U.S. Office of Personnel Management
Division for Human Capital Leadership & Merit System Accountability
Classification Appeals Program

Atlanta Field Services Group
75 Spring Street, SW., Suite 1018
Atlanta, GA 30303-3109

Classification Appeal Decision
Under section 5112 of title 5, United States Code

Appellant:	[appellant]
Agency classification:	Information Security Specialist (Automated Information Systems) GS-080-11
Organization:	[name] Office [name] Veterans Affairs Medical Center Department of Veterans Affairs [location]
OPM decision:	Information Security Specialist GS-080-9
OPM decision number:	C-0080-09-03

Marta Brito Pérez
Associate Director
Human Capital Leadership
and Merit System Accountability

August 20, 2004
Date

As provided in section 511.612 of title 5, Code of Federal Regulations, this decision constitutes a certificate that is mandatory and binding on all administrative, certifying, payroll, disbursing, and accounting officials of the government. The agency is responsible for reviewing its classification decisions for identical, similar, or related positions to ensure consistency with this decision. There is no right of further appeal. This decision is subject to discretionary review only under conditions and time limits specified in the *Introduction to the Position Classification Standards*, appendix 4, section G (address provided in appendix 4, section H).

Since this decision lowers the grade of the appealed position, it is to be effective no later than the beginning of the sixth pay period after the date of this decision, as permitted by 5 CFR 511.702. The applicable provisions of parts 351, 432, 536, and 752 of title 5, Code of Federal Regulations, must be followed in implementing the decision. If the appellant is entitled to grade retention, the two-year retention period begins on the date this decision is implemented. Since position descriptions must meet the standard of adequacy in the *Introduction to the Position Classification Standards*, section III.E, the appellant's position description must also be revised, as discussed in this decision. The servicing personnel office must submit a compliance report containing the corrected position description and a Standard Form 50 showing the personnel action taken. The report must be submitted within 30 days from the effective date of the personnel action.

Decision sent to:

[appellant]
[address]
[location]

[name]
Chief
Human Resources Management Service
Veterans Affairs Medial Center
Department of Veterans Affairs
[address]
[location]

Human Resources Officer
Office of Human Resources Management (054B)
Department of Veterans Affairs
810 Vermont Avenue, NW.
Washington, DC 20420

Deputy Assistant Secretary for Human
Resources Management (05)
Department of Veterans Affairs
810 Vermont Avenue, NW., Room 206
Washington, DC 20420

Introduction

On March 19, 2004, the Atlanta Field Services Group of the U.S. Office of Personnel Management (OPM) accepted a classification appeal from [appellant] who is employed as an Information Security Specialist (Automated Information Systems), GS-080-11. She works in the [name] Office, [name], Veterans Affairs Medical Center (VAMC), Department of Veterans Affairs, [location]. The appellant requests that her position be reclassified as an Information Technology (IT) Specialist (INFOSEC), GS-2210-12. She believes that her agency improperly reclassified her position from the IT Management Series, GS-2210, to the Security Administration Series, GS-080. We received the complete appeal administrative report from the agency on April 8, 2004. The appeal has been accepted and processed under section 5112(b) of title 5, United States Code (U.S.C.).

Both the appellant and the supervisor certified the accuracy of the position description. To help decide the appeal, we conducted a phone and onsite audit with the appellant and interviewed her immediate supervisor. We also interviewed the IT Specialist (INFOSEC) at the Veterans Integrated Service Network (VISN) [#] who has oversight responsibility for Automated Information System (AIS) security at all the VISN's facilities. In reaching our classification decision, we have carefully reviewed the audit findings and all information of record furnished by the appellant and her agency, including her official position description, number [#].

General issues

The appellant's position was previously classified as IT Specialist, GS-2210-11. On November 18, 2003, the agency conducted a desk audit and determined that the position's duties did not meet the paramount knowledge requirement for inclusion in the IT Management Series, GS-2210. The position was reclassified as Information Security Specialist (Automated Information Systems), GS-080-11, effective March 7, 2004. The appellant subsequently appealed to OPM.

The appellant makes various statements about her agency's review and evaluation of her position in arriving at its classification decision. In adjudicating this appeal, our only concern is to make our own independent decision on the proper classification of her position. By law, we must make that decision solely by comparing her current duties and responsibilities to OPM standards and guidelines (5 U.S.C. 5106, 5107, and 5112). Therefore, we have considered the appellant's statements only insofar as they are relevant to making that comparison.

Position information

A position description is the official record of the major duties and responsibilities assigned to a position by an official with the authority to assign work. A position is the duties and responsibilities that make up the work performed by an employee. Position classification appeal regulations permit OPM to investigate or audit a position and decide an appeal on the basis of the actual duties and responsibilities currently assigned by management and performed by the employee. An OPM appeal decision classifies a real operating position and not simply the position description. Therefore, this decision is based on the work currently assigned to and performed by the appellant and sets aside any previous agency decision.

Our fact finding revealed that the appellant's official position description overstates the duties and responsibilities assigned to and performed by the appellant, particularly with regard to the nature of the knowledge required by the position, supervisory controls, complexity of the work performed, and the personal contacts. The duties and responsibilities described in the position description typically are performed by positions found at higher organizational levels within an agency. For example, the position description indicates that the appellant is responsible for anticipating and resolving AIS security problems resulting from changing legal, policy, and procedural requirements. However, the record shows that this responsibility is vested in the agency headquarters policy staff and intervening staff offices within the appellant's agency. The appellant receives work direction and review from these staff offices, although the position description describes considerable independent action and does not include staff office technical review and program controls. The position description also indicates that the appellant performs AIS systems and performance analysis. These activities are highly technical in nature and are typically carried out by IT Specialists at various levels within the agency who are responsible for the technical aspects of AIS systems and network operations. Another example involves contacts while representing the agency at national meetings and conferences, or contacts with officials from other agencies. The responsibility for representing the agency at high level meetings and conferences lies at higher echelons within the agency. While the appellant may attend conferences, she does not represent or speak for the agency. Her contacts are primarily with personnel within her agency in a structured setting.

Since position descriptions must meet the standard of adequacy in the *Introduction to the Position Classification Standards*, the appellant's agency must revise her position description to meet that standard.

The [name] Office provides analytical and advisory support to facility workgroups and staff support services to program activities throughout the center and serves as the control center for surveys, data analysis, planning, workload and performance monitoring, and reporting. Programs aligned under the office include Public Relations, the Decision Support System, Strategic Planning, VA/DoD Sharing, Information Security, and Compliance and Business Integrity.

Within that office, the appellant functions as the medical center's Information Security Officer (ISO). In this capacity, she is a member of the management team responsible for planning, establishing, and implementing the center's AIS security program. The appellant is primarily responsible for implementing and monitoring the local AIS security program to ensure compliance with legal and regulatory requirements for safeguarding personnel and other sensitive data and protecting the center's automated systems from fraud, waste and abuse. She develops or updates station specific policy and procedures when required. She assures that all systems have a current system security plan. She works with IT Specialists assigned to the [name] Service (IMS) and other organizations to conduct vulnerability assessments. These assessments are to identify potential sources of damage, destruction, or alteration of systems, ensure the physical security of computer systems, terminal devices, and access controls for software and data, and ensure the proper disposition of forms, printed output, and non-computerized materials containing sensitive patient and personnel information. She monitors sensitivity level designations for all staff positions to ensure that access is on a need to know

basis, investigates security breaches, and incidents and recommends appropriate action to the center director, maintains AIS security documentation files, conducts AIS security orientation for new employees, and coordinates and conducts the center's ongoing AIS security awareness training program.

The appellant works under the administrative supervision of the Coordinator (Management Analyst, GS-343-13) who heads the Management Support Office. Technical oversight is provided by the VISN IT Specialist (INFOSEC) who functions as the VISN ISO and has functional responsibility for ISO positions. (A May 2003 reorganization of the VA Office of Information and Technology centralized all cyber security functions within VA and stipulated technical oversight of ISO positions by the VISN level ISO.) Assignments are carried out in accordance with AIS security requirements and standards established by her own and other agencies. The appellant works within program requirements and independently plans, schedules, coordinates, and carries out her work. The supervisor is kept informed of work progress and any potentially controversial matters. Supervisory assistance is normally sought only when issues arise in coordinating activities with managers in other organizations. Administrative review of work is in terms of meeting due dates and deadlines. In-depth technical reviews of the appellant's work products occur during external reviews and assessments conducted by reviewing organizations (e.g., VISN ISO, agency Inspector General (IG), and Office of Cyber Information Security (OCIS), Joint Commission on Accreditation of Health Care Organizations (JCAHCO), etc.).

The position description and other material of record furnish more information about her duties and responsibilities and how they are performed and we incorporate it by reference into this decision.

Series, title, and standard determination

The agency classified the appellant's position in the Security Administration Series, GS-080, and titled it Information Security Specialist (Automated Information Systems). The appellant believes her position is covered by the Job Family Standard for Administrative Work in the IT Group, GS-2200, and should be classified in the GS-2210 Series as IT Specialist (INFOSEC).

The GS-2210 series covers two-grade interval administrative positions that manage, supervise, lead, administer, develop, deliver, and support IT systems and services. This series covers only those positions for which the paramount requirement is knowledge of IT principles, concepts, and methods, e.g., data storage, software applications, networking. This knowledge is used to perform such functions as planning, designing, analyzing, developing and implementing systems for the organization. IT refers to systems and services used in the automated acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, assurance, or reception of information. IT includes computers, network components, peripheral equipment, software, firmware, services, and related resources.

The appellant is responsible for the implementation and monitoring of the AIS security program to protect and safeguard sensitive information related to personnel, patients, etc., at the medical center. The work performed is administrative in nature and does not require the technical

knowledge of IT principles, concepts, and methods as found at the GS-2210 series. The appellant's access to the center's AIS allows her to perform specific activities that agency regulations require be performed only by the individuals designated as ISO. These include reviewing user network activity and security event logs to monitor non-work-related excessive bandwidth usage, user access of inappropriate Internet sites, and user attempts to access unauthorized information/system areas. Activities also include conducting system scans for viruses and missing software patches, failures to log off of the system, etc. The appellant has no administrator-level access to the center's AIS network as VA regulations require that the individual designated as the ISO cannot have any operational or management responsibility for the AIS. The appellant's position does not meet criteria for classification in the GS-2210 series and evaluation using the GS-2200 JFS.

The duties and responsibilities of the appellant's position are characteristic of the work described in the GS-080 series. This series includes positions the primary duties of which are analytical, planning, advisory, operational, or evaluative work that has as its principal purpose the development and implementation of policies, procedures, standards, training, and methods for identifying and protecting information, personnel, property, facilities, operations, or material from unauthorized disclosure, misuse, theft, assault, vandalism, espionage, sabotage, or loss. Duties involve the management, supervision, or performance of work in: (1) developing, evaluating, maintaining, or operating systems, policies, devices, procedures, and methods used for safeguarding information, property, personnel, operations, and materials, and/or (2) developing and implementing policies and procedures for analyzing and evaluating the character, background, and history of employees, candidates for employment, and other persons having or proposed to be granted access to classified or other sensitive information, materials, or work sites.

We find that the appellant's position is properly allocated to the GS-080 series and titled as Information Security Specialist. Based on the titling instructions in the GS-080 standard, the agency may add a parenthetical title to further identify the specific knowledge and skills required to perform the work.

Grade determination

The GS-080 standard is written in the Factor Evaluation System (FES) format, under which factor levels and accompanying point values are assigned for each of nine factors. The total is converted to a grade level by use of the grade conversion table provided in the standard. Under the FES, each factor level description in a standard describes the minimum characteristics needed to receive credit for the described level. Therefore, if a position fails to meet the criteria in a factor level description in any significant aspect, it must be credited at a lower level. Conversely, the position may exceed those criteria in some aspects and still not be credited at a higher level. Our evaluation with respect to the nine FES factors follows.

Factor 1, Knowledge required by the position

This factor measures the nature and extent of information or facts which the workers must understand to do acceptable work. The agency credited this factor at Level 1-7.

At Level 1-6, employees apply practical knowledge of commonly applied security principles, concepts, and methodologies in carrying out assignments and developing skills in performing limited independent work. The nature of the assignments requires some application of judgment in the use of security knowledges and the employee must develop skill in weighing the impact of variables such as cost; critical personnel qualifications; variations in building construction characteristics; access and entry restrictions; equipment availability; and other issues that influence the course of actions taken in resolving security questions or issues. Employees use knowledge of security criteria, equipment, or techniques to resolve well-defined questions or conditions. Considerations include clearance level required, adjudication of security clearances when clear-cut information is present, nature of materials or information to be protected, cost-benefit relationships for security devices or equipment systems, and similar considerations. Some employees use knowledge at this level to serve as team members performing security surveys, and/or in planning and implementing specific assignments that comprise part of an overall security plan and the installation of security systems. Such assignments typically involve coordinating with other members of the team and, perhaps, security and subject-matter specialists concerned with other, related security systems which may impact on the plans and recommendations of the team.

Level 1-6 is met. As at Level 1-6, the appellant performs a variety of administrative and analytical duties related to the implementation and monitoring of a well-defined AIS program to ensure the security of sensitive patient, personnel and other data at the center. Her work requires the application of a practical knowledge of standardized security principles, concepts, and methodologies required by her own and other agencies, laws and regulations and consideration of the impact of variables relative to facilities, access restrictions, equipment, etc. She applies this knowledge in physically inspecting AIS equipment and areas where it is located; analyzing system generated data indicating improper use of AIS equipment or possible unauthorized attempts to access data and information; and checking workstation areas to monitor user password protection, security or disposal of printed material containing sensitive data, and proper logout from the system. She also checks for security breaches when indicated by network activity and security event logs, or when notified of suspicious activity by the VISN ISO and follows appropriate techniques in following up with the individual assigned to the work station identified to determine if the activity was accidental or an intentional attempt to breach security protocol. Also comparable to Level 1-6, the appellant participates as a member of a facility assessment team, conducting the AIS risk assessment portion while an assigned IT Specialist is concerned with AIS technical issues related to contingency plans to backup and restart systems and recover from a disaster. She also participates in planning meetings such as those to assist the IT staff in developing emergency contingency plans by ensuring that processes and procedures implemented by the IT staff meet all mandated security requirements.

At Level 1-7, employees use knowledge, in addition to that at the lower levels, of a wide range of security concepts, principles, and practices to review independently, analyze, and resolve difficult and complex security problems. Work situations may involve overlapping and conflicting requirements within a single facility or for a geographic region or agreements with other organizations, agencies or with foreign governments for security resources and responsibility sharing. At this level, employees often use knowledge of security program

interrelationships to coordinate the objectives and plans of two or more specialized programs, make accommodations in study or survey recommendations to allow for differing program requirements, and develop or implement procedures and practices to cover multiple security objectives. Employees at this level are also involved in serving on inter-agency or inter-organization committees and groups to identify and resolve, or to assign responsibilities for resolving, security issues, or to perform similar work.

Level 1-7 is not met. The appellant's work relates to a single facility program and does not involve the variety of security concepts, principles, and practices or independent analysis and resolution of problems of the complexity and difficulty described at this level. Problems having this degree of complexity and difficulty are normally the responsibility of the VISN ISO who is the functional reporting official for all center ISOs through their administrative supervisors. The problems typically dealt with by the appellant require a sound knowledge of standard AIS security practices, and related agency and federal security policy, guidelines, standards, and requirements found at Level 1-6.

Level 1-6 is credited for 950 points.

Factor 2, Supervisory controls

This factor covers the nature and extent of direct or indirect controls exercised by the supervisor, the employee's responsibility, and the review of completed work. The agency credited this factor at Level 2-4.

At Level 2-3, the supervisor defines the employee's scope of responsibilities and the objectives, priorities, and deadlines. The employee is provided with more detailed assistance in unusual situations which do not have clear precedents. The employee, having developed competence in the assignment, plans and carries out the steps involved, handles deviations from established procedures, and resolves problems that arise in accordance with agency or local standards, previous training and experience, established practices, or other security controls appropriate to each assignment. Projects typically involve conflicting interrelationships between security and subject-matter requirements requiring investigation and solution by the employee to determine the methods and procedures to use in the assignment. Completed work is usually evaluated for technical soundness and appropriateness in relation to the nature and level of security required by the controlled materials, information, or facility involved. Techniques used by the employee during the course of the assignment are not usually reviewed in detail.

Level 2-3 is met. The appellant receives technical direction, through monthly ISO conference calls or as required, and oversight from the VISN ISO and administrative supervision from the office Coordinator. She carries out assignments in accordance with AIS security requirements and standards established by her own and other agencies which provide timeframes for review activities. The appellant coordinates her activities with the center's building inspection team schedule and plans and coordinates work resulting from the inspection activity and other AIS monitoring activities. Comparable to Level 2-3, on team inspections she identifies actual or potential threats to AIS operations and security risks and then works with other functional staff personnel, e.g., IT, safety, environmental management, housekeeping, etc., in order to explore

actual or potential problems involving fire, water hazard, electric power supply, temperature and humidity control, and housekeeping issues, and identify degree of risk and protection procedures. The appellant ensures that any issues or problems that would adversely affect AIS operations and security are brought to the attention of management and recommends that contingency plans are included in the center's AIS security program.

The appellant is also responsible for independently developing the local policy on the use of government-owned IT equipment by employees. She identifies what is considered acceptable and unacceptable use for Internet surfing by employees and the level of punishment for unacceptable use. As at Level 2-3, the appellant's administrative supervisor is kept advised of work progress and potentially controversial issues and provides assistance only when problems are encountered in coordinating her activities with managers in other organizations. Although the supervisor does not provide specific guidance on work assignments or detailed assistance in unusual situations which do not have clear precedents, program direction and specific guidance, if required, is provided by personnel at the VISN Information Security Office or the agency's OCIS. The administrative supervisor's review of completed work is based on the appellant meeting established due dates and deadlines. The effectiveness of her work is determined through review by higher level organizations within the agency responsible for AIS security (VISN, OCIS) and external reviews conducted by other organizations (agency IG, JCAHCO, etc.).

At Level 2-4, the supervisor sets the overall objectives and decides on the resources available. The employee consults with the supervisor in determining which projects to initiate, develops deadlines, and identifies staff and other resources required to carry out an assignment. The employee, having developed expertise in the particular security specialty area, is responsible for planning and carrying out the work, resolving most of the conflicts that arise, integrating and coordinating the work of others as necessary and interpreting policy in terms of established objectives. The employee keeps the supervisor informed about progress, potentially controversial matters, or developing security conditions or requirements with far-reaching implications. Finished work is reviewed from an overall standpoint in terms of feasibility, compatibility with other security program requirements, or effectiveness in meeting objectives and achieving expected results.

Level 2-4 is not met. Unlike Level 2-4, the appellant's work is more defined in that projects, timelines, and required resources are established by her own and other agencies responsible for the development of security standards for AIS equipment and data and her position does not have a significant role in identifying and establishing parameters for new projects. The appellant establishes a calendar based on mandatory security requirements determining her significant work activities for a year. The information typically reflects what activities are to be undertaken, other parties to be involved, when the activity is to occur, the guidance on which the activity is based, etc. The activities are designated as annual, semi-annual, quarterly, or monthly including her most significant activities: the review of security plans, review of the validity of risk assessments, review of new security standards, and review of the position descriptions and performance standards of IRMS staff. Also unlike Level 2-4, the appellant's work is not so complex as to require consultation with the supervisor on matters such as identifying the personnel and resources required to accomplish projects. The limited nature of her work does

not routinely involve review for feasibility and compatibility with other programs requirements. These are matters for which responsibility lies with organizations at higher levels of the agency. Our review of security guidance revealed that the agency has put in place very specific policies and procedures that must be to be followed in implementing and monitoring the AIS security program. This precludes credit of Level 2-4.

Level 2-3 is credited for 275 points.

Factor 3, Guidelines

This factor covers the nature of guidelines and the judgment needed to apply them. Guides used in this occupation include desk manuals, established security procedures, policies, and traditional practices, and general reference materials such as national or agency directives and others that set the tone for security programs. The agency credited Level 3-3.

At Level 3-3, guidelines available and regularly used in the work are in the form of agency policies and implementing directives, manuals, handbooks, and locally developed supplements to such guides, such as building plans, survey schedules, detailed work procedures, and directives that supplement agency directions. The guidelines are not always applicable to specific conditions or there are gaps in specificity in application to specific security system requirements. The employee uses judgment in interpreting, adapting, and applying guidelines to analyze and develop security plans within the intent of available guidance and independently resolves gaps in specificity or conflicts in guidelines, consistent with stated security program objectives.

Level 3-3 is met. As at Level 3-3, guidance available to and regularly used by the appellant in carrying our her assignments include agency directives and handbooks, Code of Federal Regulations (CFR), Office of Management and Budget (OMB) circulars and bulletins, National Institute of Standards and Technology (NIST) publications, Federal Information Resources Management Regulations (FIRMR), the Health Insurance Portability and Accountability Act (HIPPA), and local policies and other guidance based on center specific circumstances, etc. The appellant adapts or interprets guidelines and develops local policies to supplement the agency guidance.

At Level 3-4, guidelines provide a general outline of the concepts, methods, and goals of security programs. The guidelines regularly applied at this level consist of broad security guidance, such as directives issued by national security agencies, general agency policy statements and objectives, and other guidance requiring refinement and coordination, or they are not specific as to how they are to be defined, implemented, and monitored. Where guidelines for performing the work are scarce or of limited use, the employee develops guides to be followed by security specialists at the same and lower levels in the organization, including facilities and programs in various geographical regions.

Level 3-4 is not met. The guidelines regularly used by the appellant are not of the broad and general nature or lacking in specificity as to require the refinement envisioned at this level. The guidance used for the appellant's work is specific in defining areas to be addressed and methods to be employed in implementing and monitoring an AIS security program to protect sensitive

information. The appellant is not involved in the development of guidance to be followed by any other security specialists. Higher organizational levels (e.g., OCIS, VISN, etc.) of the agency are responsible for developing comparable security guidance.

Level 3-3 is credited for 275 points.

Factor 4, Complexity

This factor covers the nature, number, variety, and intricacy of tasks, steps, processes, or methods in the work performed, the difficulty in identifying what needs to be done, and the difficulty and originality involved in performing the work. The agency credited Level 4-4.

At Level 4-3, employees perform various duties requiring the application of different and unrelated methods, practices, techniques, or criteria. Assignments characteristic of this level include: developing alternate security plans for a facility which describe options in levels of protection and the costs involved for a Federal or private sector facility where the minimum protection requirement is well-defined and accepted techniques are appropriate. Employees compile, analyze, and summarize information relating to the designated security requirements, develop plans for approaches that may be taken, define the level of risk involved for each plan, the costs for implementing each of several options, and recommend a course of action to meet assignment objectives. Recommendations on implementation of specific security systems and alternatives are based on factual information such as available funding, minimum regulatory requirements, delegated authorities to local managers to accept different levels of risk, and other factors that define the range of acceptable security decisions, programs, or systems related to the assignment.

Level 4-3 is met. As at Level 4-3, the appellant's work involves compiling, analyzing, and summarizing information identifying possible AIS security risks, options available to mitigate those risks, the cost of implementing the options, and other pertinent information that will assist management in making informed decisions as to the courses of action to follow. Regulatory and agency requirements for the security program are well-defined and based on commonly accepted and established techniques. Comparable to Level 4-3, the appellant conducts risk assessments and develops recommendations based on factual observations, such as consideration of available funding, minimum regulatory requirements, and the authority of the center Director to determine that a certain level of risk is acceptable. All risk assessment findings, agency requirements, and recommendations are documented and presented to the center Director.

At Level 4-4, employees perform assignments consisting of a variety of security duties involving many different and unrelated processes and methods relating to well-established areas of security planning and administration. Assignments typically concern several broad security program areas or, in a specialty area, require analysis and testing of a variety of established techniques and methods to evaluate alternatives and arrive at decisions, conclusions, or recommendations. Programs and projects may be funded by different organizations with differing security requirements or variations in ability to fund system implementation. The implementation of established security policies, practices, procedures, and techniques may have to be varied for a number of locations or situations which differ in kind and level of security, complexity, and local

conditions or circumstances requiring adjustment or modification in established approaches. Implementation of the results of analysis may have to be coordinated with other organizations and security systems to assure compatibility with existing systems and demands on available resources.

Level 4-4 is not met. The appellant's work requires performance of well-defined duties, e.g., identifying unsafe security conditions and situations, ensuring required security policies are put in place, etc., related to ensuring that the center meets all security requirements for the AIS and the protection of the sensitive data it contains. Unlike Level 4-4, her work is specific to the center's AIS and does not require varying security policies, practices, procedures, and techniques for implementation for a number of locations with differing levels of security, complexity, and local conditions. Also unlike Level 4-4, her assignments do not routinely involve analyzing or testing of techniques since those used are well-defined and are required by agency policy. The appellant's recommendations on what must be done are based on her analysis of information developed during risk assessments.

Level 4-3 is credited for 150 points.

Factor 5, Scope and effect

This factor covers the relationship between the nature of the work and the effect of work products or services both within and outside the organization. The agency credited Level 5-3.

At Level 5-3, the work involves resolving a variety of conventional security problems, questions, or situations where responsibility has been assigned for monitoring established security systems and programs or performing independent reviews and recommending actions involving well-established criteria, methods, techniques, and procedures. The employee's work products, advice, and assistance affect the effectiveness and efficiency of established security programs and contribute to the security effectiveness of newly introduced programs and facilities requiring such protective services. The effect of the work is primarily local in nature.

Level 5-3 is met. As at Level 5-3, the appellant's work involves resolving conventional AIS security problems and issues. She monitors the implementation of an established security program for the center by conducting risk assessments, ensuring that appropriate employee sensitivity level designations are granted, and ensuring that employee access to system information is limited to that related to the work performed. She monitors employee activities as they relate to improper Internet usage, attempts to access unauthorized information, attempts to bypass or defeat access controls, and failures to follow security procedures relating to the work station and information. The appellant's activities are local in nature and affect the effectiveness and efficiency of established security programs at the center.

At Level 5-4, the work involves investigating and analyzing a variety of unusual security problems, questions, or conditions associated with general questions about security or in a specialty area, formulating projects or studies to alter existing security systems substantially, or establishing criteria in an assigned area of specialization (e.g., developing specifications for security programs in a number of data processing centers). The work affects security system

design, installation, and maintenance in a wide range of activities within the organization and in non-Government organizations.

Level 5-4 is not met. The appellant's work primarily involves investigating and analyzing a variety of conventional security problems and conditions related to implementing and monitoring a security program. Her work does not involve formulating projects or studies that result in substantial alteration of security systems. Projects and studies that result in significant impact on security programs are the responsibility of organizations at higher levels within her agency. The appellant's work affects AIS security activities at the center where she is employed and does not affect other organizations within her own agency or those in the private sector.

Level 5-3 is credited for 150 points.

Factor 6, Personal contacts

This factor includes face-to-face contacts and telephone and radio dialogue with persons not in the supervisory chain. The agency credited Level 6-2. We concur.

At Level 6-2, contacts are with persons from outside the immediate employing office or organization, but usually within the same Federal agency or a major component. Typical contacts at this level are project managers responsible for substantive subject-matter programs or their designated representatives, engineers, chemists, and other technical subject-matter specialists, program analysts, and other security specialists at various levels within the agency, in field or headquarters locations.

Level 6-2 is met. The appellant's contacts are with clinical, administrative, and management personnel throughout the medical center. These contacts include all personnel who require some degree of access to and use of the center's AIS to carry out their duties. The appellant also has contacts with security specialists at other medical centers, the VISN security specialist and other personnel, and personnel at the agency's headquarters. The majority of her contacts are with personnel who are outside of her immediate organization but within her agency.

At Level 6-3, contacts are with individuals from outside the agency who represent the security program interests of other Federal agencies, contractors, private business and financial interests, State and local governments, foreign governments, public and private educational institutions, or congressional offices. This level also includes contacts with applicants and potential contractors to discuss problems concerning the granting of security clearances.

Level 6-3 is not met. The appellant's regular and recurring contacts are with computer users throughout the medical center, and individuals involved with AIS security at varying levels within her own agency. The individuals contacted are concerned only with the AIS security program as it affects the agency's accomplishment of its mission and not the security program interests of other agencies or organizations as described at this level.

Level 6-2 is credited for 25 points.

Factor 7, Purpose of contacts

The purpose of personal contacts varies from factual exchange of information to situations involving significant or controversial issues and differing viewpoints, goals, or objectives. The agency credited Level 7-3.

At Level 7-2, contacts are made to resolve security issues and problems or carry out security plans and reviews to achieve mutually agreed upon security and program objectives. Typically, the employee has extensive contacts with program managers and personnel in staff support offices for the purpose of consolidating requests of components or segments of the organization into single or coordinated security plans and similar purposes which involve explaining and coordinating security program efforts.

Level 7-2 is met. Comparable to this level, the appellant's contacts are for the purpose of resolving security related issues and problems and ensuring that the center's AIS security program meets all pertinent regulatory requirements. Contacts are established to resolve matters involving security breaches, attempts to access unauthorized information, accessing inappropriate Internet sites, excessive bandwidth use that is not work-related, failure to protect passwords or log off properly, failure to properly protect sensitive data, etc.

At Level 7-3, the purpose of contacts is to persuade program managers and other decision-making officials, with widely differing goals and interests, to follow a recommended course of action consistent with established security policies, objectives, and regulations. These contacts are often in an advisory relationship for the purpose of briefing managers on program plans and levels of spending or to change program plans so that security systems may be applied to greater advantage.

Level 7-3 is not met. The appellant has contacts with management officials in decision-making positions to present findings, recommendations, and advising on matters related to establishing and implementing the center's AIS security program. However, the record shows that the work does not require persuasion to overcome conflicting goals and interests to get management officials to follow recommendations. The security program requirements are primarily driven by law and are generally followed by management officials. Decisions not to take a recommended course of action generally result from issues regarding cost effectiveness. The center Director has delegated authority to make decisions that a certain degree of risk is acceptable if the cost of mitigation is prohibitive.

Level 7-2 is credited for 50 points.

Factor 8, Physical demands

This factor covers the requirements and physical demands placed on the employee by the work assignment. The agency credited Level 8-1.

At Level 8-1, the work is sedentary and is usually accomplished while the employee is comfortably seated at a desk or table. Some walking, standing, and carrying of light objects are also involved.

At Level 8-2, the work requires regular and recurring physical exertion, such as long periods of standing, walking, bending, stooping, reaching, crawling, and similar activities. The work may regularly involve lifting and carrying moderately heavy of objects of 50 pounds or less

Level 8-1 is met. Comparable to this level, the appellant's work is primarily sedentary requiring a significant amount of time sitting at computer workstations. Unlike Level 8-2, the work involves limited walking during physical inspections of AIS equipment areas, and periods of standing when conducting training classes, and, occasional lifting of objects weighing up to 30 pounds.

Level 8-1 is credited for 5 points.

Factor 9, Work environment

This factor considers the risks and discomforts in the employee's physical surroundings or the nature of the work assigned and the safety regulations required. The agency credited Level 9-1.

At Level 9-1, the work is primarily performed in an adequately lighted, heated and ventilated office setting involving everyday risks or discomforts requiring observance of normal safety precautions.

At Level 9-2, the work is performed in settings in which there is regular and recurring exposure to moderate discomforts and unpleasantness that may require the use of special protective gear.

Level 9-1 is met. The appellant's work is primarily performed in offices, meeting and training rooms. Work areas are typically well-lit and climate controlled. The work does not involve exposure to elements comparable to Level 9-2.

Level 9-1 is credited for 5 points.

Summary

Factor	*Level*	*Points*
1. Knowledge required by the position	1-6	950
2. Supervisory controls	2-3	275
3. Guidelines	3-3	275
4. Complexity	4-3	150
5. Scope and effect	5-3	150
6. Personal contacts	6-2	25
7. Purpose of contacts	7-2	50
8. Physical demands	8-1	5
9. Work environment	9-1	5

Total	1885

A total of 1885 points falls within the GS-9 grade level point range of 1855 -2100 points on the Grade Conversion Table.

Decision

The appellant's position is properly classified as Information Security Specialist, GS-080-9.