

Computer Systems Security Officer: Computer Systems Security Officer II

Designs, tests, and implements state-of-the-art secure operating systems, networks, and database products. Conducts risk assessment, and provides recommendations for application design. Involved in a wide range of security issues including architectures, firewalls, electronic data traffic, and network access. Uses encryption technology, penetration and vulnerability analysis of various security technologies, and information technology security research. May prepare security reports to regulatory agencies. Provides information security certification and accreditation support for all applications, systems and networks in accordance with appropriate policies and requirements. Drafts accreditation support documentation. Reviews and implements security policies and procedures. Coordinates hardware and software purchases, movement into and out of classified areas, and customer approvals. Safeguards the network against unauthorized infiltration, modification, destruction or disclosure. Conducts virus incident response and clean up. Performs system analysis and vulnerability studies. Develops, tests, and operates firewalls, intrusion detection systems, enterprise anti-virus systems and software deployment tools. Provides information security certification and accreditation support for all applications, systems and networks in accordance with appropriate policies and requirements. Drafts accreditation support documentation. Reviews and implements security policies and procedures. Coordinates hardware and software purchases, movement into and out of classified areas, and customer approvals. Safeguards the network against unauthorized infiltration, modification, destruction or disclosure. Conducts virus incident response and clean up. Performs system analysis and vulnerability studies. Develops, tests, and operates firewalls, intrusion detection systems, enterprise anti-virus systems and software deployment tools. Serves as Information Systems Security Manager (ISSM) for one or more classified programs. Performs security tasks required by the National Industrial Security Operating Manual (NISPO) and Director of Central Intelligence Directives (DCID's) for the administration and safeguarding of U.S. and foreign government classified information as it pertains to classified networks, standalone computer systems, and data encryption. Provides analysis, design, specifications, procedures, software or other technical support to the Security Department on classified networks, standalone computer systems, and data encryption. Implements and ensures compliance with applicable laws, Government regulations, customer requirements and company policies.

Knowledge

Extensive knowledge of United States Government security rules and regulations, including Department of Defense, Department of Energy, and the Intelligence Community in regard to classified Information systems. Extensive knowledge of VC's security policies and procedures.

Problem Solving

Develops solutions to a variety of problems of moderate scope and complexity. Refers to policies and practices for guidance.

Discretion/Latitude

Works under general supervision. Follows established procedures. Work is reviewed for soundness of judgment, overall adequacy and accuracy.

Impact

Contributes to the completion of milestones associated with specific projects. Failure to achieve results and/or erroneous decisions or recommendations may cause delays in program schedules and may result in the allocation of additional resources. Failure to satisfactorily perform this job may result in the loss of government contracts involving classified materials or the loss of ability to use Information Systems for classified use.

Liaison

Internal contact with all employees and levels of management. Externally deals with government security inspectors, representatives, and visitors. Represents organization or location as the prime security contact. Interacts with senior internal and external personnel on significant matters often requiring coordination between organizations and headquarter's security personnel.

Education and Experience

5+ years of directly related experience with Bachelor's Degree in Computer Science, Applications or Business Administration. Professional Certification Required.