

Position Description - Final

PD #:
Shred:

Replaces PD #:

IT Specialist (INFOSEC/PLCYPLN)

GS-2210-12

Installation:

Major Command:

Region:

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

Classified By:
Classified Date:

FLSA:
Career Program:
Functional Code:
Competitive Area:
Competitive Level:

Drug Test Required:
Financial Disclosure Required:
Requires Access to Firearms:
Position Sensitivity:
Emergency Essential:

CIPMS PD:
Acquisition Position:
Interdisciplinary:
Target Grade/FPL:
Career Ladder PD:

MAJOR DUTIES

Summary: Serves as technical expert, source of expertise, and focal point within a U.S. Army Corps of Engineers (USACE) District concerning IT security/information assurance and IT policy and planning plans, programs and initiatives. Serves as the appointed District Information Assurance Manager (IAM) to plan, develop, implement and maintain automation security programs to ensure the confidentiality integrity, and availability of automated systems, networks and data/information spanning the planning, analysis, development, implementation and maintenance phases of the District Information Technology (IT) programs. Additionally, accomplishes technical, analytical and advisory functions pertinent to the development of local policies, development of short and long range IT planning, and associated processes covering the District IT program. Within this framework, performs the following:

1. As the District's IAM is the local technical expert for and exercises overall responsibility for the Information Assurance (IA) Program. This program includes security management, software security, IT equipment security, procedural security, data communications security, and AIS media security. Plans, develops, implements and maintains District programs, policies and procedures to protect the integrity and confidentiality of 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 databases covering administrative as well as technical functions and work programs; and training and educating personnel on information systems security practices.

- Appoints, manages, reviews and audits the technical work of District Information Assurance Security Officers (IASOs) and other personnel assigned in any of the District organizations and involved in Information System Security including System Administrators (SA). Ensures that automated system design and developments, involving both in-house and contractual efforts, comply with Department of

Defense (DOD) and Army IA requirements and participates in system changes and modifications to insure the development of related system security policies and measures. Develops systems security contingency plans and data recovery procedures. Reviews and evaluates the security impact of system changes including interfaces with other systems. Coordinates IA for database design, development and maintenance of all automated data systems. Develops, coordinates and maintains the DOD Information Technology Security Certification and Accreditation Program (DITSCAP), prepares or oversees the preparation of accreditation documentation and reviews and evaluates accreditation input furnished by other IT Specialists. Maintains current AIS accreditation statements and initiates re-accreditation when security-impacting changes have occurred.

- Ensures that all District information management systems are operated & maintained according to higher authority regulations, that users have the required security clearances, authorizations and need to know, and that personnel associated with IM 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 & 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 District personnel on actual or potential computer virus threats. Establishes systems for issuing, protecting and changing system passwords. Manages the review of system audit trails and insures the thorough investigation of discrepancies. Maintains access control records and establishes access control policies covering access to systems only by authorized personnel.

- Serves as the focal point for all aspects of the District-wide IA program providing expert advice and guidance pertinent to IA program policies, guides and procedures during all stages of the automation process. Enforces security policies and safeguards for District systems including stopping system operation if warranted by the seriousness of security violations. Develops IM security plans, local policy guidance, regulations and procedures, and standard operating procedures to ensure IA regulatory requirements are followed. Provides oversight for IA programs insuring compliance with overall District plans and higher authority policies and guidance. Conducts and participates in various IA security meetings with District organizational elements and representatives of other districts to plan evaluate and determine appropriate measures needed to ensure security requirements are met. Gives presentations at meetings with District and Division level officials. Coordinates security actions with the District Security and Law Enforcement staff.

- Serves as the lead and project manager on broad and comprehensive IA reviews, investigations and studies. Leads teams of IT specialists and subject matter specialists under the matrix management concept to study IA problems, compliance matters and potential for application of new initiatives.

2. Serves as technical expert and advisor within the District concerning IT Policy and Planning specialty functions. Serves as the District lead on technical, analytical and advisory functions pertinent to the development of local IT policies and strategic plans; the development, implementation, modification, and maintenance of long and short range IT planning; development and recommendation of District-wide IT goals, objectives, policies and priorities; and ensuring that the District IT program is in compliance with higher authority policies and guidelines.

- Integrates organizational input and documentation in developing the District's IT Plans and revises and maintains such plans as required including involvement with both long and short range aspects of such plans. Provides advice and guidance to managers in meeting strategic goals. Provides oversight, direction, guidance and advisory services to all District division and separate office managers concerning unplanned and/or non-programmed needs requiring out-of-cycle inclusion in the Strategic Plan. Ensures all District information management initiatives are created and maintained in the IT Investment Portfolio

System. Provides comprehensive management advisory services and liaison to all organizational levels within the District pertinent to emerging and future advances in information technology applicable locally. Develops District policies and broad-based plans to protect the integrity and confidentiality of automated systems, networks, data, and automation resources/functions.

- Serves as the District focal point pertinent to action to expand existing computer infrastructure, evaluate needs, and activate automation improvements and enhancements. Serves as the District expert and leader for information system planning and implementation studies. Leads study team efforts under the matrix management concept on broad planning studies impacting substantial District IT resources. Analyzes program development and conducts studies within the District to evaluate and determine IT requirements. Conducts pre-study briefings of 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 and meets with District managers to discuss progress in meeting District strategic goals. Closely coordinates with Division Headquarters and U.S. Army Corps of Engineers (USACE) headquarters (HQ) levels to ensure agency compatibility and to recommend priorities for strategic planning and implementation. Represents the District at Division HQ level policy and planning meetings. Integrates varying policy changes and planning initiatives resulting from studies and develops proposals for consideration.

- Accomplishes District Information Management (IM) policy development. Develops and provides recommendations to the IM Chief concerning District-wide IM goals, objectives, policies and priorities. Reviews drafts of policies and plans assigned to lower grade specialists assigned to assist on broad reviews and studies. 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 District 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. Coordinates with District IT experts in other specialty areas to discuss the impacts of changes in existing policy and planning initiatives. Initiates and conducts briefings, and prepares summaries and correspondence within the District concerning IT budget formulation and execution matters. Develops and maintains the District portion of the Information Technology Investment Portfolio database pertinent to the management, justification and acquisition of IT. Plans, coordinates and conducts District workshops, meetings and seminars to provide advisory services, guidance and training concerning the intent and direction of the District IT program.

Performs Other Duties as Assigned

Factor 1- Knowledge Required by the Position

FL 1-7 1,250 pts.

- Broad knowledge of a wide range of IT standards, system principles, concepts, methods, policies, associated methods and tools to accomplish policy and planning job requirements and develop, evaluate, implement and disseminate affective automation security/information assurance processes/measures within the District; and, to serve as the District contact concerning and provide advisory services pertinent to IT planning and the IA program to protect the integrity and confidentiality of automated systems, networks and data. Knowledge of IA security certification and accreditation requirements and network operations and protocols to study, monitor, investigate, evaluate, assess and remedy identified and potential security vulnerabilities, threats, and compliance problems. Knowledge of higher authority guides and regulations as well as state of the art automation security methods, techniques, equipment and processes to develop local policies, regulations and guidance and provide advice and guidance to all

District elements concerning the application, implementation and maintenance of most effective automation security program.

- Knowledge and skill in the use of project management methods and techniques to serve as the lead on comprehensive and broad IA studies and studies pertinent to strategic planning, the capital investment knowledge management program plans, capital investment planning, and the District's enterprise IT goals and objectives. Knowledge of and experience in the use of oral and written communication methods and techniques to accomplish continuing coordination with District customers and make presentations at District and Division meetings, seminars and training sessions.
- Knowledge of the IT equipment available and needed implement new or changed aspects of the District's IT program. Knowledge of state-of-the-art IT, existing District IT requirements, new or changed needs, and sources of IT support/technology to develop, monitor and enhance the local IA program; and develop evaluate District IT needs, establish goals and objectives, and develop long and short range cost effective and viable plans covering a myriad of inter-related IT considerations.
- Knowledge of IT resources and infrastructure including automated systems, equipment and software, and system technology to serve as a technical specialist within the District concerning IT security/IA and District IT planning and policy development. Knowledge of the organizational structures, functions, work processes/programs of District organizations, as well as a high degree of analytical ability to gather, assemble and analyze facts, draw conclusions and devise solutions to problems which will increase the effectiveness of the District IT program. Knowledge of capital investment planning methods, principles and processes to analyze & study current and necessary systems and develop long and short range plans to effectively cover the Districts needs.

Factor 2 – Supervisory Controls

FL 2-4 450 pts.

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 District IT security process, program, and requirements; and local IT planning and policy matters. Consults with the supervisor on matters pertaining to timeframes, 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, analyses and organizes projects associated with assignments. There is a continuing requirement for coordination (users and other impacted IM Specialists), and the incumbent independently plans and carries out the necessary coordination including that involving lower level IM Specialists and efforts of contract employed persons. Is the highest level of expertise within the District concerning the above-identified assignments and independently provides advice and guidance within the District 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 timeframes, and customer satisfaction.

Factor 3 – Guidelines

FL 3-4 450 pts.

Guidelines include agency regulations, manuals and policies which provide overall goals and define limitations and overall objectives; USACE regulations, policies and procedures concerning IT Policy Planning and IT Information Security/Assurance and all automated systems used in USACE; District regulations and guidelines; and a variety of manufacturers' manuals and handbooks pertaining to the wide range of IT equipment and software in use in the District. The assignments in the assigned specialities in this job are those of the most complex category and/or have broad impacts and the guides covering this level of work are typically broad and frequently require interpretations and deviations from previously

used methods. Regularly, the incumbent must use ingenuity and experienced judgement in adapting existing methods, extensively interpret higher authority and develop new methods and approaches to resolve automation security/IA 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 District automation processes, and develop local guides, standard operating procedures, bulletins and fact sheets for distribution and use within the District concerning a myriad of the automation functions and processes. The incumbent must apply judgement to anticipate problems, research trends in state-of-the-art technology, and develop special adaptations to satisfy requirements.

Factor 4 – Complexity

FL 4-5 325 pts.

Assignments involve planning, coordinating and accomplishing overall IT security/information assurance requirements as well as policy and planning processes for the District. Work requires in-depth analysis, study & consideration of a myriad of complex IT information security/assurance and policy and planning factors and many different an unrelated processes and methods. There is a continuous requirement in this job for coordination both in the information assurance/security and the policy and planning arena. Additionally work includes the responsibility for serving as the District focal point and source of expertise concerning District IT security, policy & planning needs and problem resolution. Work is complex because of the continuing changes in District business requirements and the rapidly changing IT environment requiring the evaluation of the impacts of technological changes on District business processes and the existing Information assurance/security processes. The incumbent must remain updated on changing the most recent developments in information technology and IT security technology and continuously evaluate changing future organizational data needs. The incumbent must develop management strategies, overall 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 information assurance/security requirements. Must ensure that District IT information security/assurance plans and policy and planning initiatives are integrated and conform with Division HQ, HQ USACE and higher level plans, programs and initiatives. 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 District requirements.

Factor 5 – Scope and Effect

FL5-4 225 pts.

The work of this position involves the responsibility for serving as the District expert and focal point for all Information Assurance/Security planning, measures, modification and administration for the District **and** the full range of IT policy and planning requirements pertinent to District IT infrastructure. Is the District focal point and source of expertise for the above-identified functions. Work covers IT equipment, software, a myriad of system interfaces, data management, system analysis, and system administration. Information Assurance/Security involves 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 District IT security problems that impact District IT systems, the availability of 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 District business processes.

The IT security work impacts the continuing accessibility and availability of a variety of mission critical applications and the continuing protection of the District's IT assets through the administration of

effective information assurance/security programs. Policy and planning work impacts the District'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 information technology to the District's mission.

Factor 6 - Personal Contacts

FL 6-3 & 7-c 180 pts.

Factor 7 – Purpose of Contacts

Contacts are with IM Managers and Specialists within the employing District organizations; technical specialists in similar specialties in other Districts; managers and technical experts/specialists in the Division HQ offices; with HQ USACE specialists and functional proponents of major Corps corporate systems, and IT experts; and occasional contacts with IT experts at the DA level and other federal agencies. Contacts regularly include meetings with contractors, equipment manufacturer's representatives, providers of services (e.g., software) related to technological developments applicable to the project, and members of USACE technical committees. Contacts typically take place in moderately unstructured settings.

Contacts are to exchange information, determine IT system & 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 IT information assurance/security techniques; the use of changed strategic planning features; short and long range action plans; or resolve inequities and incompatible situations involved with the matters in either of the two assigned specialty areas. Contacts with HQ USACE are to coordinate the use of standard USACE-wide systems, coordinate policy and planning initiatives, IT plans, information assurance/security matters and issues and obtain and provide information concerning the broad-based IT situations that arise.

Factor 8 – Physical Demands

FL 8-1 5 pts.

Work is sedentary in nature

Factor 9 – Work Environment

FL 9-1 5 pts.

Work is performed in a typical office setting.

Total Points – 2,890 pts. (2755 – 3150, GS-12 point range)