U.S. Office of Personnel Management
Classification Appeal Decision
Under section 5112 of title 5, United States Code

Appellant: [Appellant's name]

Agency classification: Security Specialist
GS-080-11

Organization: [Appellant's organization/location]
Air Force Materiel Command
Department of the Air Force

OPM decision: Security Specialist
GS-080-11

OPM decision number: C-0080-11-01

//Judith A. Davis for

_____

Robert D. Hendler
Classification and Pay Claims
Program Manager
Merit System Audit and Compliance

9/12/2011

_____

Date

As provided in section 511.612 of title 5, Code of Federal Regulations (CFR), this decision constitutes a classification certificate which 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 5 CFR 511.605, 511.613, and 511.614, as cited in the *Introduction to the Position Classification Standards (Introduction)*, appendix 4, section G (address provided in appendix 4, section H).

Decision sent to:

[Appellant's name and address]

[Address of Appellant's servicing human resources office]

Chief, Civilian Force Policy
1040 AF Pentagon, AF-A1MR
Washington, DC 20330

Classification Oversight and Standardization
550 E Street East, Suite 1
Randolph Air Force Base, TX 78150-4451

Chief, Classification Appeals
Adjudication Section
Department of Defense
Civilian Personnel Management Service
1400 Key Boulevard, Suite B-600
Arlington, VA 22209-5144

Introduction

On February 28, 2011, Atlanta Oversight of the U.S. Office of Personnel Management (OPM) accepted a classification appeal from [Appellant's name]. On March 8, 2011, the appeal was transferred to Philadelphia Oversight for adjudication. The appellant's position is currently classified as a Security Specialist, GS-080-11, and is located in the [Appellant's organization/location] Air Force Materiel Command (AFMC), at [name of location] Air Force Base (AFB), [name of location]. The appellant believes his/her position should be upgraded to the GS-12 grade level. We received the complete agency administrative report (AAR) on March 21, 2011, and have accepted and decided this appeal under section 5112(b) of title 5, United States Code (U.S.C.).

To help decide the appeal, we conducted telephone interviews with the appellant on April 13 and 18, 2011, and his/her immediate supervisor on April 19, 2011. On April 27, 2011, and August 11, 2011, we also interviewed the Program Security Officer (PSO) of the AF Office of Special Investigations ([name of branch]) who is responsible for the program security management and execution of security policies and requirements for Special Access Programs (SAP) within AF and, on May 2011, we interviewed the Program Manager, [name of unit] who also serves as Assistant to the [name of unit] Commander for Special Programs. In reaching our classification decision, we have carefully considered all of the information obtained from the interviews, as well as the written information of record provided by the appellant and his/her agency.

Background information

The appellant states on December 12, 2004, he/she was promoted from a Security Specialist, GS-080-11, to Security Specialist, GS-080-12, position. On October 15, 2006, he/she was moved under the National Security Personnel System (NSPS) to a YA-080-02 position and, on June 21, 2009, he/she was reassigned within the pay band with an increase in base salary based on a management-directed reassignment. Due to the repeal of NSPS, on September 12, 2010, his/her position was converted to the General Schedule (GS) as a Security Specialist, GS-080-11.

The appellant states his/her duties increased when he/she was reassigned within the pay band and his/her position description (PD) of record at the time ([number]) was not accurate. Under 5 CFR § 9901.372(b) prior to converting an employee out of NSPS, an authorized management official must review the duties of the employee's current permanent position of record and classify the position's duties in accordance with the OPM classification standards. At the time of his/her movement out of NSPS, the agency reviewed the appellant's position but did not issue a GS PD. After his/her placement in the GS, the appellant submitted a classification appeal request to OPM through his/her servicing human resources office (HRO) and provided a draft PD with a proposed classification of Security Specialist, GS-080-12. He/she believed the draft PD was a more accurate reflection of the duties he/she was performing. To address the issue of PD accuracy, the servicing HRO conducted a desk audit. The appellant's current PD of record, [number], was developed as a result of the desk audit and, on October 21, 2010, was classified as a Security Specialist, GS-0080-11. The agency forwarded the appeal to OPM at the appellant's request.

General issues

Although his/her supervisor certified the accuracy of the appellant's PD in the appeal to OPM, the appellant certified PD [number] was not an accurate statement of the major duties and responsibilities assigned to his/her position. The appellant stated the draft PD he/she submitted with his/her appeal request provided a more detailed description of his/her duties and responsibilities. The agency stated the unclassified PD is not accurate since the duties and responsibilities the appellant performs are more narrow in scope and do not provide appropriate evidence to justify crediting Factor 2, Supervisory Controls with Level 2-5, Factor 4, Complexity with Level 4-5, or Factor 5, Scope and Effect with Level 5-4.

Our comparison of the duties described by the appellant during our telephone interviews with his/her during which he/she quoted extensively from the unclassified PD and his/her PD of record (PD [number]) revealed minor differences. The appellant places a greater emphasis on describing his/her duties which involve special access programs and information security program management. For example, the appellant stated he/she: (1) is the lead and technical authority for the [name of unit] staff offices special access and information security programs and executes and enforces all operational, functional, and mission assurance aspects of the programs; (2) is responsible for providing guidance and advice to program managers relating to industrial, personnel, physical, and operations security programs, as well as the [name of unit] Director, to ensure all security disciplines are fully "converged" from a policy and programmatic viewpoint to ensure overall information protection requirements meet mission requirements; (3) serves as the Government Special Security Officer (GSSO) and security advisor to the Capabilities Integration Director and the [name of unit] staff offices on the full spectrum of special access and information security matters; and (4) ensures the proper implementation of the security program, modifies it to meet individual and organizational needs, and ensures proper training is administered to all Directorate and [name of unit] staff offices.

The appellant's PD of record states he/she (1) independently or as a senior specialist, carries out multi-discipline security administration functions in support of day-to-day operations within the organization and develops local security procedures and operating instructions for the protection of classified materials; (2) implements and administers the information security program for assigned organizations; (3) manages the organization foreign disclosure and special access programs serving as the officer with primary responsibility for assigned nationally directed SAPs and advises the Center Commander/Director and staff, agency, representatives, contractors, and tenant activities on SAP programs, policies, procedures, and directives; and (4) manages the security education and training programs in support of collateral (all national security information classified Confidential, Secret, or Top Secret under the provisions of an Executive order for which special systems of "compartmentation" are not formally required) and special access programs that involve protection of classified information.

A PD must contain descriptive information about the major duties and responsibilities assigned to the position which, when supplemented by other information about the organization's structure, mission, and procedures, can be classified by one knowledgeable of the occupational field involved and the application of pertinent position classification standards (PCSs), principles, and practices. It is not meant to be a task list of every function performed. After

careful review, we find the appellant's PD of record, [number], meets the standards of PD adequacy for classification purposes as discussed in section III.E of the *Introduction* and we incorporate it by reference into our decision.

A PD 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 PD. Therefore, this decision is based on the work currently assigned to and performed by the appellant and sets aside any previous agency decision.

The appellant's supervisor, [name of branch], and Program Manager, Assistant to the [name of unit] Commander for Special Programs emphasized the appellant's outstanding competence and professionalism, stressing the quality of the appellant's performance. However, quality of work cannot be considered in determining the grade of a position (*The Classifier's Handbook*, chapter 5).

Position information

Based on the official PD and information of record, we find the following duties are being performed by the appellant.

The [name of unit] is one of three product centers in AFMC. Serving as the focal point for all AF armament, [name of unit] is responsible for the development, acquisition, testing, and deployment of all air-delivered weapons. [name of unit] applies advanced technology, engineering, and programming efficiencies across the entire combat capability to the war fighter. [name of unit] plans, directs, and conducts test and evaluation of U.S. and allied air armament, navigation and guidance systems, and command and control systems and supports the largest single base mobility commitment in the AF. The [name of unit] supports the [name of unit] through capabilities development, technology transition, enterprise management, and intelligence integration for creating expeditionary capabilities.

The appellant works under the supervision of the Chief, Business Operations of the [name of unit] as a senior specialist and technical authority for the [name of unit] staff office and support offices under the [name of unit] Commander. He/she advises and offers guidance to contracted security specialists and civilian personnel whose additional duties include security program responsibilities. The [name of unit] staff office consists of the Commander, lead civilian SES, executive officers, and executive planners. [name of unit] support offices consist of the program executive group; engineering; finance; judge staff advocate; contracting; ground, flight, and range safety; and Capabilities Integration Directorate. The appellant carries out day-to-day security administration functions advising the [name of unit] Commander, staff members, agency representatives, contractors, and tenant activities on SAP programs, policies, procedures, and directives. He/she interprets AF program directives to ensure compliance with national program guidance.

The appellant's functions include: revising and distributing clarifying program guidance, upon approval, as necessary; reviewing program plans for new and existing Development, Testing, and Evaluation (DT&E) programs and adjusting them to meet national security requirements; coordinating investigations with senior managers, investigators, and external contacts to address alleged security compromises or violations that take place within [name of unit] and staff offices; scheduling, conducting, and reviewing Operations Security (OPSEC) surveys; conducting formal security inspections, identifying program deficiencies, writing reports, briefing results, recommending corrective actions and verifying that appropriate action has been taken; administering security indoctrination and debriefings in support of special security programs; and ensuring all classified material is accounted for and destroyed as required by agency guidelines.

He/she develops required security briefings for new employee orientation and recurring training. The appellant also conducts reviews to ensure personnel are receiving all the security training and validates the training requirements. The appellant develops training curriculum and materials using national security and AF training policies and guidelines. He/she incorporates local requirements as needed. He/she reviews changes to agency-level policies and adjusts the existing training programs to ensure the most current information is provided to employees. The appellant conducts initial collateral and SAP training approximately six times per month in one-hour sessions. He/she also conducts quarterly collateral security training four times annually in one-hour sessions for over 250 personnel. Annual SAP refresher training is conducted four times per month in two-hour sessions for over 250 personnel. The appellant also conducts [name of serviced agency] training annually to over 250 personnel and on an as-needed basis to approximately eight personnel each month. He/she conducts Critical Nuclear Weapons Design Information Briefings approximately eight times per month in one-hour sessions and foreign travel briefings monthly on an as-needed basis in one-hour sessions.

He/she is responsible for implementing and administering the information security program. This includes developing local procedures to implement DoD, AF, and Major Command (MAJCOM) policies for the classification and protection of classified national defense and other sensitive information originated or controlled by [name of unit] activities, to include personnel access controls, need to know criteria, and physical storage and control procedures. He/she prepares all local guidance as directed within DoD and AF policy. The appellant resolves classification and declassification information issues and advises the appropriate technical personnel of any classification requirements for their programs or projects. He/she makes recommendations to resolve difficult situations complicated by conflicting or insufficient data that must be analyzed to determine if established methods are applicable, the need to deviate from normal methods and techniques, the need to temporarily waive security and investigative standards, or whether waivers can be justified. Waivers submitted by the appellant go through the [name of unit] Director for collateral issues or [name of branch] for SAPs and then submitted to the appropriate agency points of contact for approval or denial, e.g., [names of serviced agencies].

The appellant also reviews security incidents by determining if classified information was compromised and, if so, reports the incident to the [name of branch], Chief of Information

Security for collateral or PSO [name of branch] for SAPs. He/she then notifies and briefs the person who is responsible for the information involved in the incident (e.g. Commander, Director, or Program Manager); recommends an inquiry official to the person in charge, who approves the inquiry official based on the appellant's recommendation; briefs the inquiry official on how to conduct the inquiry; ensures the inquiry is completed within ten work days; and reviews the inquiry report for completeness as well as ensures the appropriateness of the recommendation(s) by the inquiry official, e.g., if classified material was compromised, what was the extent of the compromise and the circumstances surrounding it; concurs or non-concurs with the report and the recommendation(s) and briefs the person in charge. The person in charge then approves or disapproves the recommendation(s). If the recommendation(s) include the need for additional training, the appellant will provide it. If the recommendation(s) involve revocation of a security clearance, it is sent to PSO [name of branch] for further action. If no formal investigation is needed, the PSO [name of branch] for SAP or the [name of branch] Chief of Information Security for collateral closes the incident.

The appellant serves as the GSSO on all special access and information security matters providing SAP guidance, training, and direction to a civilian, military, and contractor work force at [name of unit] and [name of unit] staff organizations and locations and serves as the [name of unit] representative for all related information SAP security issues.

As a team member for the development of Security Classification Guides (SCG) and Program Protection Plans (PPP) at the [name of unit], the appellant advises team members, e.g., program managers, finance professionals, and engineers, on the security aspects of SCGs and PPPs. The appellant uses established regulations, and existing and previous SCGs and PPPs to determine what information can be used in the creation of protection guidelines. If this information is not adequate, the appellant uses knowledge gained from his/her security program background to decide how to best protect Critical Program Information (CPI) and consults with MAJCOM and [name of serviced agency]. SCGs include comprehensive guidance regarding the security classification of information concerning any system, plan, program, or project; the unauthorized disclosure of which reasonably could be expected to cause damage to national security. PPPs are single source documents used to coordinate and integrate all protection efforts designed to deny access to CPI to anyone not authorized or not having a need-to-know and prevent inadvertent disclosure of leading technology to foreign interests.

The appellant is the key advisor to the [name of unit] Commander on Sensitive Compartmented Information (SCI) physical, procedural, and TEMPEST (Emission Security, which ensures classified government networks have their information systems accredited by their local government Designated Approval Authority Representative), security matters. He/she interprets physical security policies for the [name of unit] and staff offices as well as reviews concepts of operations for proposed facilities and expansions or changes to existing facilities. He/she advises and assists staff members on the development of SCI facilities (SCIF) physical and TEMPEST construction and security plans in the form of pre-construction approval request packages, to include site analysis, layered security requirements, intrusion detection systems, and detailed security procedures for construction and post-construction periods. The appellant also conducts internal SAP and collateral inspections and assists with staff assistance visits, interprets

inspection results, provides on-the-spot guidance, and implements needed corrective actions in accordance with established guidelines.

He/she conducts surveys of industrial or other contractor-operated facilities to determine their ability to work with and store classified and sensitive information, to include information generated or stored in information technology (IT) systems. The appellant ensures clearance levels for company and management officials are commensurate with the information handled and assesses whether or not the classified and/or sensitive information can be safely held within the facility. Based on these reviews, he/she makes recommendations to [name of branch] concerning the ability of the contractor to administer an acceptable security program for accreditation. The appellant conducts periodic security reviews to examine whether the procedures, training, and facilities used by the contractors are in compliance with the requirements and terms of their security agreements practices for safeguarding classified material, and other security provisions. The appellant also orients contractors to the installation security program and advises them on measures necessary to bring their facilities up to established standards.

The appellant also implements and administers the personnel security program for SAPs. He/she ensures all requests for security clearances are properly screened and verified and all necessary forms have been completed and all documentation has been received prior to implementing the clearance process. The appellant analyzes each request to determine the validity of the access level indicated. He/she also evaluates the sensitivity of the position, degree of clearance, and special access required to perform the duties in order to determine which type of investigation is required. The appellant also reviews security clearance requests and similar related material for information that adversely reflects on the individual's loyalty or character, such as sabotage, espionage, or subversive tendencies, infamous or notorious conduct, drunkenness, or drug addiction. If the security investigation results reveal a misrepresentation of facts, he/she writes to [name of branch] summarizing any falsified or derogatory information.

Series, title, and standard determination

The appellant does not question the series or title of his/her position or the use of the position classification standard (PCS) for the Security Administration Series, GS-080 to evaluate his/her position and, based on the record, we concur. Based on the mandatory titling requirements of the GS-080 PCS, the appellant's position is allocated as Security Specialist, GS-080 since he/she performs work in more than two functional security areas other than in industrial security.

Grade determination

The GS-080 PCS uses the Factor Evaluation System (FES) under which factor levels and accompanying point values are assigned for each of the nine factors, with the total then being converted to a grade level by use of the grade-conversion table provided in the PCS. Under the FES, each factor-level description in a PCS 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 unless the deficiency is balanced by an equally important aspect that meets a higher 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, such as the steps, procedures, practices, rules, policies, theories, principles, and concepts; and the nature and extent of the skills needed to apply this knowledge.

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; interpreting new policy issuances for application in a variety of environments and locations; adjudicating complex personnel security clearances and/or developing guidelines for applying general criteria covering derogatory information that requires extensive experience and personal judgment to resolve; or planning and recommending the installation of multilayered security systems which may involve personnel access controls, physical protection devices, monitoring equipment, security forces, remote alarm equipment and other measures. 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; and serve 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.

At Level 1-8, employees having mastered a major area of security specialization or demonstrated mastery of general security administration programs, use a comprehensive knowledge of security policy requirements to function as technical authorities in assignments requiring the application of new theories and developments to security problems not susceptible to treatment by accepted security methods, technology, or procedures. In addition to mastery of the specialty area, employees at this level use knowledge of other security specialties in resolving major conflicts in policy and program objectives. Some employees use the knowledge at this level to perform key decision-making and policy-developing responsibilities in very difficult assignments such as planning for significantly new or far-reaching security program requirements, or leading or participating as a technical expert in interagency study groups for resolving problems in existing security systems and programs requiring innovative solutions.

The appellant's work meets Level 1-7. The appellant serves as the security officer for the [name of unit] staff offices and [name of unit] and applies security knowledge, regulations, and guidance in the areas of information, industrial, personnel, physical, and operations security as well as for collateral security, information, and technology which is protected up to SCI and SAP levels. Typical of this level, the appellant develops local procedures for each of these security specialties and levels based on higher level policies and directives. For example, the appellant developed operating instructions for the [name of unit] such as instructions for collateral

information, personnel, industrial and physical security procedures which included processes unique to [name of unit] and [name of unit]. The appellant develops training material and curriculum for the collateral security and operating security training program (initial training, quarterly security and operation security training) based on DoD and Air Force Instructions (AFI)s. Also similar to this level, the appellant is responsible for the security of a facility which is located within the [name of unit] that includes a Special Access Program facility (SAPF). Within the SAPF is a room that is authorized as a Sensitive Compartmented Information Facility (SCIF). SCIF and SAPF rules are different and the appellant must be knowledgeable of both policies and their interrelationships to determine and apply procedures for employee access to these facilities. Based on these policies, the appellant determines if an employee is authorized to enter the facility and applies established procedures for employee access. In addition, the appellant serves as a Tier 1 reviewer for access eligibility to SAP for the [name of unit]. The appellant uses judgment in interpreting the guidelines identified in the [agencies serviced by the appellant] 6/4, Special Access Program Tier Review Process, but must adhere to the step-by-step process provided. He/she scrutinizes candidate responses to items identified on the Standard Form-86 (SF-86), Questionnaire for National Security Positions, against the [names of serviced agencies] 6/4 and is authorized to interview candidates to clarify the record when there is insufficient data or when omissions occur. He/she formulates non-leading questions to gather information for clarification. Typical of security adjudication at Level 1-7, the appellant must determine if the candidate's personal and professional history indicates loyalty to the U.S. and if the candidate has the strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment to be granted access to SAP. The appellant has the authority at the Tier 1 level to determine if the candidate would be eligible for final access approval but cannot deny eligibility access. If the appellant determines the candidate does not meet the Tier 1 adjudication standard, the candidate's access eligibility package is forward to the Tier 2 level reviewer for further review. If the appellant determines eligibility to SAP, he/she forwards his/her recommendation through the PSO [name of branch] to the approving official, e.g., HQAF.

Typical of Level 1-7, the appellant conducts a site survey of a new SAPF for physical security program requirements using guidance from the [agencies serviced by the appellant] 6/9, Physical Security Standards for Special Access Program Facilities. Using an in-depth knowledge of these standards, he/she checks the room to determine if it meets standards, such as confirming the thickness of the walls, duct systems are within requirements, conduits have baffles, and conduits have rubber pipe breaks. He/she uses his/her knowledge of alarm systems to determine which type is needed based on whether it is a secure room, SCIP, or SAPF. The appellant instructs contractors through civil engineering (CE) on how to meet program specifications by writing a Statement of Objectives (SOO) and a Statement of Work (SOW). He/she monitors the contractor's work for proper thickness of walls, appropriate sound attenuation (such as baffles in ducts over 96 inches and white noise installation), and if balance magnetic switches for alarm systems and motion detectors (Intrusion Detection Systems) are installed to cover the entire area needing protection from intrusion, the appellant takes photographs to ensure compliance. He/she ensures a 128-bit encryption system is placed in alarm systems for SCIP or SAPF facilities and instructs the [name of branches] to create new alarm accounts for them. Once the appellant completes the [names of serviced agencies] 6/9 checklist, he/she submits it to [name of branch] (PSO) for approval. Once approved, [name of branch] will accredit the facility to operate at the SAP level. After accreditation, the appellant creates an SOP and ensures its adherence. The

appellant will also conduct an annual compliance inspection of the SAPF using [agencies serviced by the appellant] guidance. In addition, the appellant serves as a working group member for the development of SCGs and PPPs. The appellant uses established regulations, program knowledge, and existing and previous SCGs and PPS to determine what information can be used in creating protection guidelines. He/she coordinates with MAJCOM, local engineers, and program managers to ensure all CPI is identified and protection measures are in place to prevent inadvertent disclosure. If no current information exists, the appellant uses program knowledge to decide how to best protect CPI, consults with MAJCOM and [name of branch] to confirm his/her decisions, and ensures the guides conform to security standards. As at Level 1-7, the level of knowledge required to administer these security functions and understand their interrelationships is paramount.

Level 1-8 is not met. The appellant states his/her position requires his/her to "demonstrate a complete mastery of special access, information, personnel, and industrial security fields that are necessary to provide effective guidance, training, and direction to [name of unit] level organizations, activities, and units." In order to meet Level 1-8, employees rely on their vast knowledge or "mastery" of security issues in order to assist them with developing new policies to combat new potential security threats within the organization. In contrast, as at Level 1-7, the appellant uses his/her knowledge of security issues to develop local standard operating procedures (SOPs). He/she is considered the local technical security authority interpreting policy and making decisions involving policy application of established methods, equipment, and techniques from multiple sources. However, the appellant must adhere to the stringent DoD and AF policies and guidelines. Working at an operating-level AF installation, the appellant is not tasked with and is not delegated the authority to perform key decision-making and policy-developing responsibilities such as planning for significantly new or far-reaching security program requirements, or leading or participating as a technical expert in interagency study groups for resolving problems in existing security systems and programs requiring innovative solutions to resolve major conflicts in policy and program objectives, which are required for assignment of Level 1-8. In addition, the appellant's duties do not include advising top level agency security and subject-matter managers on new developments and advances in security techniques in the specialty area; planning organizing, and directing studies to develop long range (e.g., 5-10 years) studies and forecasts; recommending methods for enhancing efficiency of security systems through modifications and applications of evolving technology; evaluating and making recommendations concerning overall plans and proposals for major agency and interagency security projects; and implementing national level guidance in agency standards, guidelines, or policies for major security programs. These duties are performed by security personnel in positions found at higher AF program levels.

This factor is evaluated at Level 1-7 and 1250 points are assigned.

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.

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 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.

At Level 2-5, the supervisor provides broad administrative and policy direction through discussions of financial and program goals and national, agency, and local security policies affecting the direction of the security program. In performing the work, the employee makes extensive unreviewed technical judgments concerning the interpretation and implementation of existing security policy for the assigned specialty area(s) and in deciding which analytical and technical decisions lead to, or form the basis for, major security program policy and operational decisions by top management. The employee is regarded as a leading technical authority for the employing organization in a security specialization or over a wide range of interrelated security programs. The supervisor usually accepts the employee's recommendation without change.

Like Level 2-4, the appellant's supervisor sets the overall objectives and decides what available resources may be used. The appellant's supervisor reviews his/her work products quarterly by sampling his/her most visible projects. His/her supervisor is ultimately responsible for the development, execution, and direction of security policies, budget, and long-range operating program goals and objectives. The supervisor retains responsibility for the approval of the expenditure of allocated funds and exercises the final authority for the full range of administrative, personnel, and management actions and decisions made. The appellant is responsible for overseeing the status of funds and the scheduling rate of projects. The appellant advises and offers guidance to contracted security specialists and civilian personnel whose additional duties include security program responsibilities. His/her effectiveness in meeting objectives and achieving expected results are based on discussions with his/her supervisor. These supervisory controls are consistent with level 2-4.

Level 2-5 is not fully met. The appellant functions with the level of independence found at Level 2-5 in that the his/her supervisor considers the appellant to be a subject-matter expert on security issues and states as the Chief Financial Officer he/she does not have the expertise in security and relies on the appellant's knowledge of security to carry out assignments with a high degree of technical independence. However, the record shows the appellant does not function under the broad level of delegated authority required to meet Level 2-5. The appellant needs approval from [name of branch] prior to implementing local procedures. Although the appellant evaluates the workload and directs security contractors and civilian personnel on what sub-tasks to accomplish on his/her behalf, the appellant's supervisor sets the program's objectives. In addition, the appellant's program responsibilities are restricted to the operating level which must operate within tightly defined program parameters as previously discussed. They do not involve

a broad delegated authority which would impact the development of new or revised security policies, procedures, and controls in terms of impact on subject-matter program goals and objectives, and national security priorities. These programmatic functions are performed at higher levels in the AF.

This factor is evaluated at Level 2-4 and 450 points are assigned.

Factor 3, Guidelines

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

At Level 3-3, guidelines available and regularly used in the work are in the form of agency policies, 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 directives. The guidelines are not always applicable to specific conditions or there are gaps in specificity in application to specific security system requirements. This level also includes work situations in which the employee must interpret and apply a number of subject- matter policies and regulations such as those that apply to access to and protection of classified information. The employee analyzes the applicability of guidelines to specific circumstances and proposes regulatory or procedural changes designed to improve the effectiveness or efficiency of security controls within the intent of directions concerning the level of security required.

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; interagency security program policy proposals requiring refinement and coordination; or others that are not specific in how they are to be defined, implemented, and monitored. At this level, the employee exercises a great deal of personal judgment and discretion with broad latitude for interpreting and applying guidelines across the organization. Also included at this level is the interpretation and application of guidelines of more than one Federal agency or department which apply to security programs and organizations involved in joint responsibility control, and operations, or discrete projects at a single facility.

Like Level 3-3, the appellant uses guidelines which are vast and cover nearly all aspects of work performed in multiple security administration disciplines. The appellant is required to interpret, adapt, and apply existing guidelines. He/she is responsible for developing local instructions and procedures to supplement agency guidelines and updates them when revised policies are issued. Comparable to Level 3-3, some guidelines used by the appellant may be broad in nature and have gaps in the specificity in their application to specific security system requirements. Based on the multitude of guidelines available, the appellant must interpret and apply a number of subject-matter policies and regulations such as those that apply to assessing and protecting classified information. For example, the appellant is required to interpret and apply SAP,

collateral, information, personnel, industrial, OPSEC, and SCI security procedures. The appellant uses the [name of serviced agencies], DoD instructions, AFIs, and other Federal agency's guidance, e.g., [names and locations of serviced agencies], to resolve issues brought to his/her by engineers and program managers on how to protect classified briefings, documents, electronic media, etc. The appellant prepares and presents security training based on established guidelines and policies. Like Level 3-3, as a Tier 1 reviewer, the appellant uses judgment in interpreting guidelines identified in the [name of serviced agencies] 6/4, Special Access Program Tier Review Process; however, he/she must adhere to the step-by step process.

Unlike Level 3-4, 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 the appellant uses to perform his/her work specifically defines areas to be addressed and methods to be employed in implementing the security program and to protect sensitive information for [name of unit] staff offices and the [name of unit]. Although the appellant develops the content for local SOPs, they must be approved by [name of branch]. The appellant is not allowed to deviate from issued guidance without requesting a waiver and approval from higher levels within the organization.

This factor is evaluated at Level 3-3 and 275 points are assigned.

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.

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. Typically, such assignments 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, conclusion, or recommendations. Programs and projects may be funded by, or under the cognizance of 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.

At Level 4-5, employees perform assignments involving various projects, studies, or evaluations requiring the application of many different and unrelated processes, differing regulatory criteria and procedures, and significant departures from established practices, to reach decisions, or to develop and implement new methods and techniques that satisfy policy and operational requirements. At this level, the employee makes recommendations for changes to basic policy issuances and for implementing instructions covering established security techniques, practices,

and methods based on personal analysis of very general policy directives and objectives. An example of work at this level would be interpretation and implementation of new directions for subordinate organizations and field units, when such directions stem from additions to, or changes, in national or agency policies and programs, or identification of deficiencies in established programs.

Like Level 4-4, the appellant's assignments consist of a variety of security duties involving many different and unrelated processes and methods. For example, the appellant is responsible for the security planning and implementation aspects of collateral classified and unclassified briefings/conferences for up to 500 attendees and SAP meetings for up to 50 attendees. Based on guidance, AFI 31-401 for collateral and [names of serviced agencies] for SAP, the appellant uses various security procedures, processes, guidelines, and techniques to ensure proper security procedures are followed. In developing the security plans, the appellant surveys the conference site to detect possible security issues within the facility where the conference/briefing will take place if the site has not been previously approved for holding classified discussions. The site survey may include reviewing blueprints to analyze the room size and perimeters for unsecure areas. If a security issue is found, the appellant would coordinate with other personnel, e.g., engineers, to bring the facility into compliance. The appellant verifies conference/briefing attendees and presenters possess all required security clearances; coordinates with other components to schedule additional needed resources, e.g., military police officer and dog; and review presenter(s) classified briefing(s) to ensure they contain all proper markings and classification levels. In addition, the appellant uses the [names of serviced agencies] 6/0, DoD instructions and AFIs to resolve issues when approached by engineers and program managers on how to protect classified briefings, documents, and electronic media. If there is a complex issue, i.e., sending briefings to multiple contractors, the appellant must verify the contractor's Commercial and Government Entity (CAGE) code to determine if they can receive classified information at their facility. The appellant checks the Air Force Access Database System (AFADS) to verify if the contractors are program-briefed. If they cannot receive classified information or they have not been briefed, the appellant instructs the contractor on how to apply for facility clearance by directing them to a Defense Security Service (DSS) representative. If the contractor needs to be briefed on a program, the appellant instructs the program manager on procedures for submitting an access request that the appellant would approve and forward to [name of branch] PSO followed by [branch serviced by appellant] personnel.

Level 4-5 is not met. At this level, work assignments involve originating new security techniques, establishing criteria, or developing new information and approaches to develop solutions. This is not descriptive of the duties the appellant performs on a regular and recurring basis. He/she may adapt required checklists due to changes in technology; request a waiver to policy or procedures; or adapt situations to meet policy requirements. However, the appellant does not have the authority to develop broad security policies and regulations which require consideration of the total range of existing policies, procedures, laws, and regulations and the program goals and objectives which are to be fulfilled, which is required to meet Level 4-5. Writing security policies and regulations is retained at the DoD and AF headquarters levels. The appellant's work assignments do not include making significant departures from established practices, or developing and implementing new methods and techniques that satisfy policy and

operational requirements, but rather making decisions based on established security criteria, methods and techniques.

This factor is evaluated at Level 4-4 and 225 points are assigned.

Factor 5, Scope and effect

This factor covers the relationship between the nature of the work; i.e., the purpose, breadth, and depth of the assignment, and the effect of work products or services both within and outside the organization. Effect measures whether the work output facilitates the work of others, provides timely service of a personal nature, or impacts the adequacy of research conclusions. The concept of effect alone does not provide sufficient information to properly understand and evaluate the impact of the position. The scope of the work completes the picture allowing consistent evaluations, and only the effect of properly performed work is considered.

At Level 5-3, the work involves resolving a variety of conventional security problems, questions, or situations, such as those 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, although some programs may be part of multi-facility or nationwide program operations with interlocking security requirements.

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, in providing solutions to security problems and questions, and in developing alternatives and options that are designed to meet requirements in a variety of physical and environmental circumstances. Recommendations and technical interpretations affect the level of funding required to meet program objectives in conducting major substantive or administrative programs or services. Program and project proposals frequently cut across component or geographic lines within the agency, and may also affect the budgets, programs, and interests of other Federal agencies or organizations, public organizations, and/or private industrial firms.

Level 5-3 is met. The appellant's work involves resolving conventional security problems and issues. He/she monitors the implementation of an established security program at the center by conducting risk assessments, ensuring the appropriate personnel sensitivity level designations are granted, and ensuring that employee access to system information is limited to that related to the work performed. He/she also develops and delivers security briefings for new employee orientation and recurring training, as well as serving as a team member in developing SCGs and

PPPs, and conducting facility surveys. The appellant's work is primarily local in nature and affects the effectiveness and efficiency of the established security programs at the center.

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. His/her work does not involve formulating projects or studies that result in a substantial alteration of security systems. Although the appellant makes recommendations to senior leadership and has the authority to request waivers to policy and/or procedures, projects and studies that result in a significant impact on security programs are the responsibility of organizations at higher levels within the agency. The appellant's work affects security activities primarily within the [name of unit] staff offices and [name of unit] but also affects contractors located in other geographical areas (e.g. Midwest and Pacific coast states). Although the work has a similar geographic impact beyond the immediate installation like Level 5-4, it has a lesser programmatic impact in that it does not regularly result in substantive additions or alterations to existing security systems or operations. Similar to Level 5-3, he/she provides guidance to each contractor's Contractor Program Security Officer (private-sector counterpart) by ensuring their facilities meet established security classification specifications for working with and storing classified and sensitive information.

The factor is evaluated at Level 5-3 and 150 points is assigned.

Factor 6, Personal contacts

Personal contacts include face-to-face and telephone contacts with persons not in the supervisory chain. Levels described under this factor are based on what is required to make the initial contact, the difficulty of communicating with those contacted, and the setting in which the contact takes place.

At Level 6-2, contacts are with persons from outside the immediate employing office or organization but usually within the same Federal agency or major component thereof. Typical of 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. Roles and relative authorities of participants are explicit.

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 institutions (e.g., colleges and universities), or congressional offices. Contact with applicants and potential contractors to discuss problems concerning the granting of security clearances are also included at this level. Contacts take place in a moderately unstructured setting (e.g., 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 during the course of the contact). Also characteristic of this level are contacts with the head of the employing agency, key officials of comparable rank and authority in other agencies, or the staff of national security agencies. Contacts normally take place at formal security briefings, deliberations, conferences, or negotiations which are arranged well in

advance. Attendance at interagency committee meetings as a resource person (i.e., to provide technical security information about specific programs) is included at this level.

Like Level 6-2, the appellant's contacts are with persons from outside the immediate employing office or organization but mostly within the same Federal agency, where the roles and relative authorities of the persons contacted are explicit. The appellant's primary contacts are with staff from within various AF activities, which include [name of branch] agents, GSSOs, and Contractor Special Security Officers at other AF bases.

Level 6-3 is not met since the appellant's contacts are much more limited than is expected at this level. Although he/she has occasional contacts with other Federal agencies, to include the [name of serviced agency], and contractors, his/her dealings with these contacts take place in a structured setting and the role of each party is known in advance. The appellant has no contact with top officials at the AF or other agencies. Like Level 6-2, the appellant's contacts are primarily with AF staff.

This factor is evaluated at Level 6-2 and 25 points is assigned.

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 same contacts selected for crediting Factor 6 must be used to evaluate Factor 7.

At Level 7-2, contacts are made for the purpose of resolving security issues and problems or for carrying 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. Such contacts may also include those with managers and employees in contractor facilities to plan and coordinate inspections, provide advice, and resolve security issues.

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. This level is exemplified by contacts with managers, often in an advisory relationship, for the purpose of briefing them on program plans and levels of spending or to change program plans so that security systems may be applied to greater advantage. Also covered at this level are contacts such as hearings and interviews to discuss and resolve derogatory or potentially derogatory information that may affect the ability to grant security clearances. At this level, persuasion and negotiation are necessary due to the presence of conflicting security, budgetary, and program objectives which must be resolved. Some employees present, explain, and defend controversial security policies and regulations at meetings and conferences with officials at higher levels of security program responsibility, and/or with officials from other agencies and private companies.

Like Level 7-2, the appellant's contacts are for the purposes of resolving security issues and problems or for carrying out security plans and reviews to achieve mutually agreed upon security and program objectives. Similar to Level 7-2, the appellant's duties include verifying security levels, serving on working groups, conducting training and briefings, interviewing candidates for SAP clearance, and making recommendations and advising personnel on the interpretation of policy.

Level 7-3 is not met. The appellant's contacts are not with program managers and other decision-making officials with widely differing goals and interests, but with officials with similar goals and interest. He/she does not brief managers on their program plans, levels of spending or changes to program plans. Similar to Level 7-3, the appellant conducts interviews to discuss and resolve derogatory or potentially derogatory information that may affect the ability to grant security clearances. However, these interviews are held with affected employees to obtain clarifying information on the results of background checks performed during the Tier 1 process, not with decision-making officials as needed at Level 7-3. Since background checks with conflicting security information are forwarded to a Tier 2 reviewer for further action, the appellant's actions on these matters do not require the exercise of persuasion or negotiation found at Level 7-3.

This factor is evaluated at Level 7-2 and 50 points are assigned.

Factor 8, Physical demands

This factor covers the requirements and physical demands placed on the employee by the work assignment. This includes physical characteristics and abilities, e.g., specific agility and dexterity requirements, and the physical exertion involved in the work, e.g., climbing, lifting, pushing, balancing, stooping, kneeling, crouching, crawling, or reaching. To some extent the frequency or intensity of physical exertion must also be considered, e.g., a job requiring prolonged standing involves more physical exertion than a job requiring intermittent standing.

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 and standing may occur in the course of a normal workday in connection with travel to and attendance at meetings and conferences away from the work site.

At Level 8-2 requires regular and recurring physical exertion, such as long periods of standing, walking, or bending or requires recurring lifting of materials of moderate weight (under 50 pounds).

Level 8-1 is met. The appellant's duties require exertion typical of an office setting. The appellant's work may involve minor physical exertion, e.g., walking through rooms during inspections, and utilizing ladders to check pipes and ceilings. The physical characteristics and exertion requirements are minimal for this position and meet the intent of Level 8-1. The appellant's position does not meet Level 8-2.

This factor is evaluated at Level 8-1 and 5 points are assigned.

Factor 9, Work environment

This factor considers the risks and discomforts in an employee's physical surroundings, or the nature of the work assigned and the safety regulations required.

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.

This factor is evaluated at Level 9-1 and 5 points are assigned.

Summary

	Factor	*Level*	*Points*
1.	Knowledge Required by the Position	1-7	1250
2.	Supervisory Controls	2-4	450
3.	Guidelines	3-3	275
4.	Complexity	4-4	225
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 Points		2,435

The total of 2,435 points falls within the GS-11 range (2,355 – 2,750) on the 080 JFS grade conversion table.

Decision

The appellant's position is properly classified as Security Specialist, GS-080-11.