

Description - Final

PD #:

Replaces PD #:

Sequence #:

IT Specialist (INFOSEC/PLCYPLN)

GS-2210-13

Installation:

Major Command:

Region:

Citation 1: OPM, JFPCS Administrative Work in the Information Technology Group, GS-2200, dtd. May 2001 (Series Coverage, GS-2210)

PD Library PD:

COREDOC PD:

Classified By:

Classified Date:

FLSA:

Drug Test Required:

CIPMS PD:

Career Program:

Financial Disclosure Required:

Acquisition Position:

Functional Code:

Requires Access to Firearms:

Interdisciplinary:

Competitive Area:

Position Sensitivity:

Target Grade/FPL:

Competitive Level:

Emergency Essential:

Career Ladder PD:

PD Status:

MAJOR DUTIES

Summary: Serves as the technical expert/authority and project manager responsible for serving as the Division-wide (Division HQ and its subordinate districts) Information Assurance Manager (IAM) and for Division-wide IT policy and planning. The IAM plans, designs, develops, implements, and manages Information Assurance (IA) programs that meet current and future business requirements; designed to anticipate, assess, and minimize system vulnerabilities; and ensures the confidentiality, integrity, and availability of automated systems, networks and data/information systems. Administers and monitors compliance of programs which addresses IA operations and readiness. As the Division-wide technical authority accomplishes technical, analytical, and advisory functions pertinent to the development of Division-wide policies, plans, and processes covering the Division-wide IT program and ensuring the IT program is in compliance with higher authority policies and guidelines. Represents the Division on management reviews and assistance visits at subordinate districts regarding IA and policy and planning issues. Also ensures the rigorous application of information security/information assurance policies, principles, and practices in the delivery of all IT services involving planning

and management services. Typically, the incumbent:

1. Serves as the Division's IAM exercising overall responsibility and staff direction, operational coordination and review over the development, modification, and application of IA system issues of subordinate districts within the Division, and for the IA Program covering: security management, software, hardware, procedural, network, internet, data communications, and Automated Information Systems (AIS) media security. Manages all aspects of IA and the development, implementation, interpretation, accreditation, risk management, and maintenance of detailed IA policies, plans, programs, standards, and criteria ensuring a successful IA program. Plans, develops, implements, and manages Division-wide programs, policies, and procedures to protect the integrity and confidentiality of IT automated systems, networks, and data. Automation resources/functions covered by these programs include: micro and mini computers, peripheral equipment data and programs; remote access and output equipment to U.S. Army Corps of Engineers (USACE) regional mainframe computers; multi-user data bases covering administrative as well as technical functions and work programs; and training and educating personnel on information systems security practices.

a. Serves as a project manager, leads Division-wide efforts to develop long-range plans for IT security systems; design and implement security programs/projects designed to anticipate, identify, assess, and minimize system vulnerabilities (e.g., intrusion detection, access authentication programs, etc.); identify need for changes based on advanced/proposed new security technologies, new systems, networks, and software designs for potential security risks/threats. Reviews/resolves integration information systems security with other security disciplines, and new/advanced systems within the existing infrastructures and across platforms. Defines the scope and level of detail for Division-wide security plans and policies applicable to the security program.

b. Ensures that IT automated system design and developments, involving both in-house and contractual efforts, comply with Department of Defense (DoD) and Army IA requirements and leads others in system changes and modifications to ensure the development of related system security policies and measures. Develops systems security contingency plans and data recovery procedures. Coordinates IA for database design, development, and maintenance of all automated data systems. Develops, coordinates, and maintains Division-wide Department of Defense Information Technology Security Certification and Accreditation Program (DITSCAP); prepares or oversees the preparation of accreditation documentation and reviews and evaluates accreditation input furnished Division wide by IT specialists. Maintains current AIS accreditation statements and initiates re-accreditation when security-impacting changes have occurred.

c. Ensures that Division-wide information technology systems are operated and managed according to higher authority regulations, that users have the required security clearances, authorizations, and need to know, and that personnel associated with IT systems are provided and updated with the latest security awareness and requirements training. Conducts threat and vulnerability assessments and reports threats and technical vulnerabilities, identifies and assesses risks, and determines and implements effective measures to minimize such risks. Identifies, analyzes, and reports attempts to gain unauthorized access to information, system failures, or

suspected defects which could lead to unauthorized disclosures. Reports and advises personnel Division wide on actual or potential computer virus threats. Implements procedures for issuing, protecting, and changing system passwords. Develops procedures to generate and maintain required documentation and reporting. Manages the review of system audit trails and ensures the thorough investigation of discrepancies. Develops and establishes access control policies covering access to systems only by authorized personnel.

d. Provides advice and guidance pertinent to IA program policies, guides, and standard operating procedures (SOPs) during all stages of the automation process. Enforces security policies and safeguards for Division-wide systems including stopping system operation if warranted by the seriousness of security violations. Develops IT security plans, policy guidance, regulations, and procedures (SOPs) to ensure IA regulatory requirements are followed. Provides oversight for IA programs ensuring compliance with overall Division-wide plans and higher authority policies and guidance. Conducts and leads various IA security meetings with Division organizational elements and IT representatives of districts to plan, evaluate, and determine appropriate measures needed to ensure security requirements are met. Coordinates security actions with the Division Security and Law Enforcement staff.

2. Serves as the technical expert/authority, and advisor concerning Division-wide development, implementation, modification, and management of long- and short-range IT planning and development of Division-wide IT goals, objectives, policies, and priorities. Exercises staff direction, operational coordination and review regarding IT policy and planning issues of subordinate districts within the Division. Develops, implements, and ensures compliance with plans, policies, standards, infrastructure, and architecture of IT management and IT programs.

a. Integrates organizational input and documentation in developing a Division-wide IT plans and revises and manages such plans as required including involvement with both long- and short-range aspects of such plans. Provides oversight, guidance, and advisory services to all IT specialists concerning unplanned and/or non-programmed needs. Ensures all IT initiatives are created and maintained in a Division-wide IT Investment Portfolio System (ITIPS). Provides management advisory services and liaison to all Division-wide organizational levels pertinent to emerging and future advances in information technology.

b. Serves as a project manager/team leader in efforts to expand existing IT infrastructure, evaluate needs, and activate automation improvements and enhancements, and for information system planning and implementation studies. Analyzes program development and conducts Division-wide studies to evaluate and determine IT requirements. Conducts pre-study briefings of Division/District organizational elements being studied in-house and through contract. Evaluates data and develops study findings, conclusions, and recommendations. Conducts post-implementation studies to determine impacts of policies, automation, and utilization. Closely coordinates with higher headquarters to ensure agency compatibility and to recommend priorities

for systems development and implementation. Integrates architectures and changes resulting from studies and develops proposals for resulting systems developments.

c. Accomplishes Division-wide IT policy development. Ensures compliance with plans, policies, standards, infrastructures, and architectures of IT management and IT programs. Develops recommendations for the Director of Information Management (DIM) concerning Division-wide IM goals, objectives, policies, and priorities. Monitors IT activities to measure progress in achieving objectives. Interprets general higher authority policies and guidance pertinent to IT acquisition, management implementation, and disposal. Implements Division-wide IT-prescribed internal controls and supplements them to accommodate unique situations/operations. Provides technical expertise in contracting automated data system design and development. Develops IT plans, workload, workforce, and budget requirements. Initiates briefings, summaries, and correspondence Division-wide concerning IT budget formulation and execution matters. Develops and manages the portion of the ITIP database pertinent to the management, justification, and acquisition of Division-wide IT. Develops procedures to generate and maintain required documentation and reporting. Initiates workshops, meetings, and seminars to provide advisory services, guidance, and training concerning the intent and direction of the Division-wide program.

Performs other duties as assigned.

FACTOR 1. KNOWLEDGE REQUIRED BY THE POSITION LEVEL 1-8 1550 POINTS

A mastery of and skill in applying advanced information technology security and policy and planning principles, concepts, methods, standards, etc., sufficient to provide expert technical advice, guidance, and recommendations to Division-wide management and IT specialists on critical IT issues, and IT development applications to previously unsolvable IT problems. Leads projects associated with interrelationships of multiple IT specialties, Corps of Engineers IT architecture and integration/interoperability issues.

A mastery of and skill in project management principles, methods/techniques, etc., needed in developing plans, scheduling, estimating resources required; defining milestones and deliverables; monitoring, evaluating and reporting on activities/accomplishments; leads efforts to Division-wide IT security/policy and planning system development projects from design to support (e.g., Division-wide enterprise IT modernization plans; IT architecture and capital investment planning; Division-wide long-range IT security systems plans; integration of security programs across disciplines, etc.), and evaluation of the effectiveness of installed systems and services.

A Mastery of the IT infrastructure, functions, work processes/programs of Division-wide organizations, as well as an expert analytical ability to gather, assemble, and analyze facts, draw conclusions and devise solutions to problems which will increase the effectiveness of Division-wide IT programs, and identifying emerging security/policy and planning technology and their applications to Division-wide business processes. Mastery of and experience in the use of oral and written communication methods and techniques to accomplish continuing coordination with Division-wide IT program managers/customers, etc., and preparing and presenting briefings to

USACE, Division, District senior management officials on complex IT issues.

FACTOR 2. SUPERVISORY CONTROLS

FL 2-4 450 POINTS

Supervisor assigns functional responsibilities, an outline of overall objectives to be achieved, and the resources available for use. Assignments may come directly from the user/customer or from the supervisor and the incumbent has continuing responsibility for assignments pertaining to the Division IT security process, program, and requirements, and IT planning and policy matters. Consults with the supervisor on matters pertaining to time frames, scopes of assignments, stages of the work or application process and possible approaches on controversial or problematic situations. Independently applies and interprets guidelines and regulations and plans, analyzes and organizes projects associated with assignments. There is a continuing requirement for coordination (users and Division-wide IT specialists), and the incumbent independently plans and carries out the necessary coordination including that involving lower-level IT specialists and/or efforts of contract-employed persons. Is the highest level of expertise within the Division concerning the above-identified assignments and independently provides advice and guidance Division-wide and resolves problem matters. Completed work is typically accepted without technical change but is reviewed for effectiveness in meeting user requirements, conformance with policy, accomplishment within acceptable time frames, and customer satisfaction.

FACTOR 3. GUIDELINES

FL 3-4

450 POINTS

Guidelines include agency regulations, manuals, and policies which provide overall goals and define limitations and overall objectives; USACE regulations, policies and procedures concerning IT security and planning and all automated systems used in USACE; Division regulations and guidelines; and a variety of manufacturers' manuals and handbooks pertaining to the wide range of hardware and software in use Division wide. Guides are broad and frequently require interpretations and deviation from previously-used methods. The incumbent must use, on a regular basis, ingenuity in adapting existing methods and developing new methods and approaches to resolve automation security problems, planning, and policy requirements within the provisions of policies and regulations. The incumbent must interpret higher authority guidelines, considering the intricacies and problems encountered in the conduct of Division automation processes, and develop Division-wide guides, SOPs, bulletins, and fact sheets for distribution and use Division wide concerning a myriad of the automation functions and processes. The incumbent must apply judgment to anticipate problems, research trends in state-of-the-art technology, and develop special adaptations to satisfy requirements.

FACTOR 4. COMPLEXITY

FI 4-5 325 POINTS

Assignments involve accomplishing overall IT security requirements as well as policy and planning processes Division wide. Work requires in-depth analysis, study, and consideration of a myriad of complex automation/data management factors and many different and unrelated processes and methods. There is a continuous requirement in this job for coordination both in

the security and the policy and planning arenas. Additionally, work includes the responsibility for serving as the Division-wide technical expert/authority concerning IT security, policy and planning needs and problem resolution. Work is made complex by the continually changing Division business requirements and the rapidly changing IT environment. The incumbent must remain updated on changes, the most recent developments in IT, IT security technology, and continuously evaluate changing future organization data needs. The incumbent must develop management strategies, master plans, and implementation plans; continuously evaluate the effectiveness of current policies and ways of doing business; and develop methods and techniques for accommodation of customer IT system needs and security requirements. Projects require the consideration of state-of-the-art technology as well as numerous USACE-wide standard systems and hardware platforms requiring the use of a variety of techniques and methods to design and evaluate alternatives to best-fit Division-wide requirements.

FACTOR 5. SCOPE AND EFFECT

FL 5-4 225 POINTS

The work of this position involves the responsibility for all Information Security planning, measures, modifications, and administration Division wide and the full range of IT policy and planning requirements pertinent to Division-wide IT infrastructure. Work covers computer hardware, software, and a myriad of system interfaces, data management, system analysis, networks, Internet, and system administration. Information Security involves isolation and definition of problems, selecting, installing, and monitoring the performance of appropriate security tools; developing methods, procedures, guides, and policies for application; developing tools including firewalls, intrusion detection systems, and vulnerability self-assessment programs; and troubleshooting IT security problems that impact the availability of internet/intranet applications and recommending and implementing actions that will minimize risks. Policy and planning functions include reviewing or modifying IT program plans and policies to ensure the application, modification, and acquisition of the most cost-effective automation hardware, software, and systems to facilitate and respond to Division-wide business processes.

The IT security work impacts the continuing accessibility and availability of a variety of mission-critical applications and the continuing protection of Division-wide IT assets through the administration of effective IT security programs. Policy and planning work impacts the Division's ability to effectively incorporate IT in meeting its core business requirements and the effectiveness of plans and policies that are guides for the successful and effective application of IT to the Division's overall mission.

FACTOR 6. PERSONAL CONTACTS

FLs 6-3 & 7-C

180 POINTS

FACTOR 7. PURPOSE OF CONTACTS

Contacts are with IT managers and specialists within the employing organization, other Divisions, subordinate districts, contractor management, and other IT expert specialists, users Division wide. Contacts regularly include meetings with contractors, equipment manufacturers'

representatives, software providers related to advanced technological developments applicable to on-going/future projects. Contacts are also with information managers and specialists at USACE level and functional proponents of major Corps corporate systems, and occasional contacts with specialists and managers of IT at DA- and other Federal agency-level in moderately unstructured settings. Level 3

Contacts are to exchange information, determine IT system and security requirements, coordinate study work processes and problem resolution matters, plan study processes, and provide progress reports. Additionally, contacts are to influence others to utilize methods and procedures developed or sell them on the use of system IT and IT security techniques, planned action, or resolve inequities and incompatible situations involved with the system(s). Contacts with HQ USACE are to coordinate the use of standard USACE-wide systems, coordinate IT plans, coordinate security matters and issues, and obtain and provide information concerning the broad-based IT situations that arise. Level C

FACTOR 8. PHYSICAL DEMANDS FL 8-1 5 POINTS

Work is sedentary in nature.

FACTOR 9. WORK ENVIRONMENT FL 9-1 5 POINTS

Work is performed in a typical office setting.

TOTAL POINTS: 3190

GS-13 RANGE: 3155-3600