Personnel Qualifications

Senior Systems Engineer

The Senior Systems Engineer position requires a Bachelor's degree in Cybersecurity, Information Systems, Information Technology, Computer Science, Computer Engineering, or equivalent experience. The position requires a minimum of fifteen (15) years of experience in hardware and software requirements analysis and system specification, including the implementation, configuration, and testing of the systems specified in the SOW.

The position requires demonstrated experience with switched Ethernet networking ports and protocols, including but not limited to IPv4 and IPv6, as well as configuring and maintaining clustered switching environments such as VSX. The position also requires experience in coordinating and implementing organizational compliance with DoN and DoD Information Security and Cyber Security requirements.

The position requires expertise in DoD Security Technical Implementation Guides (STIG) requirements and implementation. Familiarity with NRL STIG requirements is required. The position further requires demonstrated experience with DoD and DON security implementation tools, including ACAS, MDE, DISA STIG Viewer, and SCAP scanning.

The position requires hands-on experience with both desktop and server versions of Windows, along with Active Directory and DNS. The position requires experience configuring, implementing, managing, and monitoring Windows Server 2019–2025 environments, including all supported client protocols, as well as performing hardware and software troubleshooting and tuning. The position requires experience managing and maintaining Windows and Linux servers in virtualized environments using Hyper-V and VMware products.

The position requires experience with automated patch management for Microsoft systems, including WSUS, and demonstrated experience configuring, implementing, and managing a local certificate authority. MCSE certification is desired.

The position also requires experience with multiple Linux operating systems and administering computational cluster environments, including cluster management systems, Storage Area Networking (SAN), fibre channel, InfiniBand interconnection, batch scheduling, and cluster monitoring. Proficiency in PowerShell scripting is required.

Additionally, the position requires knowledge and experience with DoD CAC PKI and tools such as ActivClient, Centrify, and CAC Key.

Must be able to obtain a SECRET clearance.

Senior Information Technology Systems Engineer 1

The position requires a Bachelor's degree in Cybersecurity, Information Systems, Information Technology, Computer Science, Computer Engineering, or equivalent experience. The position requires a minimum of fifteen (15) years of experience in the design, implementation, and management of Windows, Mac OS, and Linux systems and servers specified in Section 3.4.1 of the SOW.

The position requires demonstrated experience in backup management, recovery planning, and recovery implementation for supported systems. The position requires experience troubleshooting system hardware and software, as well as demonstrated knowledge and support of switched Ethernet networking ports and protocols, including but not limited to IPv4 and IPv6.

The position requires experience supporting user software applications to include Jabber VOIP, Trelix anti-virus, AtHoc and Blackberry emergency alert client, Acrobat, VPN clients, Flank Speed, Office 365

& Teams, Windows Subsystem for Linux, Hyper-V and VMware virtual machines, along with various scientific applications and their licenses.

The position requires the ability to recommend, obtain quotes for, and install printers, scanners, computers, servers, and software necessary to meet mission requirements while following DoD guidelines. The position requires knowledge, understanding, and implementation of DoD STIGs and IAVAs for Windows systems/servers, Apple MacOS, Linux, and mobile devices.

The position requires knowledge and experience with DoD CAC PKI and tools such as ActivClient, Centrify, and CAC Key. The position requires experience performing daily general system administration tasks for Windows, Linux, and Mac computers including user support, installation, configuration, backups, patches, and upgrades, along with experience maintaining and updating databases, records, and logs for user accounts, hosts, and related information.

Must be able to obtain SECRET clearance.

Senior Information Technology Systems Engineer 2

The position requires a degree in Cybersecurity, Information Systems, Information Technology, Computer Science, Computer Engineering, or equivalent experience. The position requires a minimum of ten (10) years of experience in the design, implementation, and management of Windows, Mac OS, and Linux systems and servers specified in Section 3.4.2 of the SOW.

The position requires demonstrated experience in designing, installing, upgrading, and maintaining enterprise and command-level computer systems, as well as experience with IDL, network server management, RAID server management, and web server management. The position requires experience with configuration, administration, and troubleshooting of High Availability and high-speed networking and storage used for ground control of space-based assets.

The position requires demonstrated knowledge and support of switched Ethernet networking ports and protocols, including but not limited to IPv4 and IPv6. The position requires the ability to troubleshoot endpoint communication or application issues, along with demonstrated experience in backup management, recovery planning, and implementation for supported systems.

The position requires the ability to recommend, obtain quotes for, and install printers, scanners, computers, servers, and software necessary to meet mission requirements while complying with DoD guidelines.

The position requires hands-on experience with both desktop and server versions of Windows, along with Active Directory and DNS. Experience implementing Windows ADMX and GPO's within a Government networked environment is desired. Expert knowledge of NRL DMZ configuration, management, and ACL requirements for administering Windows and Linux public-facing web servers is highly desirable.

The position requires demonstrated expertise with DoD Security Technical Installation Guides (STIG) requirements and implementation, and familiarity with NRL STIG requirements is required. The position also requires experience responding to NCDOC cyber and security incident tickets using system administration expertise and familiarity with DON IT–specific tools such as POA&Ms, STIG Viewer, ACAS, HP WebInspect, and Acunetix.

The position requires knowledge and experience with DoD CAC PKI and tools such as ActivClient, Centrify, and CAC Key. The position requires experience performing daily system administration tasks,

including user support, installation, configuration, backups, patches, and upgrades, as well as maintaining and updating databases, records, and logs for user accounts, hosts, and related information.

Must be able to obtain a SECRET clearance.

Senior Information Technology Systems Engineer 3

The position requires a Bachelor's degree in Cybersecurity, Information Systems, Information Technology, Computer Science, Computer Engineering, or equivalent experience. The position requires a minimum of fifteen (15) years of experience in the design, implementation, and management of Windows, Mac OS, and Linux systems and servers specified in Section 3.4.3 of the SOW.

The position requires demonstrated experience in designing, installing, upgrading, and maintaining enterprise and command-level computer systems, as well as experience with IDL, network server management, RAID server management, and web server management. The position requires experience with configuration, administration, and troubleshooting of Windows Server (Domain/Clustered), Linux (Multiple Environments), MacOS, and Sun Solaris operating systems used for ground control of space-based assets.

The position requires demonstrated knowledge and support of switched Ethernet networking ports and protocols, including but not limited to IPv4 and IPv6. The position requires the ability to troubleshoot system hardware and software, along with demonstrated experience in backup management, recovery planning, and implementation for supported systems.

The position requires the ability to recommend, obtain quotes for, and install printers, scanners, computers, servers, and software necessary to meet mission requirements while complying with DoD guidelines. Expert knowledge of NRL DMZ configuration, management, and ACL requirements for administering Linux public-facing web servers is highly desirable.

The position requires demonstrated expertise with DoD Security Technical Installation Guides (STIG) requirements and implementation, and familiarity with NRL STIG requirements is required. The position also requires experience responding to NCDOC cyber and security incident tickets using system administration expertise and familiarity with DON IT–specific tools such as POA&Ms, STIG Viewer, ACAS, HP WebInspect, and Acunetix.

The position requires proficiency with Hyper-V Clustering, Windows GPO/ADMX, and third-party licensing applications (Flexera, Ansys), installation and configuration of scientific and engineering tools (IDL, Matlab, Anaconda, Python, and others), knowledge and experience with DoD CAC PKI and tools such as ActivClient, Centrify, and CAC Key. The position requires experience performing daily system administration tasks, including user support, installation, configuration, backups, patches, and upgrades, as well as maintaining and updating databases, records, and logs for user accounts, hosts, and related information.

Must be able to obtain a SECRET clearance.

Senior Systems Engineer / Database Administrator

The Senior Systems Engineer/Database Administrator position requires a Bachelor's degree in Cybersecurity, Information Systems, Information Technology, Computer Science, Computer Engineering, or equivalent experience. The position requires a minimum of fifteen (15) years of experience in Oracle database administration, along with general experience working with the technologies described in section 3.3 of the SOW.

The position requires demonstrated experience with client/server and web-based development; Oracle database administration; and a broad range of application and operating system software packages, including Oracle 12C and 19C, Oracle Forms & Reports, Webutil, PL/SQL, SQL*Plus, HTML, XML, PHP, Perl, Shell scripting, and SQL Developer. The position also requires demonstrated experience in software engineering, integration, and configuration management; familiarity with Work Breakdown Structure (WBS) concepts and their relationship to database information structures; and experience in STIG/IAVA compliance. Strong interpersonal, communication, and analytical skills are required.

The position requires demonstrated experience performing Oracle database management tasks, including database infrastructure design, automation of data loads, performance tuning, SQL programming, space management, backup and recovery, and version control. The position requires expertise with DoD Security Technical Installation Guides (STIG) requirements and implementation. Familiarity with NRL STIG requirements is desirable.

The position requires experience providing user support; tuning and troubleshooting data access applications and ad hoc queries; working with database technology vendors to implement new technologies; creating technical designs; implementing procedures; and training users to achieve operational efficiency.

The position requires the ability to rapidly adapt software development activities to meet division needs as new project starts occur, including development of new forms, reports, and databases to support project and reporting requirements.

Must be able to obtain a SECRET clearance.

Systems Engineer / Database Administrator

The Systems Engineer/Database Administrator position requires a Bachelor's degree in Cybersecurity, Information Systems, Information Technology, Computer Science, Computer Engineering, or equivalent experience. The position requires a minimum of three (3) years of software/systems engineering experience related to the technologies described in section 3.3 of the SOW.

The position requires demonstrated experience with client/server and web-based development, Oracle database administration, and application and operating system software packages such as Oracle 12C and 19C, Fusion, MOD PL/SQL, OID, LDAP, Linux, Oracle Designer, Discoverer, Developer, and Oracle Forms and Reports. The position also requires demonstrated experience in software engineering, integration, and configuration management, as well as familiarity with Work Breakdown Structure (WBS) concepts and their relationship to database information structures.

The position requires experience providing user support in Windows, Linux, and/or Mac OS X environments, along with experience tuning and troubleshooting data access applications.

Must be able to obtain a SECRET clearance.