



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

VMD Systems Integrators, LLC dba VMD Corp
4114 Legato Road STE. 700
Fairfax, VA 22033
(P) 571-612-2424 | (F) 888-969-3797
<https://www.vmdcorp.com/>
Contract Administrator: Sabrina Brown-Diallo, sbrown-diallo@vmdcorp.com

Contract Number: 47QTC A24D0067
Contract Period: March 8, 2024 through March 7, 2029
Business Size: Other than Small Business

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

Pricelist current as of Modification PO-0001, effective March 08, 2024.

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>.

CUSTOMER INFORMATION:

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

SIN	SIN Description
54151HACS/54151HACSRC	Highly Adaptive Cybersecurity Services
54151S/54151SRC	Information Technology Professional Services
OLM/OLMRC	Order Level Materials

1b. Identification of the lowest priced model number and lowest unit price for that model for each special item number awarded in the contract. 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 Page 7 - 38.

2. Maximum Order: SIN 54151HACS, & 54151S - \$500,000
SIN OLM - \$250,000

3. Minimum Order: \$100.00

4. Geographic Coverage: Worldwide

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: None

8. Prompt payment terms: 1% 10 Days, 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: VMD Systems Integrators, LLC dba VMD Corp
Contracts Department
ATTN: Sabrina Brown-Diallo
4114 Legato Road STE. 700
Fairfax, VA 22033
(P) 571-612-2424 | (F) 888-969-3797 | sbrown-diallo@vmdcorp.com

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

13. Payment address (is): VMD Systems Integrators, LLC dba VMD Corp
Accounting
ATTN: Stephen Tobash
4114 Legato Road STE. 700
Fairfax, VA 22033
(P) 571-612-2452 | (F) 888-969-3797 | stobash@vmdcorp.com

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

15. Export Packing Charges: N/A

16. Terms and conditions of rental, maintenance, and repair: N/A

17. Terms and conditions of installation: N/A

18a. Terms and conditions of repair parts: N/A

18b. Terms and conditions for any other services: N/A

19. List of service and distribution points: N/A

20. List of participating dealers: N/A

21. Preventive maintenance: N/A

22a. Environmental attributes, e.g., recycled content, energy efficiency, and/or reduced pollutants: N/A

22b. If applicable, indicate that Section 508 compliance information is available for the information and communications technology (ICT) products and services and show where full details can be found (e.g. contractor's website or other location.) ICT accessibility standards can be found at:
<https://www.Section508.gov/> & <https://www.vmdcorp.com/>

23. Unique Entity Identifier (UEI) Number: ULHMANN9V8A5

24. Notification regarding registration in System for Award Management (SAM) database:
VMD Systems Integrators, LLC dba VMD Corp is registered SAM.gov.



**GSA Hourly Rates (w/IFF)
SIN 54151HACS & 54151S**

SIN	Labor Category	Year 1 03/08/2024	Year 2 03/08/2025	Year 3 03/08/2026	Year 4 03/08/2027	Year 5 03/08/2028
		- 03/07/2025	- 03/07/2026	- 03/07/2027	- 03/07/2028	- 03/07/2029
54151HACS	Chief Information Security Officer (CISO)	\$187.03	\$194.52	\$202.30	\$210.39	\$218.80
54151HACS	Cyber Security and Information Security Engineer I	\$73.19	\$76.12	\$79.16	\$82.33	\$85.62
54151HACS	Cyber Security and Information Security Engineer II	\$87.16	\$90.65	\$94.28	\$98.05	\$101.96
54151HACS	Cyber Security and Information Security Engineer III	\$104.18	\$108.35	\$112.69	\$117.19	\$121.87
54151HACS	Cyber Security and Information Security Engineer IV	\$125.27	\$130.28	\$135.49	\$140.91	\$146.54
54151HACS	Cyber Security Architect I	\$102.30	\$106.39	\$110.64	\$115.06	\$119.67
54151HACS	Cyber Security Architect II	\$115.68	\$120.30	\$125.12	\$130.13	\$135.34
54151HACS	Cyber Security Architect III	\$132.78	\$138.09	\$143.61	\$149.35	\$155.32
54151HACS	Cyber Security Architect IV	\$146.85	\$152.73	\$158.83	\$165.19	\$171.80
54151HACS	Cyber Security SME I	\$121.94	\$126.82	\$131.89	\$137.17	\$142.66
54151HACS	Cyber Security SME II	\$144.73	\$150.52	\$156.54	\$162.80	\$169.31
54151HACS	Cyber Security SME III	\$168.40	\$175.14	\$182.15	\$189.43	\$197.01
54151HACS	Cyber Security Software Developer I	\$94.53	\$98.31	\$102.24	\$106.33	\$110.58
54151HACS	Cyber Security Software Developer II	\$108.71	\$113.06	\$117.58	\$122.29	\$127.17
54151HACS	Cyber Security Software Developer III	\$132.41	\$137.71	\$143.22	\$148.96	\$154.91
54151HACS	Cyber Security Software Developer IV	\$144.82	\$150.61	\$156.63	\$162.90	\$169.42
54151HACS	Cyber Security Systems Analyst I	\$89.76	\$93.35	\$97.09	\$100.97	\$105.01
54151HACS	Cyber Security Systems Analyst II	\$110.04	\$114.44	\$119.01	\$123.77	\$128.72
54151HACS	Cyber Security Systems Analyst III	\$151.67	\$157.73	\$164.04	\$170.60	\$177.42
54151HACS	Cyber Security Systems Analyst IV	\$177.51	\$184.61	\$192.00	\$199.68	\$207.67
54151HACS	Cyber Security Test Engineer I	\$75.81	\$78.84	\$81.99	\$85.28	\$88.70
54151HACS	Cyber Security Test Engineer II	\$92.60	\$96.31	\$100.16	\$104.17	\$108.34
54151HACS	Cyber Security Test Engineer III	\$103.18	\$107.31	\$111.61	\$116.07	\$120.72
54151HACS	Cyber Security Test Engineer IV	\$112.09	\$116.57	\$121.24	\$126.09	\$131.13
54151HACS	Cyber Threat Analyst I	\$75.79	\$78.82	\$81.97	\$85.25	\$88.65
54151HACS	Cyber Threat Analyst II	\$100.98	\$105.02	\$109.22	\$113.59	\$118.14
54151HACS	Cyber Threat Analyst III	\$118.53	\$123.27	\$128.20	\$133.33	\$138.66
54151HACS	Cyber Threat Analyst IV	\$140.64	\$146.27	\$152.12	\$158.21	\$164.53

SIN	Labor Category	Year 1 03/08/2024 - 03/07/2025	Year 2 03/08/2025 - 03/07/2026	Year 3 03/08/2026 - 03/07/2027	Year 4 03/08/2027 - 03/07/2028	Year 5 03/08/2028 - 03/07/2029
54151HACS	Disaster Recovery Analyst I	\$82.98	\$86.30	\$89.75	\$93.34	\$97.08
54151HACS	Disaster Recovery Analyst II	\$95.32	\$99.13	\$103.10	\$107.22	\$111.52
54151HACS	Disaster Recovery Analyst III	\$106.15	\$110.39	\$114.80	\$119.40	\$124.17
54151HACS	Disaster Recovery Analyst IV	\$126.50	\$131.56	\$136.82	\$142.29	\$147.98
54151HACS	Information Systems Security Officer I	\$69.17	\$71.94	\$74.82	\$77.81	\$80.93
54151HACS	Information Systems Security Officer II	\$85.71	\$89.14	\$92.71	\$96.41	\$100.27
54151HACS	Information Systems Security Officer III	\$101.79	\$105.86	\$110.10	\$114.50	\$119.08
54151HACS	Information Systems Security Officer IV	\$128.98	\$134.14	\$139.51	\$145.09	\$150.89
54151HACS	Network Security Administrator I	\$76.15	\$79.19	\$82.36	\$85.65	\$89.08
54151HACS	Network Security Administrator II	\$92.99	\$96.71	\$100.57	\$104.59	\$108.78
54151HACS	Network Security Administrator III	\$104.51	\$108.70	\$113.05	\$117.57	\$122.28
54151HACS	Network Security Administrator IV	\$116.16	\$120.81	\$125.64	\$130.67	\$135.90
54151HACS	Program Manager	\$157.14	\$163.43	\$169.96	\$176.77	\$183.84
54151HACS	Project Manager I	\$92.60	\$96.31	\$100.16	\$104.17	\$108.34
54151HACS	Project Manager II	\$116.43	\$121.09	\$125.93	\$130.97	\$136.21
54151HACS	Project Manager III	\$147.40	\$153.29	\$159.43	\$165.80	\$172.43
54151HACS	Security Analyst I	\$73.70	\$76.65	\$79.72	\$82.90	\$86.22
54151HACS	Security Analyst II	\$92.14	\$95.83	\$99.66	\$103.65	\$107.79
54151HACS	Security Analyst III	\$111.06	\$115.51	\$120.13	\$124.94	\$129.93
54151HACS	Security Analyst IV	\$128.57	\$133.71	\$139.06	\$144.62	\$150.41
54151HACS	Security Awareness Training Specialist I	\$73.70	\$76.65	\$79.72	\$82.90	\$86.22
54151HACS	Security Awareness Training Specialist II	\$81.76	\$85.04	\$88.44	\$91.98	\$95.66
54151HACS	Security Awareness Training Specialist III	\$96.48	\$100.34	\$104.35	\$108.52	\$112.87
54151HACS	Security Awareness Training Specialist IV	\$116.58	\$121.25	\$126.10	\$131.14	\$136.39
54151S	Business Analyst I	\$77.65	\$80.76	\$83.99	\$87.35	\$90.84
54151S	Business Analyst III	\$104.96	\$109.16	\$113.52	\$118.07	\$122.79
54151S	Business Transformation Engineer III	\$175.90	\$182.93	\$190.25	\$197.85	\$205.76
54151S	Developer I	\$70.36	\$73.17	\$76.09	\$79.13	\$82.30
54151S	Developer II	\$106.13	\$110.37	\$114.78	\$119.38	\$124.15
54151S	Developer III	\$146.39	\$152.24	\$158.33	\$164.66	\$171.25
54151S	Engineer/Scientist VII	\$172.93	\$179.85	\$187.04	\$194.53	\$202.31
54151S	Expert / Consultant III	\$217.11	\$225.79	\$234.82	\$244.21	\$253.98
54151S	Management Analyst I	\$30.40	\$31.62	\$32.89	\$34.21	\$35.58
54151S	Management Analyst II	\$34.45	\$35.83	\$37.26	\$38.75	\$40.30
54151S	Management Analyst III	\$40.86	\$42.49	\$44.19	\$45.95	\$47.79
54151S	Management Analyst IV	\$52.98	\$55.09	\$57.30	\$59.59	\$61.97
54151S	Network Specialist	\$103.82	\$107.97	\$112.29	\$116.79	\$121.46
54151S	Network/Hardware Specialist	\$72.68	\$75.59	\$78.61	\$81.75	\$85.03

SIN	Labor Category	Year 1	Year 2	Year 3	Year 4	Year 5
		03/08/2024	03/08/2025	03/08/2026	03/08/2027	03/08/2028
		-	-	-	-	-
		03/07/2025	03/07/2026	03/07/2027	03/07/2028	03/07/2029
54151S	Principal Information Engineer	\$105.17	\$109.38	\$113.75	\$118.31	\$123.04
54151S	Program Manager I	\$115.37	\$119.98	\$124.78	\$129.76	\$134.95
54151S	Program Manager II	\$133.80	\$139.15	\$144.72	\$150.51	\$156.53
54151S	Project Manager I	\$92.27	\$95.96	\$99.80	\$103.79	\$107.94
54151S	Project Manager II	\$113.06	\$117.58	\$122.29	\$127.17	\$132.26
54151S	Subject Matter Expert	\$220.88	\$229.71	\$238.90	\$248.45	\$258.39
54151S	Systems Administrator	\$115.37	\$119.98	\$124.78	\$129.76	\$134.95
54151S	Systems Analyst I	\$80.74	\$83.97	\$87.32	\$90.82	\$94.46
54151S	Systems Analyst II	\$88.81	\$92.36	\$96.06	\$99.90	\$103.90
54151S	Systems Analyst III	\$98.80	\$102.75	\$106.86	\$111.13	\$115.58
54151S	Systems Security Specialist	\$111.87	\$116.34	\$121.00	\$125.83	\$130.87

Service Contract Labor Standards: The Service Contract Labor Standards (SCLS) are applicable to this contract as it applies to the entire Consolidated MAS Schedule and all services provided. While no specific labor categories have been identified as being subject to SCLS due to exemptions for professional employees (FAR 22.1101, 22.1102 and 29 CFR 541.300), this contract still maintains the provisions and protections for SCLS eligible labor categories. If and / or when the contractor adds SCLS labor categories / employees to the contract through the modification process, the contractor must inform the Contracting Officer and establish a SCLS matrix identifying the GSA labor category titles, the occupational code, SCLS labor category titles and the applicable WD number. Failure to do so may result in cancellation of the contract.

Labor Category Descriptions SIN 54151HACS

Chief Information Security Officer (CISO)

Functional Responsibilities: Responsible for determining enterprise information security standards. Lead the development and implementation of information security standards and procedures. Provide tactical information security advice and examining the ramifications of new technologies. Ensure that all information systems are functional and secure.

Minimum Education: Masters

Minimum Experience: 10 years

Cyber Security and Information Security Engineer I

Functional Responsibilities: Coordinate and/or perform additions and changes to network hardware and operating systems, and attached devices, including investigation, analysis, recommendation, configuration, installation, and testing of new network hardware and software. Provide direct support in the day-to-day operations on network hardware and operating systems including the evaluation of system utilization, monitoring response time and primary support for detection and correction of operational problems. Troubleshoot at the physical level of the network, working with network measurement hardware and software, as well as physical checking and testing of hardware devices at the logical level working with communication protocols. Participate in planning design, technical review and implementation for new network infrastructure hardware and network operating systems for voice and data communication networks. Maintain network infrastructure standards including network communication protocols such as TCP/IP. Provide technical consultation, training and support to IT staff as designated by the government. Diagnose and resolve complex communication problems.

Minimum Education: Bachelors

Minimum Experience: 0 years

Cyber Security and Information Security Engineer II

Functional Responsibilities: Coordinate and/or perform additions and changes to network hardware and operating systems, and attached devices, including investigation, analysis, recommendation, configuration, installation, and testing of new network hardware and software. Provide direct support in the day-to-day operations on network hardware and operating systems including the evaluation of system utilization, monitoring response time and primary support for detection and correction of operational problems. Troubleshoot at the physical level of the network, working with network measurement hardware and software, as well as physical checking and testing of hardware devices at the logical level working with communication protocols. Participate in planning design, technical review and implementation for new network infrastructure hardware and network operating systems for voice and data communication networks. Maintain network infrastructure standards including network communication protocols such as TCP/IP. Provide technical consultation, training and support to IT staff as designated by the government. Diagnose and resolve complex communication problems.

Minimum Education: Bachelors

Minimum Experience: 2 years

Cyber Security and Information Security Engineer III

Functional Responsibilities: Coordinate and/or perform additions and changes to network hardware and operating systems, and attached devices, including investigation, analysis, recommendation, configuration, installation, and testing of new network hardware and software. Provide direct support in the day-to-day operations on network hardware and operating systems including the evaluation of system utilization, monitoring response time and primary support for detection and correction of operational problems. Troubleshoot at the physical level of the network, working with network measurement hardware and software, as well as physical checking and testing of hardware devices at the logical level working with communication protocols. Participate in planning design, technical review and implementation for new network infrastructure hardware and network operating systems for voice and data communication networks. Maintain network infrastructure standards including network communication protocols such as TCP/IP. Provide technical consultation, training and support to IT staff as designated by the government. Diagnose and resolve complex communication problems.

Minimum Education: Bachelors

Minimum Experience: 5 years

Cyber Security and Information Security Engineer IV

Functional Responsibilities: Coordinate and/or perform additions and changes to network hardware and operating systems, and attached devices, including investigation, analysis, recommendation, configuration, installation, and testing of new network hardware and software. Provide direct support in the day-to-day operations on network hardware and operating systems including the evaluation of system utilization, monitoring response time and primary support for detection and correction of operational problems. Troubleshoot at the physical level of the network, working with network measurement hardware and software, as well as physical checking and testing of hardware devices at the logical level working with communication protocols. Participate in planning design, technical review and implementation for new network infrastructure hardware and network operating systems for voice and data communication networks. Maintain network infrastructure standards including network communication protocols such as TCP/IP. Provide technical consultation, training and support to IT staff as designated by the government. Diagnose and resolve complex communication problems.

Minimum Education: Masters

Minimum Experience: 8 years

Cyber Security Architect I

Functional Responsibilities: Establish system information security requirements using analysis in the development of enterprise-wide or large-scale information systems. Determine and identify high level functional and technical requirements based on interactions with the user community and knowledge of the enterprise architecture. Design security architecture to include the software, hardware, and communications to support the total requirements as well as provide for present and future cross-functional requirements and interfaces. Identify, assess, and present options for meeting the functional and technical requirements including hardware and software updates or upgrades. Be responsible for developing high level system design diagrams. Ensure these systems are compatible and in compliance with the standards for open systems architectures, the agency and OCIO architectures, and the Open Systems Interconnection (OSI) as they apply to the implementation and specification of Information

Management (IM) solution of the application platform, across the application program interface (API), and the external environment/software application. Ensure that the common operating environment is compliant; evaluate analytically and systematically problems of workflows, organization and planning and develops appropriate corrective action; Provide daily supervision and direction to staff. Create and assist in the creation of planned maturation of OCIO's technical capabilities aligned to agency and OCIO's strategic goals. Support Systems Security Architecture design and implementation of solutions' infrastructure, configuration, prototypes and production deployment and handoff. Support the enterprise management framework by complying with the Technical Reference Model (TRM). Support the agency ICAM solution project framework including planning, designing, developing, and implementing the solutions. Participate in the creation of technical demos, briefings, and oral presentations materials. Provide Technical thought leadership and SME value to client interactions. Create strategies for developing win themes and addressing business challenges and opportunities uniquely and distinctly.

Minimum Education: Bachelors

Minimum Experience: 0 years

Cyber Security Architect II

Functional Responsibilities: Establish system information security requirements using analysis in the development of enterprise-wide or large-scale information systems. Determine and identify high level functional and technical requirements based on interactions with the user community and knowledge of the enterprise architecture. Design security architecture to include the software, hardware, and communications to support the total requirements as well as provide for present and future cross-functional requirements and interfaces. Identify, assess, and present options for meeting the functional and technical requirements including hardware and software updates or upgrades. Be responsible for developing high level system design diagrams. Ensure these systems are compatible and in compliance with the standards for open systems architectures, the agency and OCIO architectures, and the Open Systems Interconnection (OSI) as they apply to the implementation and specification of Information Management (IM) solution of the application platform, across the application program interface (API), and the external environment/software application. Ensure that the common operating environment is compliant; evaluate analytically and systematically problems of workflows, organization and planning and develops appropriate corrective action; Provide daily supervision and direction to staff. Create and assist in the creation of planned maturation of OCIO's technical capabilities aligned to agency and OCIO's strategic goals. Support Systems Security Architecture design and implementation of solutions' infrastructure, configuration, prototypes and production deployment and handoff. Support the enterprise management framework by complying with the Technical Reference Model (TRM). Support the agency ICAM solution project framework including planning, designing, developing, and implementing the solutions. Participate in the creation of technical demos, briefings, and oral presentations materials. Provide Technical thought leadership and SME value to client interactions. Create strategies for developing win themes and addressing business challenges and opportunities uniquely and distinctly.

Minimum Education: Bachelors

Minimum Experience: 2 years

Cyber Security Architect III

Functional Responsibilities: Establish system information security requirements using analysis in the development of enterprise-wide or large-scale information systems. Determine and identify high level functional and technical requirements based on interactions with the user community and knowledge of the enterprise architecture. Design security architecture to include the software, hardware, and communications to support the total requirements as well as provide for present and future cross-functional requirements and interfaces. Identify, assess, and present options for meeting the functional and technical requirements including hardware and software updates or upgrades. Be responsible for developing high level system design diagrams. Ensure these systems are compatible and in compliance with the standards for open systems architectures, the agency and OCIO architectures, and the Open Systems Interconnection (OSI) as they apply to the implementation and specification of Information Management (IM) solution of the application platform, across the application program interface (API), and the external environment/software application. Ensure that the common operating environment is compliant; evaluate analytically and systematically problems of workflows, organization and planning and develops appropriate corrective action; Provide daily supervision and direction to staff. Create and assist in the creation of planned maturation of OCIO's technical capabilities aligned to agency and OCIO's strategic goals. Support Systems Security Architecture design and implementation of solutions' infrastructure, configuration, prototypes and production deployment and handoff. Support the enterprise management framework by complying with the Technical Reference Model (TRM). Support the agency ICAM solution project framework including planning, designing, developing, and implementing the solutions. Participate in the creation of technical demos, briefings, and oral presentations materials. Provide Technical thought leadership and SME value to client interactions. Create strategies for developing win themes and addressing business challenges and opportunities uniquely and distinctly.

Minimum Education: Bachelors

Minimum Experience: 5 years

Cyber Security Architect IV

Functional Responsibilities: Establish system information security requirements using analysis in the development of enterprise-wide or large-scale information systems. Determine and identify high level functional and technical requirements based on interactions with the user community and knowledge of the enterprise architecture. Design security architecture to include the software, hardware, and communications to support the total requirements as well as provide for present and future cross-functional requirements and interfaces. Identify, assess, and present options for meeting the functional and technical requirements including hardware and software updates or upgrades. Be responsible for developing high level system design diagrams. Ensure these systems are compatible and in compliance with the standards for open systems architectures, the agency and OCIO architectures, and the Open Systems Interconnection (OSI) as they apply to the implementation and specification of Information Management (IM) solution of the application platform, across the application program interface (API), and the external environment/software application. Ensure that the common operating environment is compliant; evaluate analytically and systematically problems of workflows, organization and planning and develops appropriate corrective action; Provide daily supervision and direction to staff. Create and assist in the creation of planned maturation of OCIO's technical capabilities aligned to agency and OCIO's strategic goals. Support Systems Security Architecture design and implementation of solutions'

infrastructure, configuration, prototypes and production deployment and handoff. Support the enterprise management framework by complying with the Technical Reference Model (TRM). Support the agency ICAM solution project framework including planning, designing, developing, and implementing the solutions. Participate in the creation of technical demos, briefings, and oral presentations materials. Provide Technical thought leadership and SME value to client interactions. Create strategies for developing win themes and addressing business challenges and opportunities uniquely and distinctly.

Minimum Education: Masters

Minimum Experience: 8 years

Cyber Security SME I

Functional Responsibilities: Provide technical knowledge and analysis of highly specialized applications and operational environment, high-level functional systems analysis, design, integration, documentation, and implementation advice on moderately complex problems that require an appropriate level of knowledge of the subject matter for effective implementation. Apply principles, methods, and knowledge of the functional area of capability to specific task order requirements, advanced principles and methods to exceptionally difficult and narrowly defined technical problems in engineering and other scientific applications to arrive at automated solutions. Assist other senior consultants with analysis and evaluation and with the preparation of recommendations for system improvements, optimization, development, and/or maintenance efforts in the following specialties: systems security architecture, secure networking, automation, security policy, and risk management. Commensurate experience in IT and in new and related older technology that directly relates to the required area of expertise.

Minimum Education: Bachelors

Minimum Experience: 2 years

Cyber Security SME II

Functional Responsibilities: Provide technical knowledge and analysis of highly specialized applications and operational environment, high-level functional systems analysis, design, integration, documentation, and implementation advice on moderately complex problems that require an appropriate level of knowledge of the subject matter for effective implementation. Apply principles, methods, and knowledge of the functional area of capability to specific task order requirements, advanced principles and methods to exceptionally difficult and narrowly defined technical problems in engineering and other scientific applications to arrive at automated solutions. Assist other senior consultants with analysis and evaluation and with the preparation of recommendations for system improvements, optimization, development, and/or maintenance efforts in the following specialties: systems security architecture, secure networking, automation, security policy, and risk management. Commensurate experience in IT and in new and related older technology that directly relates to the required area of expertise.

Minimum Education: Bachelors

Minimum Experience: 5 years

Cyber Security SME III

Functional Responsibilities: Provide technical knowledge and analysis of highly specialized applications and operational environment, high-level functional systems analysis, design, integration, documentation, and implementation advice on moderately complex problems that require an appropriate level of knowledge of the subject matter for effective implementation. Apply principles, methods, and knowledge of the functional area of capability to specific task order requirements, advanced principles and methods to exceptionally difficult and narrowly defined technical problems in engineering and other scientific applications to arrive at automated solutions. Assist other senior consultants with analysis and evaluation and with the preparation of recommendations for system improvements, optimization, development, and/or maintenance efforts in the following specialties: systems security architecture, secure networking, automation, security policy, and risk management. Commensurate experience in IT and in new and related older technology that directly relates to the required area of expertise.

Minimum Education: Masters

Minimum Experience: 8 years

Cyber Security Software Developer I

Functional Responsibilities: Analyze and study complex system requirements. Design software tools and subsystems to support software reuse and domain analyses and manages their implementation. Manage software development and support using formal specifications, data flow diagrams, secure coding principals, other accepted design techniques and Computer Aided Software Engineering (CASE) tools. Estimate software development costs and schedule. Review existing programs and assist in making refinements, reducing operating time, and improving current techniques. Supervise software configuration management.

Minimum Education: Bachelors

Minimum Experience: 0 years

Cyber Security Software Developer II

Functional Responsibilities: Analyze and study complex system requirements. Design software tools and subsystems to support software reuse and domain analyses and manages their implementation. Manage software development and support using formal specifications, data flow diagrams, secure coding principals, other accepted design techniques and Computer Aided Software Engineering (CASE) tools. Estimate software development costs and schedule. Review existing programs and assist in making refinements, reducing operating time, and improving current techniques. Supervise software configuration management.

Minimum Education: Bachelors

Minimum Experience: 2 years

Cyber Security Software Developer III

Functional Responsibilities: Analyze and study complex system requirements. Design software tools and subsystems to support software reuse and domain analyses and manages their implementation. Manage software development and support using formal specifications, data flow diagrams, secure coding principals, other accepted design techniques and Computer Aided Software Engineering (CASE) tools. Estimate software development costs and schedule. Review existing programs and assist in making refinements, reducing operating time, and improving current techniques. Supervise software configuration management.

Minimum Education: Bachelors

Minimum Experience: 5 years

Cyber Security Software Developer IV

Functional Responsibilities: Analyze and study complex system requirements. Design software tools and subsystems to support software reuse and domain analyses and manages their implementation. Manage software development and support using formal specifications, data flow diagrams, secure coding principals, other accepted design techniques and Computer Aided Software Engineering (CASE) tools. Estimate software development costs and schedule. Review existing programs and assist in making refinements, reducing operating time, and improving current techniques. Supervise software configuration management.

Minimum Education: Masters

Minimum Experience: 8 years

Cyber Security Systems Analyst I

Functional Responsibilities: Provide technical and administrative direction for personnel performing software development tasks, including the review of work products for correctness, adherence to the design concept and to user standards, and for progress in accordance with schedules. Coordinate with the Project and/or Program Manager to ensure problem solution and user satisfaction. Make recommendations, if needed, for approval of major systems installations. Prepare milestone status reports and deliveries/presentations on the system concept to colleagues, subordinates, and end user representatives. Provide daily supervision and direction to support staff.

Minimum Education: Bachelors

Minimum Experience: 0 years

Cyber Security Systems Analyst II

Functional Responsibilities: Provide technical and administrative direction for personnel performing software development tasks, including the review of work products for correctness, adherence to the design concept and to user standards, and for progress in accordance with schedules. Coordinate with the Project and/or Program Manager to ensure problem solution and user satisfaction. Make recommendations, if needed, for approval of major systems installations. Prepare milestone status reports and deliveries/presentations on the system concept to colleagues, subordinates, and end user representatives. Provide daily supervision and direction to support staff.

Minimum Education: Bachelors

Minimum Experience: 2 years

Cyber Security Systems Analyst III

Functional Responsibilities: Provide technical and administrative direction for personnel performing software development tasks, including the review of work products for correctness, adherence to the design concept and to user standards, and for progress in accordance with schedules. Coordinate with the Project and/or Program Manager to ensure problem solution and user satisfaction. Make recommendations, if needed, for approval of major systems installations. Prepare milestone status reports and deliveries/presentations on the system concept to colleagues, subordinates, and end user representatives. Provide daily supervision and direction to support staff.

Minimum Education: Bachelors

Minimum Experience: 5 years

Cyber Security Systems Analyst IV

Functional Responsibilities: Provide technical and administrative direction for personnel performing software development tasks, including the review of work products for correctness, adherence to the design concept and to user standards, and for progress in accordance with schedules. Coordinate with the Project and/or Program Manager to ensure problem solution and user satisfaction. Make recommendations, if needed, for approval of major systems installations. Prepare milestone status reports and deliveries/presentations on the system concept to colleagues, subordinates, and end user representatives. Provide daily supervision and direction to support staff.

Minimum Education: Masters

Minimum Experience: 8 years

Cyber Security Test Engineer I

Functional Responsibilities: Conduct and/or support authorized penetration testing on enterprise network assets. Create penetration test documentation including Rules of Engagements and penetration testing reports. Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions. Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing. Prepare audit reports that identify technical and procedural findings and provide recommended remediation strategies/solutions. Perform technical (evaluation of technology) and nontechnical (evaluation of people and operations) risk and vulnerability assessments of relevant

technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications). Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes). Research new threats, attack vectors, and risk. Analyze results of scans to identify threats and vulnerabilities, analyze controls planned or already in place, determine the likelihood that identified vulnerabilities may be exploited by testing exploitation, and provide an analysis which includes recommended remediation strategies for comprehensive security program improvements. Validate findings and research methods for mitigation when deemed necessary by the agency. This includes retesting findings to validate vulnerability remediation and/or gathering information to assist system owners with the mitigation of findings.

Minimum Education: Bachelors

Minimum Experience: 0 years

Cyber Security Test Engineer II

Functional Responsibilities: Conduct and/or support authorized penetration testing on enterprise network assets. Create penetration test documentation including Rules of Engagements and penetration testing reports. Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions. Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing. Prepare audit reports that identify technical and procedural findings and provide recommended remediation strategies/solutions. Perform technical (evaluation of technology) and nontechnical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications). Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes). Research new threats, attack vectors, and risk. Analyze results of scans to identify threats and vulnerabilities, analyze controls planned or already in place, determine the likelihood that identified vulnerabilities may be exploited by testing exploitation, and provide an analysis which includes recommended remediation strategies for comprehensive security program improvements. Validate findings and research methods for mitigation when deemed necessary by the agency. This includes retesting findings to validate vulnerability remediation and/or gathering information to assist system owners with the mitigation of findings.

Minimum Education: Bachelors

Minimum Experience: 2 years

Cyber Security Test Engineer III

Functional Responsibilities: Conduct and/or support authorized penetration testing on enterprise network assets. Create penetration test documentation including Rules of Engagements and penetration testing reports. Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions. Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing. Prepare audit reports that identify technical and procedural findings and provide recommended remediation strategies/solutions. Perform technical (evaluation of technology) and

nontechnical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications). Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes). Research new threats, attack vectors, and risk. Analyze results of scans to identify threats and vulnerabilities, analyze controls planned or already in place, determine the likelihood that identified vulnerabilities may be exploited by testing exploitation, and provide an analysis which includes recommended remediation strategies for comprehensive security program improvements. Validate findings and research methods for mitigation when deemed necessary by the agency. This includes retesting findings to validate vulnerability remediation and/or gathering information to assist system owners with the mitigation of findings.

Minimum Education: Bachelors

Minimum Experience: 5 years

Cyber Security Test Engineer IV

Functional Responsibilities: Conduct and/or support authorized penetration testing on enterprise network assets. Create penetration test documentation including Rules of Engagements and penetration testing reports. Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions. Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing. Prepare audit reports that identify technical and procedural findings and provide recommended remediation strategies/solutions. Perform technical (evaluation of technology) and nontechnical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications). Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes). Research new threats, attack vectors, and risk. Analyze results of scans to identify threats and vulnerabilities, analyze controls planned or already in place, determine the likelihood that identified vulnerabilities may be exploited by testing exploitation, and provide an analysis which includes recommended remediation strategies for comprehensive security program improvements. Validate findings and research methods for mitigation when deemed necessary by the agency. This includes retesting findings to validate vulnerability remediation and/or gathering information to assist system owners with the mitigation of findings.

Minimum Education: Masters

Minimum Experience: 8 years

Cyber Threat Analyst I

Functional Responsibilities: Conduct all-source analysis, digital forensics, and targeting to identify, monitor, assess, and counter the threat posed by malicious actors against agency information systems, critical infrastructure, and cyber-related interests. Prepare and coordinate strategic, high-level Cyber Threat assessments, and provide tactical analysis, advice, and information concerning adversary cyber actions and capabilities to the Government. Use all-source analysis and all available disciplines to research, draft, and submit information to the Government. Collaborate with government and

contractor cyber threat analysts to satisfy requests for information from stakeholders throughout the agency enterprise as well as with external partners and stakeholders including but not limited to DHS, US-CERT, OMB, GAO, OIG, and law enforcement. Submit assessments on trending topics in Cyberspace SOC leadership review, approval, and distribution. Develop and present to senior decision / policymakers' agency-relevant briefing on threats to the agency Information Environment. Apply scientific and technical knowledge to solving complex problems, produce short-term and long-term written assessments, and brief decision makers. This work demands initiative, creativity, analytic skills, and technical expertise. Participate in cyberspace-related, community of interests and present key technical intelligence to senior decision/policymakers.

Minimum Education: Bachelors

Minimum Experience: 0 years

Cyber Threat Analyst II

Functional Responsibilities: Conduct all-source analysis, digital forensics, and targeting to identify, monitor, assess, and counter the threat posed by malicious actors against agency information systems, critical infrastructure, and cyber-related interests. Prepare and coordinate strategic, high-level Cyber Threat assessments, and provide tactical analysis, advice, and information concerning adversary cyber actions and capabilities to the Government. Use all-source analysis and all available disciplines to research, draft, and submit information to the Government. Collaborate with government and contractor cyber threat analysts to satisfy requests for information from stakeholders throughout the agency enterprise as well as with external partners and stakeholders including but not limited to DHS, US-CERT, OMB, GAO, OIG, and law enforcement. Submit assessments on trending topics in Cyberspace SOC leadership review, approval, and distribution. Develop and present to senior decision / policymakers' agency-relevant briefing on threats to the agency Information Environment. Apply scientific and technical knowledge to solving complex problems, produce short-term and long-term written assessments, and brief decision makers. This work demands initiative, creativity, analytic skills, and technical expertise. Participate in cyberspace-related, community of interests and present key technical intelligence to senior decision/policymakers.

Minimum Education: Bachelors

Minimum Experience: 2 years

Cyber Threat Analyst III

Functional Responsibilities: Conduct all-source analysis, digital forensics, and targeting to identify, monitor, assess, and counter the threat posed by malicious actors against agency information systems, critical infrastructure, and cyber-related interests. Prepare and coordinate strategic, high-level Cyber Threat assessments, and provide tactical analysis, advice, and information concerning adversary cyber actions and capabilities to the Government. Use all-source analysis and all available disciplines to research, draft, and submit information to the Government. Collaborate with government and contractor cyber threat analysts to satisfy requests for information from stakeholders throughout the agency enterprise as well as with external partners and stakeholders including but not limited to DHS, US-CERT, OMB, GAO, OIG, and law enforcement. Submit assessments on trending topics in Cyberspace SOC leadership review, approval, and distribution. Develop and present to senior decision / policymakers' agency-relevant briefing on threats to the agency Information Environment. Apply

scientific and technical knowledge to solving complex problems, produce short-term and long-term written assessments, and brief decision makers. This work demands initiative, creativity, analytic skills, and technical expertise. Participate in cyberspace-related, community of interests and present key technical intelligence to senior decision/policymakers.

Minimum Education: Bachelors

Minimum Experience: 5 years

Cyber Threat Analyst IV

Functional Responsibilities: Conduct all-source analysis, digital forensics, and targeting to identify, monitor, assess, and counter the threat posed by malicious actors against agency information systems, critical infrastructure, and cyber-related interests. Prepare and coordinate strategic, high-level Cyber Threat assessments, and provide tactical analysis, advice, and information concerning adversary cyber actions and capabilities to the Government. Use all-source analysis and all available disciplines to research, draft, and submit information to the Government. Collaborate with government and contractor cyber threat analysts to satisfy requests for information from stakeholders throughout the agency enterprise as well as with external partners and stakeholders including but not limited to DHS, US-CERT, OMB, GAO, OIG, and law enforcement. Submit assessments on trending topics in Cyberspace SOC leadership review, approval, and distribution. Develop and present to senior decision / policymakers' agency-relevant briefing on threats to the agency Information Environment. Apply scientific and technical knowledge to solving complex problems, produce short-term and long-term written assessments, and brief decision makers. This work demands initiative, creativity, analytic skills, and technical expertise. Participate in cyberspace-related, community of interests and present key technical intelligence to senior decision/policymakers.

Minimum Education: Masters

Minimum Experience: 8 years

Disaster Recovery Analyst I

Functional Responsibilities: Previous experience in business recovery or disaster recovery planning required. General knowledge of business processes, management structures, and technology programs/platforms are preferred. Strong verbal and written communications skills are desirable. Provide support in the development of a government agencies emergency management and business recovery plans; perform functions pertaining to the agencies business risk assessments; review and develop business recovery strategies; draft procedures for identifying failures and invoking contingency plans; create response procedures and identifying communications channels; communicate with various response teams during testing and actual execution of recovery procedures. Support the design, development, installation, implementation, and administration of backup solutions. Make recommendations to the user community and the operations group on system enhancements.

Minimum Education: Bachelors

Minimum Experience: 0 years

Disaster Recovery Analyst II

Functional Responsibilities: Previous experience in business recovery or disaster recovery planning required. General knowledge of business processes, management structures, and technology programs/platforms are preferred. Strong verbal and written communications skills are desirable. Provide support in the development of a government agencies emergency management and business recovery plans; perform functions pertaining to the agencies business risk assessments; review and develop business recovery strategies; draft procedures for identifying failures and invoking contingency plans; create response procedures and identifying communications channels; communicate with various response teams during testing and actual execution of recovery procedures. Support the design, development, installation, implementation, and administration of backup solutions. Make recommendations to the user community and the operations group on system enhancements.

Minimum Education: Bachelors

Minimum Experience: 2 years

Disaster Recovery Analyst III

Functional Responsibilities: Previous experience in business recovery or disaster recovery planning required. General knowledge of business processes, management structures, and technology programs/platforms are preferred. Strong verbal and written communications skills are desirable. Provide support in the development of a government agencies emergency management and business recovery plans; perform functions pertaining to the agencies business risk assessments; review and develop business recovery strategies; draft procedures for identifying failures and invoking contingency plans; create response procedures and identifying communications channels; communicate with various response teams during testing and actual execution of recovery procedures. Support the design, development, installation, implementation, and administration of backup solutions. Make recommendations to the user community and the operations group on system enhancements.

Minimum Education: Bachelors

Minimum Experience: 5 years

Disaster Recovery Analyst IV

Functional Responsibilities: Previous experience in business recovery or disaster recovery planning required. General knowledge of business processes, management structures, and technology programs/platforms are preferred. Strong verbal and written communications skills are desirable. Provide support in the development of a government agencies emergency management and business recovery plans; perform functions pertaining to the agencies business risk assessments; review and develop business recovery strategies; draft procedures for identifying failures and invoking contingency plans; create response procedures and identifying communications channels; communicate with various response teams during testing and actual execution of recovery procedures. Support the design, development, installation, implementation, and administration of backup solutions. Make recommendations to the user community and the operations group on system enhancements.

Minimum Education: Masters

Minimum Experience: 8 years

Information Systems Security Officer I

Functional Responsibilities: Develop and maintain all security documentation for systems under their purview. These documents shall include but are not limited to Privacy Threshold Analysis (PTA), Privacy Impact Assessments (PIA), System of Record Notices (SORNs), System Categorization, System Security Plans (SSP), Business Impact Assessments (BIA), Contingency Plan and Tests (CP and CPT), Security Authorization Briefing, Recommendation, Memo. Provide support for:

- System-level policies, processes, and procedures development, review, and updates
- Management of FISMA Inventory
- POA&M Management
- Risk Management
- Security Awareness & IT Role-Based Training Tracking
- Audit Support
- Security and Privacy-Related Data Call Support
- System Security Lifecycle Support
- Security Assessment & Authorization (SAA) System Owner Document Creation and Updates
- Continuous Monitoring System Owner Document Creation and Updates.

Review Change Requests (CR) to ensure that new systems include the appropriate security requirements at all phases of the SDLC. Complete Security Impact Analysis of changes as part of the CR process to ensure that the change will not have a negative impact to the OCIO GSS. Ensure analysis is completed within the timeframes outlined for CRs and Security Impact Analysis. Assist system owner and agency security stakeholders in capturing all system weaknesses in POA&Ms. Notify the Enterprise Security Operations Center (ESOC) of actual or suspected computer security incidents, including PH and/or PHI breaches. Assist the ESOC and System Owner on all IT security and privacy incident reporting and subsequent resolution/remediation.

Minimum Education: Bachelors

Minimum Experience: 0 years

Information Systems Security Officer II

Functional Responsibilities: Develop and maintain all security documentation for systems under their purview. These documents shall include but are not limited to Privacy Threshold Analysis (PTA), Privacy Impact Assessments (PIA), System of Record Notices (SORNs), System Categorization, System Security Plans (SSP), Business Impact Assessments (BIA), Contingency Plan and Tests (CP and CPT), Security Authorization Briefing, Recommendation, Memo. Provide support for:

- System-level policies, processes, and procedures development, review, and updates
- Management of FISMA Inventory
- POA&M Management
- Risk Management
- Security Awareness & IT Role-Based Training Tracking
- Audit Support
- Security and Privacy-Related Data Call Support
- System Security Lifecycle Support
- Security Assessment & Authorization (SAA) System Owner Document Creation and Updates
- Continuous Monitoring System Owner Document Creation and Updates.

Review Change Requests (CR) to ensure that new systems include the appropriate security requirements at all phases of the SDLC. Complete Security Impact Analysis of changes as part of the CR process to ensure that the change will not have a negative impact to the OCIO GSS. Ensure analysis is completed within the timeframes outlined for CRs and Security Impact Analysis. Assist system owner and agency security stakeholders in capturing all system weaknesses in POA&Ms. Notify the Enterprise Security Operations Center (ESOC) of actual or suspected computer security incidents, including PH and/or PHI breaches. Assist the ESOC and System Owner on all IT security and privacy incident reporting and subsequent resolution/remediation.

Minimum Education: Bachelors

Minimum Experience: 2 years

Information Systems Security Officer III

Functional Responsibilities: Develop and maintain all security documentation for systems under their purview. These documents shall include but are not limited to Privacy Threshold Analysis (PTA), Privacy Impact Assessments (PIA), System of Record Notices (SORNs), System Categorization, System Security Plans (SSP), Business Impact Assessments (BIA), Contingency Plan and Tests (CP and CPT), Security Authorization Briefing, Recommendation, Memo. Provide support for:

- System-level policies, processes, and procedures development, review, and updates
- Management of FISMA Inventory
- POA&M Management
- Risk Management
- Security Awareness & IT Role-Based Training Tracking
- Audit Support
- Security and Privacy-Related Data Call Support
- System Security Lifecycle Support
- Security Assessment & Authorization (SAA) System Owner Document Creation and Updates
- Continuous Monitoring System Owner Document Creation and Updates.

Review Change Requests (CR) to ensure that new systems include the appropriate security requirements at all phases of the SDLC. Complete Security Impact Analysis of changes as part of the CR process to ensure that the change will not have a negative impact to the OCIO GSS. Ensure analysis is completed within the timeframes outlined for CRs and Security Impact Analysis. Assist system owner and agency security stakeholders in capturing all system weaknesses in POA&Ms. Notify the Enterprise Security Operations Center (ESOC) of actual or suspected computer security incidents, including PH and/or PHI breaches. Assist the ESOC and System Owner on all IT security and privacy incident reporting and subsequent resolution/remediation.

Minimum Education: Bachelors

Minimum Experience: 5 years

Information Systems Security Officer IV

Functional Responsibilities: Develop and maintain all security documentation for systems under their purview. These documents shall include but are not limited to Privacy Threshold Analysis (PTA), Privacy Impact Assessments (PIA), System of Record Notices (SORNs), System Categorization, System Security

Plans (SSP), Business Impact Assessments (BIA), Contingency Plan and Tests (CP and CPT), Security Authorization Briefing, Recommendation, Memo. Provide support for:

- System-level policies, processes, and procedures development, review, and updates
- Management of FISMA Inventory
- POA&M Management
- Risk Management
- Security Awareness & IT Role-Based Training Tracking
- Audit Support
- Security and Privacy-Related Data Call Support
- System Security Lifecycle Support
- Security Assessment & Authorization (SAA) System Owner Document Creation and Updates
- Continuous Monitoring System Owner Document Creation and Updates.

Review Change Requests (CR) to ensure that new systems include the appropriate security requirements at all phases of the SDLC. Complete Security Impact Analysis of changes as part of the CR process to ensure that the change will not have a negative impact to the OCIO GSS. Ensure analysis is completed within the timeframes outlined for CRs and Security Impact Analysis. Assist system owner and agency security stakeholders in capturing all system weaknesses in POA&Ms. Notify the Enterprise Security Operations Center (ESOC) of actual or suspected computer security incidents, including PH and/or PHI breaches. Assist the ESOC and System Owner on all IT security and privacy incident reporting and subsequent resolution/remediation.

Minimum Education: Masters

Minimum Experience: 8 years

Network Security Administrator I

Functional Responsibilities: Perform the daily activities of configuration and operation of systems which may be mainframe, mini, or client/server based. Perform the optimizing of system operation and resource utilization and perform system capacity analysis and planning. Provide assistance to users in accessing and using business systems. Commensurate experience and education.

Minimum Education: Bachelors

Minimum Experience: 0 years

Network Security Administrator II

Functional Responsibilities: Perform the daily activities of configuration and operation of systems which may be mainframe, mini, or client/server based. Perform the optimizing of system operation and resource utilization and perform system capacity analysis and planning. Provide assistance to users in accessing and using business systems. Commensurate experience and education.

Minimum Education: Bachelors

Minimum Experience: 2 years

Network Security Administrator III

Functional Responsibilities: Perform the daily activities of configuration and operation of systems which may be mainframe, mini, or client/server based. Perform the optimizing of system operation and resource utilization and perform system capacity analysis and planning. Provide assistance to users in accessing and using business systems. Commensurate experience and education.

Minimum Education: Bachelors

Minimum Experience: 5 years

Network Security Administrator IV

Functional Responsibilities: Perform the daily activities of configuration and operation of systems which may be mainframe, mini, or client/server based. Perform the optimizing of system operation and resource utilization and perform system capacity analysis and planning. Provide assistance to users in accessing and using business systems. Commensurate experience and education.

Minimum Education: Masters

Minimum Experience: 8 years

Program Manager

Functional Responsibilities: Serve as the program manager responsible for organizing, directing, and managing all aspects of contract operational support functions involving multiple complex and inter-related project tasks that often require managing teams of contractor personnel at multiple locations. Provide overall direction of program activities. Manage and maintain contractor interface with the senior levels of the customer's organization. Consult with customer and contractor personnel to formulate and review task plans and deliverables, ensuring conformance with program and project task schedules, costs, contractual obligations. Establish and maintain technical and financial reports to show progress of projects to management and customers, organize and assign responsibilities to subordinates, oversee the successful completion of all assigned tasks, and assume the initiative and provide support to marketing personnel in identifying and acquiring potential business.

Minimum Education: Masters

Minimum Experience: 10 years

Project Manager I

Functional Responsibilities: Work directly with the government customer, who establishes direction, priorities, and provides overall operational guidance. Provide direct support and advice to the government customer and Federal team. Manage project scope, deliverables, and schedule. Manage work of all contractor and subcontract staff assigned to the Contract such that activities and deliverables are completed on time and to the customer's satisfaction. Directly oversee and participate in activities requiring senior technical and management skills, as appropriate. Assists the with tasks associated with formal meetings, (e.g., establishment of agenda, meeting minutes, tracking status of action items and deliverables, etc.). Prepare and submit all required reports to Contract Officer (CO) and COR. Apply project methodology (such as, scoping, planning, designing, building, deploying, and closing out project) using critical thinking and leadership skills. Assist in responding to data calls from senior leadership, Agency offices, the GAO, OMB, OIG, and other Federal Agencies.

Minimum Education: Bachelors

Minimum Experience: 2 years

Project Manager II

Functional Responsibilities: Work directly with the government customer, who establishes direction, priorities, and provides overall operational guidance. Provide direct support and advice to the government customer and Federal team. Manage project scope, deliverables, and schedule. Manage work of all contractor and subcontract staff assigned to the Contract such that activities and deliverables are completed on time and to the customer's satisfaction. Directly oversee and participate in activities requiring senior technical and management skills, as appropriate. Assists the with tasks associated with formal meetings, (e.g., establishment of agenda, meeting minutes, tracking status of action items and deliverables, etc.). Prepare and submit all required reports to Contract Officer (CO) and COR. Apply project methodology (such as, scoping, planning, designing, building, deploying, and closing out project) using critical thinking and leadership skills. Assist in responding to data calls from senior leadership, Agency offices, the GAO, OMB, OIG, and other Federal Agencies.

Minimum Education: Bachelors

Minimum Experience: 5 years

Project Manager III

Functional Responsibilities: Work directly with the government customer, who establishes direction, priorities, and provides overall operational guidance. Provide direct support and advice to the government customer and Federal team. Manage project scope, deliverables, and schedule. Manage work of all contractor and subcontract staff assigned to the Contract such that activities and deliverables are completed on time and to the customer's satisfaction. Directly oversee and participate in activities requiring senior technical and management skills, as appropriate. Assists the with tasks associated with formal meetings, (e.g., establishment of agenda, meeting minutes, tracking status of action items and deliverables, etc.). Prepare and submit all required reports to Contract Officer (CO) and COR. Apply project methodology (such as, scoping, planning, designing, building, deploying, and closing out project) using critical thinking and leadership skills. Assist in responding to data calls from senior leadership, Agency offices, the GAO, OMB, OIG, and other Federal Agencies.

Minimum Education: Masters

Minimum Experience: 8 years

Security Analyst I

Functional Responsibilities: Conduct Intrusion Detection Monitoring Operations. Monitor all agency networks and perimeter boundaries to wider networks. Review and analyze sensor data provided by agency Cybersecurity Automated Systems. Use correlated data analysis to identify unauthorized activity detected by Cybersecurity Automated Systems. Conduct near real-time review of logs when a security event is detected. Search for and report distributed, long-term, coordinated, low-visibility network-based attacks across agency networks to identify possible unauthorized activity. Follow formal procedures for creating and distributing warnings and notifications to the agency. Provide interim guidance and countermeasures to defend against identified threats. Review, and when appropriate recommend/update network/system configuration or rule sets in response to changes in the threat environment and notify the agency. Distribute formal guidance to ISOs that support best practices for security configuration.

Minimum Education: Bachelors

Minimum Experience: 0 years

Security Analyst II

Functional Responsibilities: Conduct Intrusion Detection Monitoring Operations. Monitor all agency networks and perimeter boundaries to wider networks. Review and analyze sensor data provided by agency Cybersecurity Automated Systems. Use correlated data analysis to identify unauthorized activity detected by Cybersecurity Automated Systems. Conduct near real-time review of logs when a security event is detected. Search for and report distributed, long-term, coordinated, low-visibility network-based attacks across agency networks to identify possible unauthorized activity. Follow formal procedures for creating and distributing warnings and notifications to the agency. Provide interim guidance and countermeasures to defend against identified threats. Review, and when appropriate recommend/update network/system configuration or rule sets in response to changes in the threat environment and notify the agency. Distribute formal guidance to ISOs that support best practices for security configuration.

Minimum Education: Bachelors

Minimum Experience: 2 years

Security Analyst III

Functional Responsibilities: Conduct Intrusion Detection Monitoring Operations. Monitor all agency networks and perimeter boundaries to wider networks. Review and analyze sensor data provided by agency Cybersecurity Automated Systems. Use correlated data analysis to identify unauthorized activity detected by Cybersecurity Automated Systems. Conduct near real-time review of logs when a security event is detected. Search for and report distributed, long-term, coordinated, low-visibility network-based attacks across agency networks to identify possible unauthorized activity. Follow formal procedures for creating and distributing warnings and notifications to the agency. Provide interim guidance and countermeasures to defend against identified threats. Review, and when appropriate recommend/update network/system configuration or rule sets in response to changes in the threat environment and notify the agency. Distribute formal guidance to ISOs that support best practices for security configuration.

Minimum Education: Bachelors

Minimum Experience: 5 years

Security Analyst IV

Functional Responsibilities: Conduct Intrusion Detection Monitoring Operations. Monitor all agency networks and perimeter boundaries to wider networks. Review and analyze sensor data provided by agency Cybersecurity Automated Systems. Use correlated data analysis to identify unauthorized activity detected by Cybersecurity Automated Systems. Conduct near real-time review of logs when a security event is detected. Search for and report distributed, long-term, coordinated, low-visibility network-based attacks across agency networks to identify possible unauthorized activity. Follow formal procedures for creating and distributing warnings and notifications to the agency. Provide interim guidance and countermeasures to defend against identified threats. Review, and when appropriate recommend/update network/system configuration or rule sets in response to changes in the threat environment and notify the agency. Distribute formal guidance to ISOs that support best practices for security configuration.

Minimum Education: Masters

Minimum Experience: 8 years

Security Awareness Training Specialist I

Functional Responsibilities: Provide support for coordinating, developing, and delivering computer-related security training to the user community. Provide second level support and coordinate training with help desks. Provide standards, services, and guidance on IT related training programs that are designed to enable government agency personnel to use information technologies and systems more productively. Services include the development, delivery, and/or coordination of training courses and materials that address specific agency needs. Possess thorough knowledge of appropriate hardware and software (ex. - PCs, Microsoft (MS) Windows). Understand computer functions and related technical terminology and how they are applied in everyday business situations. Possess exceptional interpersonal skills and superior oral and written communication skills.

Minimum Education: Bachelors

Minimum Experience: 0 years

Security Awareness Training Specialist II

Functional Responsibilities: Provide support for coordinating, developing, and delivering computer-related security training to the user community. Provide second level support and coordinate training with help desks. Provide standards, services, and guidance on IT related training programs that are designed to enable government agency personnel to use information technologies and systems more productively. Services include the development, delivery, and/or coordination of training courses and materials that address specific agency needs. Possess thorough knowledge of appropriate hardware and software (ex. - PCs, Microsoft (MS) Windows). Understand computer functions and related technical terminology and how they are applied in everyday business situations. Possess exceptional interpersonal skills and superior oral and written communication skills.

Minimum Education: Bachelors

Minimum Experience: 2 years

Security Awareness Training Specialist III

Functional Responsibilities: Provide support for coordinating, developing, and delivering computer-related security training to the user community. Provide second level support and coordinate training with help desks. Provide standards, services, and guidance on IT related training programs that are designed to enable government agency personnel to use information technologies and systems more productively. Services include the development, delivery, and/or coordination of training courses and materials that address specific agency needs. Possess thorough knowledge of appropriate hardware and software (ex. - PCs, Microsoft (MS) Windows). Understand computer functions and related technical terminology and how they are applied in everyday business situations. Possess exceptional interpersonal skills and superior oral and written communication skills.

Minimum Education: Bachelors

Minimum Experience: 5 years

Security Awareness Training Specialist IV

Functional Responsibilities: Provide support for coordinating, developing, and delivering computer-related security training to the user community. Provide second level support and coordinate training with help desks. Provide standards, services, and guidance on IT related training programs that are designed to enable government agency personnel to use information technologies and systems more productively. Services include the development, delivery, and/or coordination of training courses and materials that address specific agency needs. Possess thorough knowledge of appropriate hardware and software (ex. - PCs, Microsoft (MS) Windows). Understand computer functions and related technical terminology and how they are applied in everyday business situations. Possess exceptional interpersonal skills and superior oral and written communication skills.

Minimum Education: Masters

Minimum Experience: 8 years

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. Successful completion of each course in specialized or emerging technology (Windows Oracle, PowerBuilder, Web development, internet/intranet security, and XML, etc.) may be substituted for one year of experience.

Labor Category	Standard Qualifications		Substitution				
	Min Edu	Min Exp	PhD	Masters	Bachelors	Associates	High School
Chief Information Security Officer (CISO)	Masters	10	8	10	12	14	16
Cyber Security and Information Security Engineer I	Bachelors	0	0	0	0	2	4
Cyber Security and Information Security Engineer II	Bachelors	2	0	0	2	4	6

	Standard Qualifications		Substitution				
Labor Category	Min Edu	Min Exp	PhD	Masters	Bachelors	Associates	High School
Cyber Security and Information Security Engineer III	Bachelors	5	1	3	5	7	9
Cyber Security and Information Security Engineer IV	Masters	8	6	8	10	12	14
Cyber Security Architect I	Bachelors	0	0	0	0	2	4
Cyber Security Architect II	Bachelors	2	0	0	2	4	6
Cyber Security Architect III	Bachelors	5	1	3	5	7	9
Cyber Security Architect IV	Masters	8	6	8	10	12	14
Cyber Security SME I	Bachelors	2	0	0	2	4	6
Cyber Security SME II	Bachelors	5	1	3	5	7	9
Cyber Security SME III	Masters	8	6	8	10	12	14
Cyber Security Software Developer I	Bachelors	0	0	0	0	2	4
Cyber Security Software Developer II	Bachelors	2	0	0	2	4	6
Cyber Security Software Developer III	Bachelors	5	1	3	5	7	9
Cyber Security Software Developer IV	Masters	8	6	8	10	12	14
Cyber Security Systems Analyst I	Bachelors	0	0	0	0	2	4
Cyber Security Systems Analyst II	Bachelors	2	0	0	2	4	6
Cyber Security Systems Analyst III	Bachelors	5	1	3	5	7	9
Cyber Security Systems Analyst IV	Masters	8	6	8	10	12	14
Cyber Security Test Engineer I	Bachelors	0	0	0	0	2	4
Cyber Security Test Engineer II	Bachelors	2	0	0	2	4	6
Cyber Security Test Engineer III	Bachelors	5	1	3	5	7	9
Cyber Security Test Engineer IV	Masters	8	6	8	10	12	14
Cyber Threat Analyst I	Bachelors	0	0	0	0	2	4
Cyber Threat Analyst II	Bachelors	2	0	0	2	4	6
Cyber Threat Analyst III	Bachelors	5	1	3	5	7	9
Cyber Threat Analyst IV	Masters	8	6	8	10	12	14
Disaster Recovery Analyst I	Bachelors	0	0	0	0	2	4
Disaster Recovery Analyst II	Bachelors	2	0	0	2	4	6
Disaster Recovery Analyst III	Bachelors	5	1	3	5	7	9

	Standard Qualifications		Substitution				
Labor Category	Min Edu	Min Exp	PhD	Masters	Bachelors	Associates	High School
Disaster Recovery Analyst IV	Masters	8	6	8	10	12	14
Information Systems Security Officer I	Bachelors	0	0	0	0	2	4
Information Systems Security Officer II	Bachelors	2	0	0	2	4	6
Information Systems Security Officer III	Bachelors	5	1	3	5	7	9
Information Systems Security Officer IV	Masters	8	6	8	10	12	14
Network Security Administrator I	Bachelors	0	0	0	0	2	4
Network Security Administrator II	Bachelors	2	0	0	2	4	6
Network Security Administrator III	Bachelors	5	1	3	5	7	9
Network Security Administrator IV	Masters	8	6	8	10	12	14
Program Manager	Masters	10	8	10	12	14	16
Project Manager I	Bachelors	2	0	0	2	4	6
Project Manager II	Bachelors	5	1	3	5	7	9
Project Manager III	Masters	8	6	8	10	12	14
Security Analyst I	Bachelors	0	0	0	0	2	4
Security Analyst II	Bachelors	2	0	0	2	4	6
Security Analyst III	Bachelors	5	1	3	5	7	9
Security Analyst IV	Masters	8	6	8	10	12	14
Security Awareness Training Specialist I	Bachelors	0	0	0	0	2	4
Security Awareness Training Specialist II	Bachelors	2	0	0	2	4	6
Security Awareness Training Specialist III	Bachelors	5	1	3	5	7	9
Security Awareness Training Specialist IV	Masters	8	6	8	10	12	14

Labor Category Descriptions

SIN 54151S

Business Analyst I

Functional Responsibilities: Documents business requirements, authors test scripts, and develops other software documentation. Conducts requirements analysis and testing; helps build a strong client relationship; and provides client assistance with solving problems. In addition to supporting requirements evaluation, the business analyst supports all phases of the Software Development Life Cycle (SDLC) including project management support, process implementation, product evaluation, quality assurance, and systems documentation. Works closely with various project stakeholders including customers, project managers, technical leads, and others. Experience with the full lifecycle development is required; experience using tools to author, manage and test requirements is a plus (i.e. Rational RequisitePro). Experience using the Rational Unified Process methodology, particularly Use-Case development, is a plus. Excellent written and verbal skills are required. The candidate must be a self-starter with a great attitude and good communication skills.

Minimum Education: Bachelors

Minimum Experience: 2 years

Business Analyst III

Functional Responsibilities: Oversees plans for automated data processing systems from project inception to conclusion. Analyzes user needs to determine requirements and conducts feasibility studies. Identifies resources required for each task. May supervise a large support staff and/or serve as liaison to client staff. Provides strategic guidance to other technical staff in areas such as specifications, architectures, and information system design. Researches developments in field of expertise and applies them to the client environment including emerging technologies, lessons learned, best practices, and assessment methodologies. Interfaces with client personnel at all organizational levels. Develops white papers and system documentation. Converts functional specifications to technical specifications. Works independently without direct supervision.

Minimum Education: Bachelors

Minimum Experience: 5 years

Business Transformation Engineer III

Functional Responsibilities: Identifies, assesses, and records near-, medium-, and long-term business needs and technology solutions. Conducts requirements gathering meetings, prepare meeting notes, and follow up on agreed action items. Provide use-case scenarios. Prepares and tracks project plans for project inception to completion. Manages day-to-day individual workload, monitors milestones and critical dates. Documents business requirements and communicates them to build team. Facilitates the implementation of new functionality, training, and troubleshooting. Promotes teamwork and knowledge sharing in pursuit of effective problem solving. Position requires three years of business technology experience with a variety of assignments.

Minimum Education: Bachelors

Minimum Experience: 8 years

Developer I

Functional Responsibilities: Analyzes and studies complex system requirements. Designs software tools and subsystems to support software reuse and domain analyses and manages their implementation. Responsible for implementing software from formal specifications, data flow diagrams, and other accepted design techniques. Interprets software requirements and design specifications to code and integrates and tests software components. Works independently with minimal direct supervision.

Minimum Education: Associates

Minimum Experience: 2 years

Developer II

Functional Responsibilities: Works closely with management, technical team and customers to clarify project objectives. Assists in defining software requirements and establishing standards and methodologies for design and development of software applications. Responsible for implementing software from formal specifications, data flow diagrams, another accepted design techniques. Interprets software requirements and design specifications to code and integrates and tests software components. May have supervisory responsibility.

Minimum Education: Bachelors

Minimum Experience: 4 years

Developer III

Functional Responsibilities: Analyzes and studies complex system requirements. Designs software tools and subsystems to support software reuse and domain analyses and manages their implementation. Manages software development and support using formal specifications, data flow diagrams, and other accepted design techniques. Interprets software requirements and design specifications to code and integrates and tests software components. Estimates software development costs and schedule. May supervise a staff of programmers and/or other engineers. Works independently without direct supervision.

Minimum Education: Bachelors

Minimum Experience: 7 years

Engineer/Scientist VII

Functional Responsibilities: Makes decisions and recommendations that are recognized as authoritative and have an important impact on engineering activities. Requires the use of advanced techniques and the modification and of theories, precepts, and practices of the field and related sciences and disciplines.

Minimum Education: Bachelors

Minimum Experience: 15 years

Expert / Consultant III

Functional Responsibilities: Demonstrated experience and ability to confer with client executive management using industry expertise to define the client's strategic enterprise goals and advises in the reengineering of high level business processes to meet these goals. Demonstrated experience and ability to analyze client requirements and recommend development or acquisition strategies. Demonstrated experience and ability to assist client in developing strategies and concepts. Ability to make recommendations and advise on system-wide improvements, risk management, information management/information technology, optimization, and maintenance efforts in the functional area being addressed. Demonstrated experience and ability to effectively communicate, both orally and in writing.

Minimum Education: Masters

Minimum Experience: 12 years

Management Analyst I

Functional Responsibilities: Responsible for a multiple of program management areas to include but not limited to finance, contracts, and security. Researches, analyzes, and develops reports, spreadsheets, forms, and databases. Responsible for automated support and reporting for Program Management, and direct support to management efforts as directed.

Minimum Education: Associates

Minimum Experience: 5 years

Management Analyst II

Functional Responsibilities: Responsible for a multiple of program management areas to include but not limited to finance, contracts, and security. Researches, analyzes, and develops reports, spreadsheets, forms, and databases. In addition, scope of work shall require specialized experience in certain areas for support in order to be able to do the job. Contractor personnel shall have higher level of responsibility in areas of support.

Minimum Education: Bachelors

Minimum Experience: 4 years

Management Analyst III

Functional Responsibilities: Responsible for direct support to the program manager providing functions to include systems acquisition planning and electronic commerce. Responsible for financial reporting, accounting support, financial planning, audit support, and general financial management support services.

Minimum Education: Bachelors

Minimum Experience: 5 years

Management Analyst IV

Functional Responsibilities: Responsible for accounting services, transcription services, financial data entry, and financial reporting support.

Minimum Education: Bachelors

Minimum Experience: 8 years

Network Specialist

Functional Responsibilities: Designs, installs, maintains, and coordinates the use of complex networks. Evaluates hardware and software. Develops security procedures. Analyzes network designs and researches new technologies. Troubleshoots and resolves complex problems. Implements and coordinates network policies, procedures, and standards. Trains end users. Supervisory responsibilities. May be responsible for penetration testing, survivability and vulnerability analysis, and contingency/disaster recovery planning. Works independently without direct supervision.

Minimum Education: Bachelors

Minimum Experience: 4 years

Network/Hardware Specialist

Functional Responsibilities: System analysis and evaluation of hardware and network capabilities and configurations. Must demonstrate the ability to work independently or under only general direction. Reviews computer systems in terms of machine capabilities and man-machine YY. Prepares reports and studies concerning hardware. Prepares functional requirements and specifications for hardware acquisitions. Ensures that problems have been properly identified and solutions will satisfy the user's requirements. Designs and optimizes network topologies. Directs and leads preparation of engineering plans and site installation Technical Design Packages. Develops hardware installation schedules. Directs and leads preparation of drawings documenting configuration changes at each site. Prepares site installation and test reports.

Minimum Education: Associates

Minimum Experience: 4 years

Principal Information Engineer

Functional Responsibilities: Performs advanced specialized systems programming duties including design, specifications development, and computerized information systems implementation to include web-based applications. Supervises programmers and other technical staff on complex projects. Consults with user management and technical staff to clarify client needs, problems, and strategy. Assigns, coordinates, and reviews work developers. May train lower-level staff. Works independently without direct supervision.

Minimum Education: Bachelors

Minimum Experience: 7 years

Program Manager I

Functional Responsibilities: Responsible for overall program management of complex, multi-task IT contracts. Oversees all technical operations, prepares financial and budget reports, and tracks financial and contractual requirements. Responsible for cost and quality control. Works with client representatives to ensure smooth contract operation. Manages technical and administrative personnel. Works independently without direct supervision.

Minimum Education: Bachelors

Minimum Experience: 7 years

Program Manager II

Functional Responsibilities: Responsible for overall program management of complex, multi-task IT contracts. Oversees all technical operations, prepares financial and budget reports, and tracks financial and contractual requirements. Responsible for cost and quality control. Works with client representatives to ensure smooth contract operation. Manages technical and administrative personnel. Works independently without direct supervision.

Minimum Education: Bachelors

Minimum Experience: 10 years

Project Manager I

Functional Responsibilities: Manages small projects or single tasks on large, complex projects. Directs completion of tasks within estimated timeframes and budget constraints. Schedules and assigns duties to subordinates and subcontractors and ensures assignments are completed as directed. Ensures compliance with contract requirements. May be a senior technical expert who provides advice, design, and development on complex technical tasks. Works independently without direct supervision.

Minimum Education: Bachelors

Minimum Experience: 4 years

Project Manager II

Functional Responsibilities: Manages small projects or single tasks on large, complex projects. Schedules and assigns duties to subordinates and subcontractors and ensures assignments are completed as directed. Ensures compliance with contract requirements. May be a senior technical expert who provides advice, design, and development on complex technical tasks. Leads software projects on a variety of software platforms. Skills should include cost and budget management, risk management, resource management and very strong customer interfacing abilities. Must be strong at creating and verifying software project documentation including systems requirements, systems designs, test plans, and project reviews. Works independently without direct supervision. Must possess strong written and oral communication skills to ensure effective interaction with customers and project team members.

Minimum Education: Bachelors

Minimum Experience: 8 years

Subject Matter Expert

Functional Responsibilities: Highly skilled individual who has the technological expertise in the specific functional tasks required for performance of the task order. Significant professional accomplishments relevant to the engineering/scientific topic or key considerations.

Minimum Education: Bachelors

Minimum Experience: 3 years

Systems Administrator

Functional Responsibilities: Administration of UNIX, Windows NT, Banyan Vines or Novell systems or open systems and/or legacy systems. General experience includes operations experience on a large-scale computer system or a multi-server local area network. Supervises and manages the daily activities of configuration and operation of business systems which may be mainframe, mini, or client/server based. Optimizes system operation and resource utilization and performs system capacity analysis and planning. Provides assistance to users in accessing and using business systems.

Minimum Education: Bachelors

Minimum Experience: 4 years

Systems Analyst I

Functional Responsibilities: Analyzes, develops, and reviews computer systems. Defines and analyzes problems and develops system requirements and program specifications. Prepares required systems documentation.

Minimum Education: Associates

Minimum Experience: 4 years

Systems Analyst II

Functional Responsibilities: Analyzes user needs to determine requirements and conducts feasibility studies. Identifies resources required for each task. May supervise a small support staff and/or serve as liaison to client staff. Researches developments in field of expertise and applies them to the client environment including emerging technologies, lessons learned, best practices, and assessment methodologies. Interfaces with client personnel at all organizational levels. Develops white papers and system documentation. Converts functional specifications to technical specifications. Works independently without direct supervision.

Minimum Education: Bachelors

Minimum Experience: 4 years

Systems Analyst III

Functional Responsibilities: Possesses an understanding of requirements analysis and requirements management, along with broad familiarity with a range of technology solution areas and current knowledge of industry trends and developments. Guides clients through the analytical portions of a software project by leading client meetings, strategy sessions and making recommendations when necessary. Works closely with customers, managers, and other technical team members to synthesize

information into a clear development approach. Has extensive experience with full lifecycle development methodologies, including the Rational Unified Process, in particular Use-Case development and UML Modeling. Possesses excellent written and oral communication skills and has excellent time management, job scoping, and estimating skills as well. Assists project manager with the planning and re-sourcing of design, development, testing and delivery phases of projects

Minimum Education: Bachelors

Minimum Experience: 7 years

Systems Analyst IV

Functional Responsibilities: System analysis and evaluation of hardware and network capabilities and configurations. Must demonstrate the ability to work independently or under only general direction. Reviews computer systems in terms of machine capabilities and man-machine interface. Prepares reports and studies concerning hardware. Prepares functional requirements and specifications for hardware acquisitions. Ensures that problems have been properly identified and solutions will satisfy the user's requirements. Designs and optimizes network topologies. Directs and leads preparation of engineering plans and site installation Technical Design Packages. Develops hardware installation schedules. Directs and leads preparation of drawings documenting configuration changes at each site. Prepares site installation and test reports.

Minimum Education: Bachelors

Minimum Experience: 5 years

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. Successful completion of each course in specialized or emerging technology (Windows Oracle, PowerBuilder, Web development, internet/intranet security, and XML, etc.) may be substituted for one year of experience.

Labor Category	Standard Qualifications		Substitution				
	Min Edu	Min Exp	PhD	Masters	Bachelors	Associates	High School
Business Analyst I	Bachelors	2	0	0	2	4	6
Business Analyst III	Bachelors	5	1	3	5	7	9
Business Transformation Engineer III	Bachelors	8	4	6	8	10	12
Developer I	Associates	2	0	0	0	2	4
Developer II	Bachelors	4	0	2	4	6	8
Developer III	Bachelors	7	3	5	7	9	11
Engineer/Scientist VII	Bachelors	15	11	13	15	17	19
Expert / Consultant III	Masters	12	10	12	14	16	18

	Standard Qualifications		Substitution				
Labor Category	Min Edu	Min Exp	PhD	Masters	Bachelors	Associates	High School
Management Analyst I	Associates	5	0	1	3	5	7
Management Analyst II	Bachelors	4	0	2	4	6	8
Management Analyst III	Bachelors	5	1	3	5	7	9
Management Analyst IV	Bachelors	8	4	6	8	10	12
Network Specialist	Bachelors	4	0	2	4	6	8
Network/Hardware Specialist	Associates	4	0	0	2	4	6
Principal Information Engineer	Bachelors	7	3	5	7	9	11
Program Manager I	Bachelors	7	3	5	7	9	11
Program Manager II	Bachelors	10	6	8	10	12	14
Project Manager I	Bachelors	4	0	2	4	6	8
Project Manager II	Bachelors	8	4	6	8	10	12
Subject Matter Expert	Bachelors	3	0	1	3	5	7
Systems Administrator	Bachelors	4	0	2	4	6	8
Systems Analyst I	Associates	4	0	0	2	4	6
Systems Analyst II	Bachelors	4	0	2	4	6	8
Systems Analyst III	Bachelors	7	3	5	7	9	11
Systems Security Specialist	Bachelors	5	1	3	5	7	9