

Position Description

PD#: D2178000

Replaces PD#: D1849000

Sequence#:

**IT SPECIALIST (INFOSEC)
GS-2210-11**

Servicing CA: NGB

Agency: NGB

Directorate: A6

Cmd Code: ANG WING

Org: BASE COM UNIT

Citation 1: USOPM OPM JOB FAMILY PCS FOR ADMINISTRATIVE WORK IN THE INFORMATION TECHNOLOGY GROUP, GS-2200, INFORMATION TECHNOLOGY MANAGEMENT, GS-2210, DATED MAY 2001.

Citation 2: USOPM PCS FOR TELECOMMUNICATIONS SERIES GS-0391, DATED MAY 2001.

Classified By: Charda Bright HR SPEC. (CLASS)
Pen & Ink Changes

FLSA: EXEMPT

Drug Test Required: VARIES

DCIPS PD: NO

Career Program:
VARIES

**Financial Disclosure
Required:** NO

Acquisition Position: NO

Functional Code:

Requires Access to Firearms:
VARIES

Interdisciplinary: NO

Competitive Area:
VARIES

Position Sensitivity: VARIES

Security Access: VARIES

Competitive Level:
VARIES

Target Grade/FPL: 11

Career Ladder PD: NO

Emergency Essential:

Bus Code: VARIES

Personnel Reliability Position:
VARIES

[]

**Information
Assurance:** N

Influenza Vaccination: NO

PD Status: VERIFIED

Position Duties: See Attached

INTRODUCTION:

This position is located in the Plans and Resources Flight of a Base Communications Squadron. The purpose of this position is to serve as the Base Information Assurance Manager who is the wing commander's authority and focal point for Information Assurance. Manages the communication-computer security (COMPUSEC) program, Electronic Key Management System (EKMS), Emission Security, and Information Assurance Awareness Programs.

MAJOR DUTIES:

1. Serves as the Wing Information Assurance Manager. Applies Information Technology (IT) security principles, methods, and security products to protect and maintain the availability, integrity, confidentiality, and accountability of information system resources and information processed throughout the system's life cycle. Establishes and publishes base-wide policy to manage the INFOSEC (also known as COMPUSEC) program and provides advice and guidance in its implementation and in procedures used in the development and operation of systems. Assists all base organizations in the development of their individual INFOSEC program. Disseminates information and ensures computer security practices are adhered to by all functional areas. Reviews, analyzes, and validates certification and accreditation (C&A) packages. Continuously identifies and analyzes threats and vulnerabilities to the information systems to maintain an appropriate level of protection. Ensures computer software designs address information system security requirements. Accomplishes risk analysis, security testing, and certification due to modifications or changes to computer systems. Evaluates, assesses, or locally tests and approves all hardware, software, and firmware products that provide security features prior to use on any accredited information system or network. Certifies all software prior to installation and use on communications and computer systems. Executes computer security plans and enforces mandatory access control techniques such as trusted routers, bastion hosts, gateways, firewalls, or other methods of information systems protection.
2. Manages the Network Security Program. Maintains required information assurance certification IAW DoD 8570.01-M, Federal Information Security Management Act of 2002, Clinger Cohen Act of 1996. Implements and advises on IT security policies and procedures to ensure protection of information transmitted to the installation, among organizations on the installation, and from the installation using Local Area Networks (LAN), Wide Area Networks (WAN), the World Wide Web, or other communications modes. Utilizes current and future multi-level security products collectively to provide data integrity, confidentiality, authentication, non-repudiation, and access control of the LAN. Reports to MAJCOM, Air Force Communications Agency, National Security Agency, and Air Force Computer Emergency Response Team all incidents involving viruses, tampering, or unauthorized system entry. Controls access to prevent unauthorized persons from using network facilities. Limits access to privileged programs (i.e., operating system, system parameter and configuration files, and databases), utilities, and security-relevant programs/data files to authorized personnel. Implements methods to prevent or minimize direct access, electronic or other forms of eavesdropping, interpreting electro-mechanical emanations, electronic intercept, telemetry interpretation, and other techniques designed to gain unauthorized access to IT

information, equipment, or processes. Evaluates unusual circumstances to recognize and define potential vulnerabilities and selects and oversees the installation of physical and technical security barriers to prevent others from improperly obtaining such information. Conducts the Information Assurance Awareness Program which uses computer-based training for both initial and recurring information protection training. Maintains required course records.

3. Serves as the Communications Security (COMSEC) Manager for all cryptographic activities including managing the Cryptographic Access Program (CAP). Formulates and develops communications security criteria and requirements for inclusion in mobility, contingency, and exercise plans. Maintains accountability for sensitive cryptographic materials and related COMSEC information. Oversees issuance of COMSEC materials. Maintains COMSEC inventory. Prepares and evaluates written plans for emergency actions and ensures personnel are fully qualified in the execution of plans. Investigates COMSEC security incidents to determine the possibility of compromise to COMSEC materials and ensures documentation and reporting to appropriate channels. Performs destruction, receiving, issuing transferring and inspecting COMSEC material within the most stringent timelines. Furnishes written guidance to user accounts concurring effective dates, accounting procedures, destruction requirements, and physical security of COMSEC materials including key. Performs semi-annual functional reviews of all COMSEC user accounts, physically inspecting the user's COMSEC facilities, reviewing procedures, and audit of all cryptographic holdings. Manages the Certification Authority Workstation. Manages the CAP by conducting briefings prior to granting access to cryptographic information. Documents cryptographic access certificates and acts as liaison for scheduling polygraph examinations of personnel enrolled in the program.

4. Implements and manages the Electronic Key Management System (EKMS) program. This includes system configuration and operation of the Local Management Device, Data Transfer Device, and Key Processor. Initializes the system, performs system backups, determines operator access, and control functions (privilege management), reloads and configures the operating system's parameters. Installs or oversees installation of local COMSEC account hardware and software, including training alternates in the AFEKMS operations. Serves as secure voice equipment (e.g., STE, secure VoIP) user Representative and Emissions Security Program Manager. Develops, implements, and monitors security systems for the protection of controlled cryptographic cards, documents, ciphers, devices, communications centers, and equipment.

5. Adheres to management control plan requirements by conducting self inspection and staff assistance visits. Resolves identified discrepancies.

6. Performs other duties as assigned.

FES Factor Evaluation:

FACTOR 1 - KNOWLEDGE REQUIRED BY THE POSITIONS FL 1-7, 1250 PTS

-- Knowledge of a full range of IT security principles, methods, regulations, policies, products and services sufficient to develop specifications to ensure compliance with security requirements at the LAN level and to plan and coordinate the delivery of an IT security awareness training program for end users at all levels at the installation.

-- Knowledge of a full range of IT security requirements for certification and accreditation; network operations and protocols; systems testing and evaluation; and performance management methods sufficient to implement and coordinate activities designed to ensure, protect, and restore IT systems, services, and capabilities; to monitor and evaluate systems compliance with IT security requirements; provide advice and guidance in implementing IT security policies and procedures in the development and operation of network systems; to plan and conduct security accreditation reviews for installed systems or networks; and to recommend new or revised security measures and countermeasures based on the results of accreditation reviews.

-- Knowledge of a wide range of IT and communication computer security techniques, requirements, methods, sources, and procedures in INFOSEC, EKMS, EMSEC, and secure voice (e.g., STE, Secure VoIP) Automated Software security.

-- Knowledge of the EKMS program and related hardware and software, including knowledge of operating systems, local COMSEC Management Software, relational data base management systems, computer-communications software.

-- Knowledge of a broad range of telecommunications equipment, operating techniques, concepts, principles, practices, requirements, methods, sources, and procedures (including familiarity with approaches used by telecommunications organizations in other agencies and/or the private sector) sufficient to manage the Communications Security (COMSEC) program, and the Cryptographic Access Program to interpret policy originating from higher organizational levels and to analyze and resolve difficult and complex telecommunications security problems where telecommunications knowledge is paramount.

-- Knowledge of system software and systems development life cycles including systems documentation, design development, configuration management, cost analysis, data administration, systems integration, and testing.

-- Knowledge of IT security requirements sufficient to develop and evaluate program documentation to include: mission needs statements, operational requirements documents and support plans, specifications, and proposals.

-- Skill to develop and evaluate program documentation to include mission needs statements, operational requirements documents and support plans, specifications, proposals, and plans for systems operational test and evaluation of communications and information security systems.

-- Ability to serve as the focal point for information security, providing authoritative advice and assistance on complex, technical, controversial, and precedent setting matters to improve the IT security program comprising many unique organizations and large, complex computer and communications security systems.

-- Ability to apply sound judgment in the use of security knowledge and in weighing the impact of variables such as granting access to classified keying material and other issues that influence the course of actions taken in resolving security questions or issues.

-- Ability to apply policies, principles, and IT security concepts sufficient to carry out activities leading to security C&A.

-- Ability to apply findings of assessments to mitigate IT security risks through the implementation of corrective actions.

FACTOR 2 SUPERVISORY CONTROLS FL 2-4, 450 PTS

The supervisor, in consultation with the specialist, makes assignments, determines overall priorities, and sets time frames for completion. The incumbent independently plans and carries out projects and analyses of the organization's requirements, coordinates with other security specialists and National Guard Bureau headquarters. The incumbent, having developed expertise in different areas of security (i.e., computer, communications, emissions, secure voice, etc.) is independently responsible for planning and carrying out the work, resolving most of the complex, controversial, or unprecedented issues or conflicts that arise, applying and interpreting policy on own initiative in terms of established objectives. The supervisor is kept informed of progress, potentially controversial matters or unusual conditions with far-reaching implications, such as security violations. Supervisor reviews completed work for soundness of overall approach, adherence to requirements, effectiveness in meeting requirements and feasibility of recommendations.

FACTOR 3 GUIDELINES FL 3-3, 275 PTS.

Guidelines consist of National Guard Bureau, Air National Guard, Air Force, National Security Agency, Air Force Intelligence Agency, Air Force Cryptological Support Center, numerous DOD manuals, MAJCOM supplements, training manuals, technical software manuals, and manufacturer's manuals/instructions. Guidelines are extensive, generally specific, but are not always directly applicable to the problem and may have gaps in specificity. Incumbent is responsible for determining applicability, adapt as necessary, and research additional options. The incumbent is relied upon to select the appropriate techniques for accomplishing required tasks and interpreting regulation and policy documents to meet objectives.

FACTOR 4 COMPLEXITY FL 4-4, 225 PTS

The position deals with a variety of IT and communication-computer security duties requiring the application of different and unrelated procedures pertinent to the IT field. Analyzing threats and vulnerabilities to the information systems protection function involves consideration of plans, applicable policies, regulations, procedures, unusual circumstances and alternative methods of implementing and monitoring security requirements. Evaluates and implements new network security technologies and anticipates the need for changes to preclude compromise of information. Recommendations or actions must weigh needs and objectives and be selected from many alternatives. Uses judgment to interpret data and evaluate possible means of providing required information assurance through electronic, physical, digital, fiber, software, or procedural means that are available or proposed.

FACTOR 5 SCOPE AND EFFECT FL 5-3, 150 PTS

The work involves resolving a variety of IT systems security problems, capabilities, and situations. The incumbent installs, implements, and maintains protective programs and is responsible for managing and directing communications-computer systems security programs, conducting independent reviews, and recommending corrective actions which follow established methods, techniques, and procedures. The work affects the adequacy of such activities as computer security investigations, internal operations, or computer system change conclusions and contributes to the protection of the infrastructure from unauthorized access and contributes to the integrity and availability of systems and networks.

FACTOR 6 PERSONAL CONTACTS &
FACTOR 7 PURPOSE OF CONTACTS FL 3B, 110 PTS

Personal contacts include other IT security specialists, telecommunications specialists, programmers, system/database administrators, network/LAN administrators, and functional area users in other organizations outside of the immediate organization. Contacts also include individuals or groups from outside the agency including consultants, contractors, vendors, representatives of professional organizations, and management officials from higher headquarters. Such contacts are often on an ad hoc basis with the incumbent having to determine the role and authority of participants as meetings progress. Serves as the liaison between base level customers and MAJCOM Information Protection Office.

The purpose is to plan, coordinate, advise on work efforts, or to resolve security related problems by influencing or motivating individuals or groups who are working toward mutual goals and who have basically cooperative attitudes. The incumbent must use persuasion to convince management to accept recommendations for solving security problems.

FACTOR 8 PHYSICAL DEMANDS FL 8-1, 5

The work is mostly sedentary involving some walking, standing, and carrying of light items. The work does not require any special physical effort.

FACTOR 9 WORK ENVIRONMENT FL 9-1, 5

The work is performed in a typical office setting with adequate lighting, heating and ventilation. Work environment involves everyday risks. Special safety precautions are not required.

OTHER SIGNIFICANT FACTS:

Maintains required information assurance certification IAW DoD 8570.01-M, Federal Information Security Management Act of 2002, Clinger Cohen Act of 1996, and current AF directives.

Conducts travel to and from offsite worksite(s) from the normal work area to perform assigned duties. This may include Operating Locations (OL) and/or Geographically Separated Units (GSU). Due to distances involved, travel may involve one or more overnight stays.

NGB QUALIFICATIONS:

To qualify for the National Guard Dual Status 2210, GS-11, the incumbent must have at least 36 months experience, education, or training using a number of alternative approaches, techniques and requirements appropriate to an assigned computer applications area or computer specialty area in an organization. Experience planning the sequence of actions necessary to accomplish the assignment involving coordination with others outside the organizational unit and development of project controls. Experience that required adaptations of guidelines or precedents to meet the needs of the assignment. Experience preparing documentation on cost/benefit studies where it involved summarizing the material and organizing it in a logical fashion.

Total Points: 2470

Range : 2355-2750 = GS-11

Final Classification: IT Specialist (INFOSEC), GS-2210-11