree + 3 or more years of relevant technical experience
	High School diploma + 6 or more years relevant technical experience
Equivalent to Bachelor's (Level III)	Associates degree + 5 or more years of relevant technical experience
	High School diploma + 7 or more years relevant technical experience
Equivalent to Master's (Level IV)	Bachelor's degree + 7 years of relevant technical experience
	Associates degree + 9 or more years of relevant technical experience
	High School diploma + 11 or more years relevant technical experience
Equivalent to Master's (Level V)	Bachelor's degree + 9 or more years of relevant technical experience
	Associates degree + 11 or more years of relevant technical experience

Experience & Degree Substitution Equivalencies

*Experience exceeding the minimum shown may be substituted for education. Likewise, education exceeding the minimum shown may be substituted for experience.

LABOR CATEGORY	STANDARD QUALS		SUBSTITUTIONS				
	Min Education	Min Exp	PhD	Masters	Bachelors	Associates	High School
IAM Applications Developer I	Bachelors	0	0	0	0	2	4
IAM Applications Developer II	Bachelors	2	0	0	2	3	6
IAM Applications Developer III	Bachelors	3	0	1	3	5	7
IAM Applications Developer IV	Masters	5	3	5	7	9	11
IAM Architect I	Bachelors	0	0	0	0	2	4

LABOR CATEGORY	STANDARD QUALS		SUBSTITUTIONS				
	Min Education	Min Exp	PhD	Masters	Bachelors	Associates	High School
IAM Architect II	Bachelors	2	0	0	2	3	6
IAM Architect III	Bachelors	3	0	1	3	5	7
IAM Architect IV	Masters	5	3	5	7	9	11
IAM Data Architect I	Bachelors	0	0	0	0	2	4
IAM Data Architect II	Bachelors	2	0	0	2	3	6
IAM Data Architect III	Bachelors	3	0	1	3	5	7
IAM Data Architect IV	Masters	5	3	5	7	9	11
IAM Database Specialist I	Bachelors	0	0	0	0	2	4
IAM Database Specialist II	Bachelors	2	0	0	2	3	6
IAM Database Specialist III	Bachelors	3	0	1	3	5	7
IAM Database Specialist IV	Masters	5	3	5	7	9	11
IAM Help Desk Specialist I	Bachelors	0	0	0	0	2	4
IAM Help Desk Specialist II	Bachelors	2	0	0	2	3	6
IAM Help Desk Specialist III	Bachelors	3	0	1	3	5	7
IAM Help Desk Specialist IV	Masters	5	3	5	7	9	11
IAM Identity Specialist I	Bachelors	0	0	0	0	2	4
IAM Identity Specialist I	Bachelors	2	0	0	2	3	6
IAM Identity Specialist I	Bachelors	3	0	1	3	5	7
IAM Identity Specialist I	Masters	5	3	5	7	9	11
IAM Information Assurance/ Security Specialist I	Bachelors	0	0	0	0	2	4
IAM Information Assurance/ Security Specialist II	Bachelors	2	0	0	2	3	6
IAM Information Assurance/ Security Specialist III	Bachelors	3	0	1	3	5	7
IAM Information Assurance/ Security Specialist IV	Masters	5	3	5	7	9	11
IAM Network Engineer I	Bachelors	0	0	0	0	2	4
IAM Network Engineer II	Bachelors	2	0	0	2	3	6
IAM Network Engineer III	Bachelors	3	0	1	3	5	7
IAM Network Engineer IV	Masters	5	3	5	7	9	11
IAM Network Specialist I	Bachelors	0	0	0	0	2	4
IAM Network Specialist II	Bachelors	2	0	0	2	3	6
IAM Network Specialist III	Bachelors	3	0	1	3	5	7
IAM Network Specialist IV	Masters	5	3	5	7	9	11
IAM Project Manager I	Bachelors	0	0	0	0	2	4
IAM Project Manager II	Bachelors	2	0	0	2	3	6
IAM Project Manager III	Bachelors	3	0	1	3	5	7

LABOR CATEGORY	STANDARD QUALS		SUBSTITUTIONS				
	Min Education	Min Exp	PhD	Masters	Bachelors	Associates	High School
IAM Project Manager IV	Masters	5	3	5	7	9	11
IAM Quality Assurance Specialist I	Bachelors	0	0	0	0	2	4
IAM Quality Assurance Specialist II	Bachelors	2	0	0	2	3	6
IAM Quality Assurance Specialist III	Bachelors	3	0	1	3	5	7
IAM Quality Assurance Specialist IV	Masters	5	3	5	7	9	11
IAM Software Engineer I	Bachelors	0	0	0	0	2	4
IAM Software Engineer II	Bachelors	2	0	0	2	3	6
IAM Software Engineer III	Bachelors	3	0	1	3	5	7
IAM Software Engineer IV	Masters	5	3	5	7	9	11
IAM Subject Matter Expert I	Bachelors	0	0	0	0	2	4
IAM Subject Matter Expert II	Bachelors	2	0	0	2	3	6
IAM Subject Matter Expert III	Bachelors	3	0	1	3	5	7
IAM Subject Matter Expert IV	Masters	5	3	5	7	9	11
IAM Subject Matter Expert V	Masters	7	5	7	9	11	N/A
IAM Systems Administrator I	Bachelors	0	0	0	0	2	4
IAM Systems Administrator II	Bachelors	2	0	0	2	3	6
IAM Systems Administrator III	Bachelors	3	0	1	3	5	7
IAM Systems Administrator IV	Masters	5	3	5	7	9	11
IAM Systems Engineer I	Bachelors	0	0	0	0	2	4
IAM Systems Engineer II	Bachelors	2	0	0	2	3	6
IAM Systems Engineer III	Bachelors	3	0	1	3	5	7
IAM Systems Engineer IV	Masters	5	3	5	7	9	11
IAM Test Engineer I	Bachelors	0	0	0	0	2	4
IAM Test Engineer II	Bachelors	2	0	0	2	3	6
IAM Test Engineer III	Bachelors	3	0	1	3	5	7
IAM Test Engineer IV	Masters	5	3	5	7	9	11

Place of Performance

The labor categories provided are for both Contractor and Customer facilities.

Clearance

The labor categories provided are for a Secret and below clearance.

Labor Category Descriptions

The descriptions provided describe the functional responsibilities, education, and experience requirements for each labor category.

IAM APPLICATIONS DEVELOPER I

Functional Responsibility: Delivers IdAM/ICAM support in an entry-level capacity. Engages in identity lifecycle tasks, authentication processes, and access governance operations across enterprise systems. Drafts technical documentation and assists with compliance requirements, applying close attention to accuracy. Partners with administrators, engineers, and other specialists to promote secure integration. Handles responsibilities that may include troubleshooting, basic system configuration, and user assistance. Participates in team knowledge exchanges and contributes to growth when opportunities arise. Applies technical skills to strengthen IdAM/ICAM operations while aligning with organizational policies and federal guidance.

IAM APPLICATIONS DEVELOPER II

Functional Responsibility: Executes IdAM/ICAM support functions at an intermediate level. Supports activities related to identity lifecycle management, authentication mechanisms, and enterprise access governance. Prepares and maintains technical documentation while ensuring compliance obligations are satisfied. Works closely with engineers, administrators, and related specialists to integrate and secure systems effectively. Undertake tasks that involve problem resolution, configuration adjustments, and user-facing support. Shares expertise with peers and offers limited mentoring to less experienced colleagues. Builds on technical knowledge to refine IdAM/ICAM operations in accordance with organizational strategy and federal standards.

IAM APPLICATIONS DEVELOPER III

Functional Responsibility: Performs IdAM/ICAM responsibilities at a senior level. Leads contributions to identity lifecycle management, authentication strategies, and access governance within enterprise environments. Develop detailed technical documents and ensure compliance frameworks are applied rigorously. Collaborate with engineers, administrators, and other specialists to guarantee effective and secure integration of systems. Addresses complex troubleshooting challenges, advanced configuration needs, and escalated user support. Guides team members, mentors junior staff, and strengthens shared technical practices. Applies advanced expertise to optimize IdAM/ICAM capabilities while maintaining alignment with organizational objectives and federal requirements.

IAM APPLICATIONS DEVELOPER IV

Functional Responsibility: Oversees enterprise-level IdAM/ICAM development and integration. Directs initiatives related to identity lifecycle processes, authentication models, and governance across large, complex systems. Author and validate technical documentation, ensuring all compliance mandates are embedded within operations. Coordinates with senior engineers, system administrators, and technical leads to design secure, scalable solutions. Resolves high-level issues, architects system configurations, and supports mission-critical user access needs. Provides mentorship to less experienced developers, fostering technical and professional growth within the

team. Advances IdAM/ICAM practices to support modernization, Zero Trust principles, and federal security strategies.

IAM ARCHITECT I

Functional Responsibility: Supports enterprise architecture tasks in IdAM/ICAM environments. Assists in documenting system designs, integration points, and access management workflows. Participates in evaluating identity-related technologies and helps ensure interoperability across applications. Works alongside senior architects to align technical solutions with organizational and federal standards. Prepares diagrams, models, and reference materials to illustrate authentication and authorization processes. Gains exposure to compliance frameworks such as NIST and OMB guidance. Builds foundational expertise in enterprise-level identity system architecture.

IAM ARCHITECT II

Functional Responsibility: Designs intermediate enterprise architecture solutions for IdAM/ICAM programs. Develop system integration models and contribute to designing authentication and federation services. Coordinates with administrators and developers to align identity and access services across multiple platforms. Reviews solutions for compliance with NIST, DoD, and agency-specific standards. Refines system documentation, architecture diagrams, and technical roadmaps. Engages in solution testing and validation to ensure resilience and scalability. Guides junior staff in applying architectural practices for secure identity environments.

IAM ARCHITECT III

Functional Responsibility: Leads the creation of IdAM/ICAM enterprise architectures that support organizational missions. Defines frameworks, integration patterns, and technology standards for identity governance and authentication services. Collaborate with system engineers, project managers, and security specialists to align solutions with Zero Trust principles. Oversee compliance audits and ensure enterprise designs meet federal security requirements. Develop roadmaps for modernization and cloud-based identity management. Resolves high-complexity challenges related to scalability, data federation, and multi-enclave access. Provides mentorship to developing architects and contributes to strategic planning efforts.

IAM ARCHITECT IV

Functional Responsibility: Directs enterprise-wide IdAM/ICAM architecture strategy. Establishes vision, policies, and governance structures that guide long-term identity and access management solutions. Oversee large-scale system integration, federation, and Zero Trust adoption across mission-critical environments. Advises senior leadership on emerging technologies and their application to enterprise security goals. Coordinates multi-stakeholder alignment to ensure interoperability and compliance with NIST SP 800-207, RMF, and OMB requirements. Resolves the most complex architecture challenges while enabling seamless identity services across diverse systems. Provides coaching and direction to senior architects and technical leads, ensuring architectural practices remain secure and adaptive.

IAM DATA ARCHITECT I

Functional Responsibility: Supports entry-level IdAM/ICAM data architecture tasks. Contributes to the development of schemas and data structures that ensure secure identity management and access control. Assists in maintaining metadata repositories and identity-related data dictionaries. Works with more senior architects to validate compliance with organizational and federal standards. Participate in data quality reviews and helps document data governance procedures. Collaborates with administrators and developers to ensure proper integration of identity-related datasets. Builds foundational knowledge of data architecture to support secure and effective IdAM/ICAM services.

IAM DATA ARCHITECT II

Functional Responsibility: Designs intermediate-level IdAM/ICAM data solutions. Develop schemas, data flows, and integration points for identity and access management systems. Maintains and improves metadata and governance repositories to ensure security and compliance. Partners with system administrators, developers, and engineers to align identity-related data across applications and platforms. Performs data validation and reconciliation to strengthen reliability. Assists in refining standards and procedures to improve governance of sensitive identity data. Enhances team effectiveness by mentoring junior analysts in data management principles.

IAM DATA ARCHITECT III

Functional Responsibility: Leads complex IdAM/ICAM data architecture initiatives. Defines enterprise schemas, workflows, and integration methods that underpin identity and access management services. Validates and enforces compliance with NIST, DoD, and agency-specific standards for data security. Collaborate with engineers and administrators to architect data services that ensure scalability, resilience, and auditability. Directs advanced reconciliation and optimization of identity-related datasets. Produces technical documentation, governance standards, and operational procedures for data services. Provides guidance and mentoring to less experienced team members while contributing to strategic modernization initiatives.

IAM DATA ARCHITECT IV

Functional Responsibility: Shapes enterprise-wide IdAM/ICAM data architecture strategy. Establishes the vision, standards, and frameworks for identity-related data governance and integration. Directs the design of high-level data flows, master data repositories, and identity schema models for large-scale federal environments. Ensures solutions comply with NIST, OMB, and Zero Trust Architecture mandates. Coordinates with program managers, senior engineers, and stakeholders to align identity data governance with mission objectives. Resolves the most complex integration and reconciliation challenges while supporting mission-critical enterprise needs. Guides organizational policy for identity data management and mentors staff. Advances the enterprise toward optimized, compliant, and future-ready IdAM/ICAM data services.

IAM DATABASE SPECIALIST I

Functional Responsibility: Assists with foundational database tasks that support IdAM/ICAM operations. Performs entry-level database administration functions such as loading identity-related datasets, maintaining user access tables, and running validation queries. Follows established

procedures to ensure identity and credential data are securely stored and retrievable. Works closely with senior database specialists and system administrators to support troubleshooting. Documents processes and updates basic database management artifacts. Gains familiarity with security compliance requirements for identity data. Develops baseline skills to enable secure and reliable database support for ICAM services.

IAM DATABASE SPECIALIST II

Functional Responsibility: Manages intermediate database functions within IdAM/ICAM environments. Configures user accounts, access roles, and permissions within enterprise identity-related databases. Execute data validation, backup, and recovery activities to safeguard credentialing and authentication data. Coordinates with developers and engineers to integrate applications with identity databases. Monitors performance metrics, tunes queries, and resolves routine issues impacting IdAM/ICAM data services. Prepares and maintains documentation of database schemas and operational processes. Provides occasional guidance to junior specialists, strengthening the overall support structure for ICAM databases.

IAM DATABASE SPECIALIST III

Functional Responsibility: Directs advanced database administration for IdAM/ICAM services. Oversees database configuration, security, and performance optimization across multiple environments. Designs and enforces standards for data integrity, access control, and audit logging. Works collaboratively with system engineers and application developers to integrate complex identity services and workflows. Troubleshoots escalated incidents, implements disaster recovery plans, and ensures high availability of identity-related databases. Produces comprehensive documentation, including architecture diagrams, compliance reports, and standard operating procedures. Mentors junior staff, guiding their development in secure database practices.

IAM DATABASE SPECIALIST IV

Functional Responsibility: Leads enterprise-level database strategy and operations for IdAM/ICAM services. Defines standards for credentialing data architecture, security, and lifecycle management across large-scale environments. Architects replication, redundancy, and failover solutions to guarantee resilient access management systems. Advises senior leadership on emerging database technologies and their application to Zero Trust identity frameworks. Oversees compliance with federal cybersecurity policies, including NIST and OMB guidance. Resolves highly complex database performance and integration challenges, ensuring mission continuity. Provides mentorship and direction to mid- and senior-level specialists while establishing policies for identity data management across the enterprise.

IAM HELP DESK SPECIALIST I

Functional Responsibility: Handles entry-level support requests related to IdAM/ICAM systems. Responds to password resets, account provisioning, and access troubleshooting. Follows established scripts and workflows to resolve basic identity service issues. Escalates complex problems to higher-tier staff while documenting actions taken. Monitors help desk ticket queues and provide timely updates to users. Learns to apply federal security and privacy practices in user support. Develops baseline knowledge of authentication, credentialing, and access governance.

IAM HELP DESK SPECIALIST II

Functional Responsibility: Addresses intermediate user support needs within IdAM/ICAM environments. Assists with account lifecycle management, multifactor authentication, and access control issues. Uses diagnostic tools to troubleshoot problems and provide accurate resolutions. Collaborates with system administrators and engineers to resolve recurring issues. Maintains detailed records of incidents and recommends improvements to help desk workflows. Provides limited guidance to junior staff and promotes customer-focused support. Applies understanding of federal identity policies to strengthen service quality.

IAM HELP DESK SPECIALIST III

Functional Responsibility: Resolves advanced IdAM/ICAM incidents requiring deeper technical expertise. Investigates complex account provisioning errors, authentication failures, and integration issues. Develops and maintains troubleshooting documentation and user guides. Coordinates with engineering teams to identify root causes and implement corrective actions. Conducts training sessions for junior help desk personnel. Reviews recurring incidents to propose systemic improvements. Ensures user support aligns with organizational security policies and compliance requirements.

IAM HELP DESK SPECIALIST IV

Functional Responsibility: Oversees IdAM/ICAM help desk operations and sets service delivery standards. Directs escalation procedures and supervises junior specialists. Leads response to critical access issues and high-priority incidents. Develop training programs, knowledge bases, and troubleshooting workflows to improve help desk effectiveness. Coordinates closely with system engineers and project managers to address systemic problems and user impact. Ensures compliance with NIST SP 800-63 and federal access management guidance during user support operations. Mentors team members and fosters a culture of accountability and service excellence.

IAM IDENTITY SPECIALIST I

Functional Responsibility: Assists with entry-level identity lifecycle tasks across enterprise environments. Supports user onboarding, account provisioning, and credentialing operations under supervision. Reviews and updates identity records for accuracy while following established processes. Collaborates with administrators to ensure authentication mechanisms function properly. Documents work performed and contributes to compliance reporting. Gains exposure to identity governance and access control frameworks used in federal programs. Builds foundational skills in IdAM/ICAM operations.

IAM IDENTITY SPECIALIST II

Functional Responsibility: Carries out intermediate identity management responsibilities. Administers user accounts, roles, and entitlements to align with organizational policies. Configures authentication workflows, multifactor solutions, and federated login services. Monitors access control systems to detect irregularities and resolve routine issues. Works with engineers and developers to integrate applications into identity governance platforms. Provides guidance to junior staff in performing standard identity operations. Ensures documentation and audit logs meet

compliance standards. Strengthens enterprise access security through proactive account management.

IAM IDENTITY SPECIALIST III

Functional Responsibility: Leads advanced identity management tasks supporting large-scale environments. Designs and implements role-based and attribute-based access controls. Oversees provisioning, de-provisioning, and federation of accounts across multiple enclaves. Coordinates with system engineers and security analysts to enhance authentication mechanisms and Zero Trust access models. Troubleshoots escalated identity issues, addressing integration and performance challenges. Produces detailed technical documentation, including compliance evidence and workflow diagrams. Mentors less experienced specialists and contributes to workforce development. Aligns identity management services with federal cybersecurity directives.

IAM IDENTITY SPECIALIST IV

Functional Responsibility: Directs enterprise-level identity governance strategies. Establishes policies for credentialing, authentication, and access management across mission-critical systems. Leads integration of advanced identity technologies, including federation platforms, PKI, and Zero Trust frameworks. Advises senior leadership on identity risks, compliance requirements, and modernization strategies. Overseas the resolution of the most complex identity issues, ensuring resilience and scalability of services. Develops and enforces enterprise standards for auditing, reporting, and data protection. Coaches junior and mid-level specialists to strengthen organizational expertise. Shapes enterprise-wide IdAM/ICAM operations to support secure and compliant mission delivery.

IAM INFORMATION ASSURANCE/SECURITY SPECIALIST I

Functional Responsibility: Supports entry-level security tasks within IdAM/ICAM environments. Assists with monitoring authentication systems, reviewing audit logs, and documenting incidents. Applies baseline security controls to protect credentialing and access data. Works under supervision to validate compliance with organizational standards. Contributes to system assessments by gathering data and preparing reports. Develops familiarity with NIST SP 800-53 controls and federal identity assurance practices. Builds foundational understanding of how security integrates with identity services.

IAM INFORMATION ASSURANCE/SECURITY SPECIALIST II

Functional Responsibility: Implements intermediate security measures to safeguard IdAM/ICAM services. Administers access control lists, reviews audit trails, and validates multifactor authentication deployments. Coordinates with administrators and engineers to remediate vulnerabilities affecting identity systems. Maintains security documentation, including standard operating procedures and compliance evidence. Provides limited mentoring to junior specialists on applying assurance practices. Monitors adherence to federal frameworks such as NIST SP 800-63 and SP 800-171. Strengthens organizational security posture through proactive identity system oversight.

IAM INFORMATION ASSURANCE/SECURITY SPECIALIST III

Functional Responsibility: Leads advanced information assurance activities across identity platforms. Conducts security risk assessments, penetration testing of authentication services, and reviews of system configurations. Ensures enforcement of Zero Trust principles and alignment with DoD and federal mandates. Coordinates with system engineers to implement corrective actions and enhance defense-in-depth strategies. Develops and validates security documentation required for ATO processes. Mentors junior staff and provides guidance on applying assurance and compliance controls. Responds to escalated incidents involving access control or identity compromise. Enhances enterprise assurance practices for mission-critical IdAM/ICAM operations.

IAM INFORMATION ASSURANCE/SECURITY SPECIALIST IV

Functional Responsibility: Oversees enterprise-wide security assurance strategies for IdAM/ICAM services. Establishes policies and governance frameworks to ensure compliance with NIST, FIPS, and OMB requirements. Direct large-scale security assessments, audits, and red team exercises focused on identity and access systems. Advises senior leadership on risks, vulnerabilities, and mitigation strategies. Resolves the most complex incidents, ensuring continuity of identity services during cyber events. Shapes organizational approaches to multifactor authentication, PKI integration, and privileged access security. Provides mentorship to senior-level specialists and engineers, ensuring consistent adoption of assurance practices. Advances enterprise security to align with Zero Trust and federal cyber priorities.

IAM NETWORK ENGINEER I

Functional Responsibility: Supports identity-aware network operations in an entry-level capacity. Assists in configuring network components that enable authentication and access control services. Follows established procedures to implement firewall rules, routing updates, and VPN settings that support secure identity integration. Helps monitor network performance and documents findings for review by senior engineers. Coordinates with administrators to troubleshoot connectivity issues affecting identity systems. Develops familiarity with identity federation traffic flows and security policies governing access networks. Builds baseline skills in network engineering for ICAM environments.

IAM NETWORK ENGINEER II

Functional Responsibility: Configures intermediate network services to support IdAM/ICAM solutions. Implements authentication-aware routing, firewall rules, and access control lists to align with organizational policies. Coordinates with identity specialists to integrate federation and multifactor authentication traffic flows. Monitors network segments for performance bottlenecks and resolves routine issues. Documents configurations, diagrams, and procedures that support compliance audits. Provides occasional guidance to junior engineers and technicians. Strengthens the reliability and security of network services that underpin identity and access management.

IAM NETWORK ENGINEER III

Functional Responsibility: Leads advanced networking initiatives that enable secure identity services. Designs segmented architectures that enforce Zero Trust access models. Optimizes

routing and traffic flow for federated authentication, SSO, and credential validation services. Conducts in-depth troubleshooting of complex connectivity and performance issues. Collaborates with system architects and cybersecurity specialists to integrate IdAM/ICAM with enterprise networks. Produces detailed documentation, standards, and policies governing secure traffic management. Mentors less experienced engineers, building organizational depth in network security engineering. Ensures enterprise networking aligns with federal identity and cybersecurity requirements.

IAM NETWORK ENGINEER IV

Functional Responsibility: Directs enterprise-level network engineering strategies for IdAM/ICAM operations. Establishes standards for secure traffic flows supporting authentication, authorization, and federation across multiple enclaves. Oversees network segmentation, redundancy, and disaster recovery design to ensure mission continuity of identity services. Advises leadership on emerging networking technologies and their impact on Zero Trust adoption. Resolves the most complex integration and performance challenges for global identity traffic. Coordinates with cross-functional teams to enforce compliance with NIST and DoD guidance. Provides coaching and oversight to senior engineers, ensuring consistency in secure networking practices. Shapes enterprise network architectures to advance resilient, scalable IdAM/ICAM operations.

IAM NETWORK SPECIALIST I

Functional Responsibility: Assists with daily operational tasks that support identity-enabled networks. Monitors basic connectivity for authentication services, VPN access, and directory synchronization. Follows guidance from senior staff to perform routine checks on switches, routers, and firewalls linked to IdAM/ICAM functions. Documents configurations and incident tickets to ensure traceability. Escalates complex issues to higher-level engineers. Gains exposure to secure network management practices in support of identity services. Builds an introductory understanding of how network components underpin authentication and access control.

IAM NETWORK SPECIALIST II

Functional Responsibility: Executes intermediate network support functions within IdAM/ICAM environments. Configure standard firewall rules, port settings, and VPN parameters that support credentialing and federation traffic. Troubleshoots user connectivity issues related to authentication and access management. Monitors logs to identify recurring incidents and coordinates resolutions with engineers. Produces updates to network documentation and diagrams for compliance purposes. Assists in implementing security controls across network devices. Provides limited mentorship to entry-level specialists and promotes operational consistency.

IAM NETWORK SPECIALIST III

Functional Responsibility: Manages advanced network operations that sustain IdAM/ICAM services. Administers identity-related traffic flows across multiple enclaves, ensuring security and efficiency. Develops procedures for routing, firewall, and load balancing in support of federated authentication and multifactor access. Coordinates closely with system engineers and cybersecurity specialists to resolve escalated connectivity issues. Documents enterprise network standards and assist with compliance audits. Mentors junior staff, teaching best practices in secure

networking for identity systems. Strengthens the resilience of identity services by optimizing network performance and security posture.

IAM NETWORK SPECIALIST IV

Functional Responsibility: Oversees enterprise-scale network support for IdAM/ICAM operations. Establishes procedures for maintaining secure authentication traffic across global or multi-enclave environments. Directs advanced troubleshooting and recovery efforts when identity services are disrupted by network faults. Advises senior leadership on risks, performance trends, and emerging technologies. Coordinates with architects and program managers to ensure network strategies aligned with Zero Trust and federal identity requirements. Develop policies and documentation governing network device management for compliance. Coaches' senior-level specialists, strengthening enterprise capacity to deliver secure and resilient identity-enabled networks.

IAM PROJECT MANAGER I

Functional Responsibility: Coordinates entry-level project activities for IdAM/ICAM initiatives. Tracks schedules, deliverables, and milestones under the supervision of senior managers. Prepares meeting notes, status updates, and project documentation. Assists in managing resources, assignments, and team coordination. Ensure tasks align with established project plans and compliance requirements. Monitors risks and escalate issues to leadership as needed. Builds foundational knowledge of federal project management standards and IdAM/ICAM governance.

IAM PROJECT MANAGER II

Functional Responsibility: Manages intermediate projects or workstreams within IdAM/ICAM programs. Develop project schedules, assign resources, and track progress against deliverables. Coordinates with technical teams, stakeholders, and customers to ensure objectives are met. Maintains project documentation, risk registers, and compliance artifacts. Oversee reporting activities and communicate project status to leadership. Guides junior staff on applying project management practices. Ensure projects remain on schedule, within scope, and compliant with organizational and federal requirements.

IAM PROJECT MANAGER III

Functional Responsibility: Leads complex IdAM/ICAM projects that span multiple teams or systems. Defines project scope, objectives, and timelines in collaboration with stakeholders. Oversees planning, resource allocation, and execution of large-scale identity initiatives. Tracks budgets, risks, and dependencies, applying corrective actions to maintain alignment with mission priorities. Produce detailed project reports and ensure deliverables meet compliance and performance standards. Mentors junior project managers and provides oversight of their work. Aligns project outcomes with organizational strategies and federal identity modernization goals.

IAM PROJECT MANAGER IV

Functional Responsibility: Directs enterprise-level IdAM/ICAM programs that involve multiple projects and stakeholders. Establishes governance frameworks and ensures program activities align with strategic objectives. Manages senior project teams, providing oversight, guidance, and

accountability. Advises leadership on project risks, resource needs, and emerging priorities. Develops long-term schedules, milestone plans, and reporting structures for mission-critical identity initiatives. Ensures program outcomes comply with NIST, OMB, and federal cybersecurity mandates. Coaches and mentors senior project managers, strengthening organizational project management capability. Shapes enterprise IdAM/ICAM program execution to support secure, resilient mission outcomes.

IAM QUALITY ASSURANCE SPECIALIST I

Functional Responsibility: Assists with basic quality checks on IdAM/ICAM systems and applications. Reviews test scripts, validates account provisioning steps, and verifies authentication workflows. Follow established procedures to confirm that access management functions operate as intended. Documents test results and submits findings to senior staff. Identifies simple discrepancies and escalates issues for resolution. Gains familiarity with compliance-driven testing requirements, such as NIST-based assurance practices. Builds foundational skills in quality control for identity systems.

IAM QUALITY ASSURANCE SPECIALIST II

Functional Responsibility: Executes intermediate quality assurance tasks for IdAM/ICAM solutions. Designs and conduct functional tests of identity provisioning, authentication, and access control features. Develops test documentation and maintains records for audit purposes. Collaborate with developers and system administrators to identify and correct issues. Tracks defect resolution and ensure changes meet acceptance criteria. Mentors junior testers in proper QA processes and reporting practices. Apply federal assurance frameworks to validate system compliance and security controls.

IAM QUALITY ASSURANCE SPECIALIST III

Functional Responsibility: Leads advanced testing efforts across IdAM/ICAM environments. Develops comprehensive test plans covering system integration, performance, and security aspects of identity management. Coordinates testing activities with developers, engineers, and program managers. Analyzes test results to identify systemic issues and recommends corrective measures. Oversees regression testing to validate upgrades and patches. Produce detailed reports for compliance audits and risk assessments. Guides junior and mid-level testers, fostering consistency in QA practices. Ensure testing supports mission assurance and aligns with federal standards.

IAM QUALITY ASSURANCE SPECIALIST IV

Functional Responsibility: Directs enterprise-level quality assurance strategies for IdAM/ICAM services. Establishes policies, frameworks, and metrics for testing identity-related systems. Oversees QA teams conducting integration, performance, and security testing across large-scale deployments. Ensure testing practices align with NIST, OMB, and Zero Trust requirements. Advises senior leadership on risks and quality trends affecting mission-critical identity operations. Coordinates enterprise audits and system acceptance activities. Mentors senior QA staff and enforces consistency across test practices. Shapes organizational quality standards to enhance reliability and compliance in IdAM/ICAM programs.

IAM SOFTWARE ENGINEER I

Functional Responsibility: Develops entry-level software components supporting IdAM/ICAM systems. Writes code for authentication modules, access control features, and identity service integrations under close supervision. Assists with debugging and unit testing to ensure secure functionality. Documents work performed and supports compliance-driven software practices. Collaborate with senior engineers to gain familiarity with identity governance workflows. Learns to apply secure coding standards in alignment with federal cybersecurity guidance. Builds foundational experience in software engineering within ICAM environments.

IAM SOFTWARE ENGINEER II

Functional Responsibility: Implements intermediate software solutions for IdAM/ICAM services. Designs and develop authentication workflows, federation connectors, and role-based access management features. Conducts code reviews, system testing, and defect resolution to improve reliability. Works with administrators and analysts to ensure proper data exchange between applications and identity platforms. Prepares technical documentation to support audits and compliance requirements. Provides guidance to junior developers on secure coding techniques. Strengthens enterprise identity services through reliable and compliant software development.

IAM SOFTWARE ENGINEER III

Functional Responsibility: Leads advanced software engineering tasks for IdAM/ICAM environments. Architects and implements complex identity features such as multifactor authentication integrations, attribute-based access controls, and large-scale federation services. Oversees testing and validation of software components to ensure scalability and security. Coordinates with architects, security specialists, and administrators to align solutions with enterprise identity frameworks. Troubleshoot high priority defects and ensure system resilience through continuous improvement. Produces technical documentation, test reports, and compliance evidence. Mentors junior and mid-level developers, strengthening team expertise.

IAM SOFTWARE ENGINEER IV

Functional Responsibility: Directs enterprise software development initiatives for IdAM/ICAM systems. Defines architecture for authentication, authorization, and federation modules across mission-critical applications. Leads development teams in applying DevSecOps practices, secure coding standards, and compliance-driven development lifecycles. Advises leadership on modernization strategies, emerging technologies, and Zero Trust requirements. Resolves the most complex software challenges, ensuring resilience and mission readiness of identity services. Produces enterprise-wide coding standards and technical documentation to support audits and accreditation. Coaches senior engineers and developers, ensuring software practices advance organizational and federal objectives.

IAM SUBJECT MATTER EXPERT I

Functional Responsibility: Contributes specialized knowledge in support of IdAM/ICAM initiatives. Applies entry-level subject matter expertise to assist in implementing identity governance, authentication, and access management practices. Participates in requirements analysis and offers input on technical solutions. Supports testing, documentation, and compliance

activities under supervision. Collaborates with senior experts to gain exposure to enterprise-level identity challenges. Build familiarity with NIST frameworks and federal security directives. Develops baseline proficiency as an IdAM/ICAM subject matter contributor.

IAM SUBJECT MATTER EXPERT II

Functional Responsibility: Applies intermediate expertise to IdAM/ICAM solutions. Advises teams on identity lifecycle management, multifactor authentication, and federation practices. Assists with developing standards, policies, and technical procedures. Provides input on integration design, risk management, and compliance validation. Prepares documentation to support audits and system accreditation. Mentors junior specialists on applying identity management best practices. Enhances organizational capability by applying subject matter knowledge to technical and operational challenges.

IAM SUBJECT MATTER EXPERT III

Functional Responsibility: Leads advanced IdAM/ICAM subject matter activities. Provides authoritative guidance on identity governance, Zero Trust adoption, and large-scale access control strategies. Supports enterprise architecture design and advises system engineers on secure integration methods. Conducts assessments of identity platforms to ensure compliance with federal requirements. Prepares detailed technical documents and compliance evidence for ATO processes. Mentors junior and mid-level experts, strengthening team-wide expertise. Shapes organizational identity strategies to address complex mission and cybersecurity objectives.

IAM SUBJECT MATTER EXPERT IV

Functional Responsibility: Directs subject matter expertise for enterprise IdAM/ICAM programs. Advises senior leadership on identity governance frameworks, modernization strategies, and risk management. Provides expert input into solution architecture, security control implementation, and compliance audits. Oversee technical assessments, penetration testing of identity systems, and strategic integration efforts. Develop policies and frameworks to guide enterprise adoption of secure identity solutions. Mentors senior specialists and contributes to organizational knowledge growth. Ensures enterprise practices align with NIST, OMB, and federal Zero Trust mandates.

IAM SUBJECT MATTER EXPERT V

Functional Responsibility: Shapes enterprise-wide IdAM/ICAM strategy as the highest-level subject matter authority. Defines vision and long-term goals for identity governance, federation, and access management across mission-critical systems. Advises executive leadership on risks, compliance, and emerging technologies. Oversee development and integration of large-scale identity services in alignment with Zero Trust principles. Resolves the most complex identity and access management challenges, ensuring resilience and scalability. Develop enterprise policies, road maps, and compliance frameworks that guide future operations. Coaches senior leaders and expert staff, elevating organizational capability to meet evolving federal cybersecurity requirements.

IAM SYSTEMS ADMINISTRATOR I

Functional Responsibility: Assists in supporting IdAM/ICAM system environments at the entry level. Monitors account provisioning, authentication services, and directory synchronization under close supervision. Performs basic system maintenance tasks such as applying patches and updates. Documents standard operating procedures and records changes for compliance purposes. Escalates complex issues to higher-level administrators. Learns to apply security policies and federal requirements within identity-related systems. Builds foundational knowledge of system administration in IdAM/ICAM contexts.

IAM SYSTEMS ADMINISTRATOR II

Functional Responsibility: Maintains IdAM/ICAM systems and services at an intermediate level. Configures user accounts, authentication services, and access control mechanisms. Monitors system logs and performance data to identify and resolve issues affecting identity services. Coordinates with developers and engineers to integrate applications into existing identity environments. Prepare documentation to support compliance audits and accreditation. Provides limited guidance to entry-level administrators. Strengthens organizational reliability by ensuring identity systems remain secure and functional.

IAM SYSTEMS ADMINISTRATOR III

Functional Responsibility: Oversees advanced administration of IdAM/ICAM platforms. Implements directory services, federation components, and multifactor authentication systems. Troubleshoot escalated issues and optimize system performance across multiple environments. Produces technical documentation and contributes to security accreditation packages. Coordinates with architects and project managers to align administration practices with enterprise strategies. Mentors junior and mid-level administrators, sharing best practices for identity system management. Enhance resilience and compliance with enterprise identity services.

IAM SYSTEMS ADMINISTRATOR IV

Functional Responsibility: Directs enterprise-level IdAM/ICAM administration efforts. Establishes standards, procedures, and policies for managing authentication and access systems. Leads configuration of large-scale directory services, PKI integrations, and Zero Trust identity solutions. Oversees patch management, system hardening, and incident response for identity platforms. Advises senior leadership on risks, compliance, and modernization strategies. Provides mentorship and direction to administrators at all levels. Ensures mission-critical identity systems operate securely, efficiently, and in full compliance with federal mandates.

IAM SYSTEMS ENGINEER I

Functional Responsibility: Supports entry-level engineering tasks within IdAM/ICAM environments. Assists in configuring system components that enable authentication, authorization, and federation services. Performs routine maintenance and applies security patches under supervision. Documents configurations and prepare basic diagrams of identity system architectures. Collaborates with administrators to troubleshoot issues affecting access services. Gains exposure to NIST-aligned engineering practices for identity systems. Builds foundational technical skills in secure systems engineering.

IAM SYSTEMS ENGINEER II

Functional Responsibility: Implements intermediate IdAM/ICAM engineering solutions. Configures directory services, multifactor authentication systems, and access control workflows. Monitors performance metrics and perform analysis to ensure reliability and scalability. Coordinates with developers to integrate applications into identity environments. Produces technical documentation, compliance artifacts, and system procedures. Provides occasional guidance to junior engineers. Enhance organizational capabilities by applying engineering expertise to strengthen identity services.

IAM SYSTEMS ENGINEER III

Functional Responsibility: Leads advanced IdAM/ICAM engineering initiatives. Designs and optimizes authentication services, federation frameworks, and enterprise access management systems. Conducts testing, validation, and troubleshooting for escalated issues. Coordinates with architects and security specialists to ensure alignment with Zero Trust and federal mandates. Produces detailed system designs, technical reports, and compliance documentation. Mentors junior engineers, transferring advanced knowledge of IdAM/ICAM engineering practices. Strengthens mission assurance through resilient and secure identity service engineering.

IAM SYSTEMS ENGINEER IV

Functional Responsibility: Directs enterprise-level IdAM/ICAM engineering efforts. Establishes engineering standards, system baselines, and governance processes for identity services. Leads the design of complex authentication frameworks, PKI integrations, and large-scale federation solutions. Oversee performance tuning, system modernization, and incident resolution for mission-critical identity platforms. Advises senior leadership on engineering risks, technology trends, and compliance requirements. Provides mentorship to engineers across all levels, ensuring knowledge transfer and consistent practices. Shapes enterprise engineering approaches to support scalable and compliant IdAM/ICAM solutions.

IAM TEST ENGINEER I

Functional Responsibility: Assists in executing entry-level testing of IdAM/ICAM systems. Follows predefined test scripts to validate account provisioning, authentication workflows, and access control mechanisms. Documents test results and prepare reports for review by senior testers. Escalates issues that require advanced troubleshooting. Collaborate with developers and administrators to confirm system functions meet basic requirements. Learn compliance-driven testing practices aligned with NIST and federal identity standards. Builds introductory skills in system testing for identity services.

IAM TEST ENGINEER II

Functional Responsibility: Conducts intermediate testing tasks for IdAM/ICAM platforms. Designs test cases for multifactor authentication, federation, and role-based access workflows. Performs integration testing to verify proper communication across applications and directories. Tracks defects, validates fixes, and maintains test documentation for compliance purposes. Coordinates with engineers and quality assurance specialists to identify and resolve issues.

Provides guidance to junior testers in executing repeatable test procedures. Enhances reliability of enterprise identity services through structured testing practices.

IAM TEST ENGINEER III

Functional Responsibility: Leads advanced testing of IdAM/ICAM systems and integrations. Develops comprehensive test plans covering scalability, resilience, and compliance requirements. Executes penetration and performance tests focused on identity services. Collaborates with system architects and security specialists to validate alignment with Zero Trust models. Produces detailed test reports for audits, risk assessments, and accreditation packages. Mentors junior and mid-level testers, promoting consistency in testing practices. Identifies systemic issues and recommends corrective actions to improve mission-critical identity services.

IAM TEST ENGINEER IV

Functional Responsibility: Directs enterprise-level IdAM/ICAM test strategies. Establishes organizational policies, frameworks, and metrics for testing authentication and access systems. Oversee test teams performing integration, regression, and performance testing across multiple environments. Advises leadership on testing outcomes, risks, and readiness of identity solutions. Ensure enterprise testing aligns with NIST, OMB, and DoD requirements. Resolve the most complex testing challenges affecting mission assurance. Provides mentorship and oversight to senior testers, ensuring quality standards are consistently applied. Shapes enterprise testing practices to support secure, resilient, and compliant IdAM/ICAM operations.