PERSONNEL QUALIFICATIONS

Information Assurance, Computer Security, and
Network Infrastructure Support

1. INTRODUCTION

The Naval Research Laboratory (NRL) established a representative matrix of the labor categories and skills to which the contractor shall propose. Resumes shall use the same labor category headings to relate the experience of the candidates to the standards set forth below. If the contractor uses a labor category terminology other than that used in this provision, the contractor must provide a matrix clearly relating their proposed labor categories to those in the provision. All security requirements shall be met at time of proposal submission.

Note: Educational requirements for any of the labor categories in this document can be substituted as follows:

Degree	**Substitution**
Associate's Degree	2 years of additional related work experience
Bachelor's Degree	4 years of additional related work experience; or Associate's degree plus 2 years of additional related work experience

2.0 PERSONNEL REQRUIREMENTS

The following labor categories are required for this effort. Their associated qualifications are on the subsequent pages.

Electronics Technician Level IV

Position Requirements

Key Personnel: No

Security Clearance: Top Secret-SCI

Degree: Associate's or Electronic Technical Certification

Degree Field: Electronics, mathematics, science, or another technical field.

Experience: 8 years developing, maintaining, enhancing, and tracking high-speed network equipment, routers, switches, and servers in Research & Development (R&D) and production enclaves.

Responsibilities

- Provide support to space, ground, and communications systems.
- Develop, maintain, and enhance high-speed network systems and maintenance CONOPS to support Research & Development Enclaves with external connections to Production Enclaves.
- Address offensive actions in the R&D domain in support of rapidly changing cybersecurity requirements.
- Performs a variety of complex technical duties, including systems modification, troubleshooting, tests, and major repairs on electronic and electro-mechanical equipment, as a part of a maintenance and operations process.
- Apply an in-depth knowledge of electronic theory and practices.
- Support and modify hardware and system configuration to support the DoD RMF and DNI 503 C&A process.
- Design and configure thick and thin client architectures.
- Read and interpret schematic and wiring diagrams, wave forms and diagnostic results, assembly drawings and specifications, and relates these to overall system performance or malfunctions.
- Implement and maintain network and system configuration in accordance with TEMPEST guidelines.
- Configure SANS and NAS storage systems to support Government projects.
- Disassembles and reassembles complex equipment for the repair or replacement of defective parts, wiring, and electrical or mechanical units.
- Assembles and fabricates systems from the component-level, using correct wire wrap, solder, and assembly techniques.
- Assists in the design of electronic circuits and mechanical modifications to permit successful interfacing of equipment to related systems.
- Create and maintain department configuration management databases and spreadsheets for networks and hardware configuration.
- Maintain a detail software and hardware license agreement database and tracking and ordering support supplies as required.
- Inspects, tests, and advises on the operation and troubleshooting of equipment such as computer systems and associated peripheral hardware.
- Troubleshoot communications and cryptologic equipment
- Knowledge working with fiber, CAT6 cables and LC, SC, ST connectors.
- Directs or coordinates the work of other technicians, as assigned.

Network Administrator Level IV KEY

Position Requirements

Key Personnel:	Yes
Security Clearance:	Top Secret-SCI
Training & Certifications:	DoD 8570.01 IAT level II at the computing environment (CE)
Degree:	Bachelors
Degree Field:	Mathematics, Engineering, Computer Science, Computer Networks and Security or another technical field.
Experience:	6 years developing, maintaining, defending from cybersecurity threats, and enhancing high-speed network systems to support R&D capabilities in development and production enclaves.

Responsibilities

- Develop, maintain, and enhance high-speed network systems.
- Manage Research & Development and Production Enclaves.
- Address offensive actions in the cyber domain.
- Implement technology information directives such as DoD Risk Management Framework (RMF) and Intelligence Community Directive (ICD) 503 process.
- Implement Information Assurance and Information Condition (INFOCON) requirements.
- Apply a broad range of network concepts to assignments of a complex and sophisticated nature to solve scientific and/or engineering problems through the use of data processing equipment.
- Install and configure CISCO, Brocade, and Juniper network equipment.
- Work with IOS and NXOS applications.
- Apply techniques for analyzing, designing, installing, configuring, maintaining, and repairing network infrastructure and application components.
- Use network application tools (Solar Winds, CiscoNetwork Asst. WireShark, Red Seal...).
- Define a network layout, protocols and bandwidth requirements to support DoD and IC R&D and operational requirements.
- Provide direction, and recommendations regarding network configuration and installations.
- Engineer secured and hardened mission-critical systems for Comprehensive Network Defense.
- Work with fiber, CAT6 cables and LC, SC, ST cable connectors.

Desired Qualifications

- 2 additional years of relevant work experience administering workstations and securing servers to protect against cyber security threats in a R&D enclave.

System Administrator Level I

Position Requirements

Key Personnel:	No
Security Clearance:	Top Secret-SCI
Training & Certifications:	DoD 8570.01 IAT level II at the computing environment (CE)
Degree:	Associate's
Degree Field:	Computer Science, Information System Management, Cybersecurity Management or another technical field.
Experience:	3 years administering computer systems and securing them from cybersecurity threats to support R&D capabilities.

Responsibilities

- Collaborate with other Systems administrators to maintain computer systems, IAVAs compliance, and identify user security requirements.
- Support Research & Development information systems connected to Production information systems.
- Install new/rebuild existing servers and configure hardware, peripherals, services, settings, directories, storage, etc. in accordance with standards and project/operational requirements.
- Gather and enter security data inputs into the eMASS C&A tool.
- Gather and enter security data inputs into the XACTA C&A tool.
- Perform the DoD RMF and DNI ICD 503 activities to meet the C&A requirements.
- Research and recommend innovative, and where possible automated approaches for system administration tasks.
- Identify approaches that leverage resources and provide economies of scale.
- Perform daily system monitoring, verifying the integrity and availability of all hardware, server resources, systems and key processes, reviewing system and application logs, and verifying completion of scheduled jobs such as backups.
- Perform backup operations, ensuring all required file systems and system data are successfully backed up to the appropriate media, recovery tapes or disks are created, and media is recycled and sent off site as necessary.
- Create, change, and delete user accounts per request.
- Repair and recover from hardware or software failures. Coordinate and communicate with impacted constituencies.
- Apply Operating System (OS) patches and upgrades on a regular basis, and upgrade administrative tools and utilities.
- Configure / add new services as necessary.
- Maintain operational, configuration, or other procedures.
- Perform ongoing performance tuning, hardware upgrades, and resource optimization as required.
- Configure CPU, memory, and disk partitions as required.
- Evaluate and install patches.
- Resolve software related problems.
- Perform system backups and recovery.
- Use Information Assurance security monitoring tools (i.e. WASSP, ACAS, HBSS).

System Administrator Level III

Position Requirements

Key Personnel:	No
Security Clearance:	Top Secret-SCI
Training & Certifications:	DoD 8570.01 IAT level II at the computing environment (CE)
Degree:	Bachelor's
Degree Field:	Computer Science, Information System Management, Cybersecurity Management or another technical field.
Experience:	2 years administering computer systems and securing them from cybersecurity threats to support R&D capabilities in development and production enclaves.

Responsibilities

- Collaborate with other Systems Administrators to maintain computer systems, IAVAs compliance, and identify user security requirements.
- Support Research & Development and Production information systems.
- Monitor, maintain, configure and secure multiple McAfee's Host Base Security Solution (HBSS) point products in different environments.
- Design, configure, and install a NESSUS scanning environment (physical or virtual).
- Maintain ePolicy Orchestrator, deploy Virus Scan Enterprise (VSE) and Host Intrusion Prevention (HIPS), and create exceptions to allow authorized applications to run without triggering events.
- Update and manage ePolicy Orchestrator's master repository using scheduled server task.
- Implement the DoD RMF and DNI ICD 503 directives to meet C&A requirements.
- Maintain system patching, as well as operating systems, in accordance with Security Technical Implementation Guide (STIG) compliance.
- Perform configuration verification and vulnerability assessment scans using Tenable Assured Compliance Assessment Solution (ACAS) Management.
- Create and schedule client and server tasks for software, patch, and hot fix deployment to managed end points.
- Build system configuration baselines that leverage the DISA Security Technical Implementation Guides (STIG) and Security Content Automation Protocol (SCAP) for both Windows and Linux operating systems.
- Administer software used on the domain including, but not limited to:
    - Good Mobile Control Server version 2.7.4.1115
    - BlackBerry Enterprise Mobile Server version 2.4.18.19
    - Apple Mac OS (32-bit and 64-bit).
- Troubleshoot HBSS deployments in Windows and Linux environments.

System Administrator Level III-Active Directory

Position Requirements

Key Personnel:	No
Security Clearance:	Top Secret-SCI
Training & Certifications:	DoD 8570.01 IAT level II at the computing environment (CE)
Degree:	Bachelor's
Degree Field:	Computer Science, Information System Management, Cybersecurity Management or another technical field.
Experience:	4 years administering computer systems and securing them from cybersecurity threats to support R&D capabilities in development and production enclaves.

Responsibilities

- Collaborate with other Systems administrators to maintain computer systems, IAVAs compliance, and identify user security requirements.
- Support Research & Development and Production information systems.
- Support all aspects of an Active Directory network including:
    - DNS, Firewall and SMTP gateways.
    - LAN, WAN and all remote connectivity
    - Ethernet Topology.
    - Configuration Management and Report Generation.
    - Implementing Global Policies.
    - Good Mobile Control Server version 2.7.4.1115
    - BlackBerry Enterprise Mobile Server version 2.4.18.19
    - Samsung Mobile Servers
    - Apple Mac OS (32-bit and 64-bit)
    - Managing all aspects of an Email Exchange Server.
- Implement multi-level security (MLS) architectures such as the DODIIS Trusted Workstation (DTW) or the Dell Integrity Secure Consolidated Client technology.
- Administer Microsoft operating systems including, but not limited to, Windows Server (2012, 2016), Windows OS (7, 8, 10 secure platform).
- Implement information Assurance and Information Condition (INFOCON) requirements.
- Design and configure a VM environment to support R&D and Production networks.
- Develop documentation for software evaluation, installation procedures, security policies, and user guides for several clients.
- Administer cloud architectures and configure cloud resources to support R&D and Production networks.
- Administer thick and thin client architectures.
- Implement, attain and test operating systems against DISA Security Technical Implementation Guidelines (STIG)
- Build and maintain IA security monitoring tools (i.e. WASSP, SCAP, ACAS, NESSUS, WUS, HBSS…).
- Define a network layout, protocols and bandwidth requirements to support DoD and IC R&D and operational requirements.
- Implement DoD and DNI information technology directives such as Navy's RMF and ICD 503 process.
- Engineer secured and hardened mission-critical systems for Comprehensive Network Defense.

System Administrator Level III-RHEL/Linux KEY

Position Requirements

Key Personnel:	Yes
Security Clearance:	Top Secret-SCI
Training & Certifications:	DoD 8570.01 IAT level II at the computing environment (CE)
Degree:	Bachelor's
Degree Field:	Computer Science, Information System Management, Cybersecurity Management or another technical field.
Experience:	4 years administering computer systems and securing them from cybersecurity threats to support R&D capabilities in development and production enclaves.

Responsibilities

- Collaborate with other Systems administrators to maintain computer systems, IAVAs compliance, and identify user security requirements.
- Support Research & Development and Production information systems.
- Work with a RHEL OS version 6.7, 6.9, 7.3 and 7.4 configurations within a VM environment.
- Use command line to support CentOS, Linux, SOLARIS, RHEL, and other Unix/Linux systems.
- Engineer systems administration-related solutions for various project and operational needs.
- Install and configure systems which support infrastructure and/or R&D activities.
- Contribute to and maintain security posture of systems in accordance with DISA Security Technical Implementation Guides, CTOs, and IAVM policies.
- Support physical server, workstations, thin clients, and virtual systems and environments.
- Perform account management and security management of Unix and Linux OS resources to include servers, workstations, tablets, and Smartphones (i.e. Android, Apple devices).
- Engineer secured and hardened mission-critical systems for Comprehensive Network Defense.
- Implement multi-level security (MLS) architectures such as the DODIIS Trusted Workstation (DTW) or the Dell Integrity Secure Consolidated Client technology.
- Define Information Assurance and Information Condition (INFOCON) requirements.
- Implement, attain, and test operating system DISA Security Technical Implementation Guidelines (STIG).
- Use security monitoring tools (i.e. WASP, SCAP, ACAS, HBSS…).
- Implement DoD and DNI information technology directives such as RMF and ICD 503.

Desired Qualifications

- 2 years of relevant work experience administering workstations and securing servers to protect against cyber security threats in a R&D enclave.

System Administrator Level III-RHEL/Linux

Position Requirements

Key Personnel:	No
Security Clearance:	Top Secret-SCI
Training & Certifications:	DoD 8570.01 IAT level II at the computing environment (CE)
Degree:	Bachelor's
Degree Field:	Computer Science, Information System Management, Cybersecurity Management or another technical field.
Experience:	4 years administering computer systems and securing them from cybersecurity threats to support R&D capabilities in development and production enclaves.

Responsibilities

- Collaborate with other Systems administrators to maintain computer systems, IAVAs compliance, and identify user security requirements.
- Support Research & Development and Production information systems.
- Work with a RHEL OS version 6.7, 6.9, 7.3 and 7.4 configurations within a VM environment.
- Use command line to support CentOS, Linux, SOLARIS, RHEL, and other Unix/Linux systems.
- Engineer systems administration-related solutions for various project and operational needs.
- Install and configure systems which support infrastructure and/or R&D activities.
- Contribute to and maintain security posture of systems in accordance with DISA Security Technical Implementation Guides, CTOs, and IAVM policies.
- Support physical server, workstations, thin clients, and virtual systems and environments.
- Perform account management and security management of Unix and Linux OS resources to include servers, workstations, tablets, and Smartphones (i.e. Android, Apple devices).
- Engineer secured and hardened mission-critical systems for Comprehensive Network Defense.
- Implement multi-level security (MLS) architectures such as the DODIIS Trusted Workstation (DTW) or the Dell Integrity Secure Consolidated Client technology.
- Define Information Assurance and Information Condition (INFOCON) requirements.
- Implement, attain, and test operating system DISA Security Technical Implementation Guidelines (STIG).
- Use security monitoring tools (i.e. WASP, SCAP, ACAS, HBSS…).
- Implement DoD and DNI information technology directives such as RMF and ICD 503.

System Administrator Level III-Windows

Position Requirements

Key Personnel:	No
Security Clearance:	Top Secret-SCI
Training & Certifications:	DoD 8570.01 IAT level II at the computing environment (CE)
Degree:	Bachelor's
Degree Field:	Computer Science, Information System Management, Cybersecurity Management or another technical field.
Experience:	2 years administering computer systems and securing them from cybersecurity threats to support R&D capabilities in development and production enclaves.

Responsibilities

- Collaborate with other Systems administrators to maintain computer systems, IAVAs compliance, and identify user security requirements.
- Support Research & Development information systems connected to Production information systems.
- Develop new cybersecurity risk mitigation plans and methods.
- Use multi-level security (MLS) architectures such as the DODIIS Trusted Workstation (DTW) or the Dell Integrity Secure Consolidated Client technology.
- Administer software used on the domain including, but not limited to:
    - Windows Server (2012, 2016)
    - Windows OS (Windows 7, Win 10 secure platform)
    - Good Mobile Control Server version 2.7.4.1115
    - BlackBerry Enterprise Mobile Server version 2.4.18.19
    - Samsung Mobile Servers
    - Apple Mac OS (32-bit and 64-bit)
- Address Information Assurance (IA) and Information Condition (INFOCON) requirements.
- Build and maintain IA security monitoring tools (i.e. WASSP, SCAP, ACAS, NESSUS, WUS, HBSS…).
- Design and configure a VM environment to support R&D and Production networks.
- Use cloud architectures and configure cloud resources to support R&D and Production networks.
- Satisfy DoD and DNI information technology directives such as Navy's RMF and ICD 503 process.
- Engineer secured and hardened mission-critical systems for Comprehensive Network Defense.
- Configure and test operating systems in accordance with the DISA Security Technical Implementation Guidelines (STIG).
- Build, maintain and configure hardware with encryption applications to satisfy data at rest security requirements
- Create, maintain, upgrade, manage, document, and decommission systems through ICD 503 and Navy RMF processes.

System Administrator Level V KEY

Position Requirements

Key Personnel:	Yes
Security Clearance:	Top Secret-SCI
Training & Certifications:	DoD 8570.01 IAM level II at the computing environment (CE)
Degree:	Bachelor's
Degree Field:	Computer Science, Information System Management, Cybersecurity Management or another technical field.
Experience:	8 years administering computer systems and securing computer systems from cybersecurity threats to support R&D capabilities in development and production enclaves.

Responsibilities

- Collaborate with other Systems administrators to maintain computer systems, IAVAs compliance, identify user security requirements, and manage Research & Development and Production networks.
- Engineer secured and hardened mission-critical systems for Comprehensive Network Defense.
- Define implementation strategy for technology information directives such as DoD Risk Management Framework (RMF) and Intelligence Community Directive (ICD) 503.
- Provide level III Information Assurance (IA) Cybersecurity risk management oversight and compliance monitoring.
- Use Enterprise Mission Assurance Support Service (eMASS) tool.
- Use ICD 503 (XACTA) tool.
- Monitor system daily and respond immediately to security or usability problems.
- Administer RHEL OS including versions 6.7, 6.9, 7.3, and 7.4 within a VM environment
- Use command line to administer CentOS and Linux systems.
- Support all aspects of an Active Directory network to include LAN, WAN, all remote connectivity, DNS, Firewall, SMTP gateways, Ethernet topologies, configuration management, report generation, and implementation.
- Design and configure a VM environment to support R&D and Production networks.
- Develop documentation for software evaluation, installation procedures, security policies, and user guides for several clients.
- Design and maintain SharePoint sites.
- Build virtual servers and workstations.
- Design, implement, maintain, upgrade, manage, document, and decommission cloud computing systems to support R&D and Production networks.
- Assess requirements and present systems design recommendations as well as industry best practices.
- Prepare detailed presentations/briefings to clearly explain the benefits of an architectural approach to clients and stakeholders.
- Coordinate the activities of others (internal staff, client staff, subcontractors, associates and staff from collaborating and/or competing suppliers) and manage stakeholder expectations and requirements.

Desired Qualifications

- 3 additional years of relevant work experience administering workstations and securing servers to protect against cyber security threats in a R&D enclave.

System Administration Specialist

Position Requirements

Key Personnel:	No
Security Clearance:	Top Secret-SCI
Training & Certifications:	DoD 8570.01 IAT level II at the computing environment (CE)
Degree:	Bachelors
Degree Field:	Computer Science, Information System Management, Cybersecurity Management or another technical field.
Experience:	4 years administering computer systems and securing them from cybersecurity threats to support R&D capabilities.

Responsibilities

- Collaborate with other Systems administrators to maintain computer systems.
- Support Research & Development information systems.
- Support all aspects of an Active Directory network including:
    - Create, change, and delete user accounts per request.
    - DNS, Firewall and SMTP gateways.
    - LAN, WAN and all remote connectivity
    - Ethernet Topology.
    - Configuration Management and Report Generation.
    - Implementing Global Policies.
    - Managing all aspects of an Email Exchange Server.
- Administer Microsoft operating systems including, but not limited to, Windows Server (2012, 2016, 2019), Windows OS (10 secure platform).
- Configure and maintain a VM environment to support R&D networks.
- Develop documentation for software evaluation, installation procedures, security policies, and user guides for several clients.
- Implement, attain and test operating systems against DISA Security Technical Implementation Guidelines (STIG)
- Build and maintain IA security monitoring tools (i.e. SCAP, ACAS, NESSUS, HBSS…).
- Research and recommend innovative, and where possible automated approaches for system administration tasks.
- Identify approaches that leverage resources and provide economies of scale.
- Perform daily system monitoring, verifying the integrity and availability of all hardware, server resources, systems and key processes, reviewing system and application logs, and verifying completion of scheduled jobs such as backups.
- Perform backup operations, ensuring all required file systems and system data are successfully backed up to the appropriate media, recovery tapes or disks are created, and media is recycled and sent off site as necessary.
- Perform system backups and recovery.

- Repair and recover from hardware or software failures.
- Perform configuration verification and vulnerability assessment scans using Tenable Assured Compliance Assessment Solution (ACAS) Management.
- Apply Operating System (OS) patches and upgrades on a regular basis, and upgrade administrative tools and utilities.
- Evaluate and install software patches.
- Configure / add new services as necessary.
- Perform ongoing performance tuning, hardware upgrades, and resource optimization as required.
- Configure CPU, memory, and disk partitions as required.
- Resolve software related problems.
- Build system configuration baselines that leverage the DISA Security Technical Implementation Guides (STIG) and the Security Content Automation Protocol (SCAP).
- Build, maintain and configure hardware with encryption applications to satisfy data at rest security requirements