**Introduction**

This position is located Enterprise Information Security Office (EISO), Office of Information Technology (OIT).

The incumbent in this position serves as an IT Security Specialist.

**Major Duties and Responsibilities**

Assists senior IT Specialist in the implementation of information security policies, standards, and processes for PBGC Information Technology (IT) infrastructure, system monitoring, and intrusion management for business systems and financial systems and their associated databases.

Assists in coordinating, developing and conducting annual information Security Awareness Training, Role Base Training, and specialized training within the EISO.

Promotes awareness of security issues and ensures sound security principles are reflected in organizations’ visions and goals.

Performs access control and account monitoring duties related to accessing IT applications and resources. Develops and implements programs to ensure that systems, network, and data users are aware of, understand and, adhere to systems security policies and procedures.

Participates in systems security contingency plans and disaster recovery procedures and activities.

Ensures the application of information security information assurance (IA) policies, principles, and best practices in the delivery of IT services.

Consults with customers to identify and specify requirements.

Responds to inquiries and requests for assistance with security issues, identifies problems, troubleshoots and provides advice to assist users.

Coordinates and facilitates Security Assessment and Authorization (SA&A) activities.

Reviews government regulations, policies, guidelines and standards on Computer and Information Security to ensure compliance with PBGC’s Enterprise Information Security Program (EISP).

May be required to serve on ad hoc or special task forces in connection with implementation of new EISP policies, organization alignments, review and resolution of newly identified EISP problems, etc.

Prepares requisition forms for IT security hardware and software purchases.

Performs other related duties as assigned.

**Factor 1 – Knowledge Required by the Position Level 1-7 = 1250 Points**

Knowledge of Federal and PBGC information security concepts, principles, methods, directives and practices and the laws, regulations, guidelines and policies which govern the establishment and maintenance of EISP encompassing an enterprise-wide multi-tiered security infrastructure, and information security, audit and control programs.

Technical knowledge of PBGC computer systems applications, capabilities, operations tools and numerous business operations to establish, implement, and secure PBGC’s information security infrastructure.

Knowledge of risk analysis techniques and methodologies in order to identify threats to, and vulnerability of IT resources to determine the possibility of an adverse effect occurring.

Knowledge of the Federal Information Security Management Act.

Ability to communicate orally and in writing to discuss technical solutions to information security, organizational, and management problems.

**Factor 2 – Supervisory Controls Level 2-4 = 450 Points**

The Senior Agency Information Security Officer assigns work in terms of areas of continuing responsibility and scope of assignment. The employee is responsible for independently planning and carrying out assignments including approach to be taken; resolving most conflicts that arise; coordinating the work of contractor and federal government employees with others; interpreting policy on own initiative in terms of established objectives; and keeps the SAISO informed of progress and of potentially controversial matters. Completed work is reviewed for soundness of overall approach, effectiveness in meeting requirements or producing expected results, the feasibility of recommendations, and adherence to requirements.

**Factor 3 – Guidelines Level 3-4 = 450 Points**

Guidelines include Federal regulations governing OIT and protection of security infrastructures, established PBGC corporate policies and procedures, technical and operational objectives. These guidelines are inapplicable or have gaps in specificity that require considerable interpretation and/or adaptation for application to issues and problems. The employee uses judgment, initiative, and resourcefulness in deviating from established methods.

**Factor 4 – Complexity Level 4-4 = 225 Points**

The work consists of implementing and maintaining IT security systems and conducting audits of IT systems and operations to ensure that agency is in compliance with all applicable laws and regulations; necessary controls are in place; and systems operate as intended and provide all necessary capabilities. The employee reviews systems documentation, including IT project implementation, security policies and procedures, hardware, software, network diagrams, configuration management controls, and contractual agreements for compliance with applicable standards.. Exercises judgment to continually evaluate and recommend the adoption of new IT security methods and present audit findings to supervisor, colleagues, and program officials, and develop recommendations for improvement in information security management, where appropriate.

**Factor 5 – Scope and Effect Level 5-3= 150 Points**

The work involves analyzing and defining the security requirements for new enterprise applications available on PBGC’s network infrastructure recommending selection and installation of appropriate security tools, and supporting the implementation of an IT security program consisting of standards, procedures, and guidance to protect information available on a major wide area network from unauthorized access. Work contributes to the protection of the infrastructure from unauthorized access.

**Factor 6 – Personal Contacts Level 6-3 = 60 Points**

Contacts include PBGC managerial and technical staff, contractor management, vendor representatives in a moderately unstructured setting. For example, the contacts are not established on a routine basis; the purpose and extent of each contact is different; and the role and authority of each party is identified and developed during the course of the contact.

**Factor 7 – Purpose of Contacts Level 7-3 = 120 Points**

The purpose is to plan, coordinate, or advise on work efforts, or to resolve security issues or operating problems by persuading and influencing supervisors and managers to accept and implement findings and recommendations. The employee may encounter resistance as a result of issues such as competing objectives or resource problems. The employee must be skillful in approaching contacts to obtain the desired effect, e.g., gaining compliance with established policies and regulations by persuasion or negotiation.

**Factor 8 – Physical Demands Level 8-1 = 5 Points**

The work is sedentary. Typically, the employee may sit comfortably to do the work. However, there may be some walking, standing, bending, stooping and/or carrying of light items such as papers, books, etc. Occasional travel may be required.

**Factor 9 – Work Environment Level 9-1 = 5 Points**

The work is performed in an office setting, which is adequately lighted, heated and ventilated.