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

Appellant:	[name]
Agency classification:	General Supply Specialist GS-2001-9
Organization:	[office] [installation] Defense Logistics Agency [city and State]
OPM decision:	Physical Security Specialist (Parenthetical title at agency discretion) GS-080-9
OPM decision number:	C-0080-09-04

/s/ Kevin E. Mahoney
Kevin E. Mahoney
Deputy Associate Director
Center for Merit System Accountability

8/8/06
Date

As provided in section 511.612 of title 5, Code of Federal Regulations, this decision constitutes a classification 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 the 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 changes the classification of the appealed position, it is to be effective no later than the beginning of the fourth pay period after the date of this decision (5 CFR 511.702). The servicing human resources 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]

[Servicing human resources office]

Executive Director
Human Resources
Defense Logistics Agency
8725 John J. Kingman Road, Suite 3630
Fort Belvoir, Virginia 22060-6221

Ms. Janice W. Cooper
Chief, Classification Appeals
Adjudication Section
Department of Defense
Civilian Personnel Management Service
1400 Key Boulevard, Suite B-200
Arlington, Virginia 22209-5144

Introduction

On March 3, 2006, the San Francisco Field Services Group of the Center for Merit System Accountability, U.S. Office of Personnel Management (OPM), accepted a position classification appeal from [appellant], who occupies a General Supply Specialist, GS-2001-9, position in the [office] at [installation], [program component], Defense Logistics Agency, in [city and State]. (The appeal was subsequently transferred to the Center's Washington, DC, office.) [Appellant] requested that her position be classified as GS-391-11 or GS-2210-11. We accepted and decided this appeal under the provisions of section 5112 of title 5, United States Code.

We conducted a telephone audit with the appellant on May 22, 2006, and a subsequent telephone interview with her supervisor, [name]. We also interviewed other work contacts of the appellant to obtain information pertinent to her appeal. We decided this appeal by considering the audit findings and all other information of record furnished by the appellant and her agency, including her official position description [number] and other material received in the agency administrative report on March 24, 2006.

General issues

To support her request for reclassification, the appellant submitted position descriptions (PDs) for two positions, a Communications Security Specialist, GS-391-12, at the Department of the Army, Pentagon Information Technology Services, in Washington, DC, and an Information Technology Specialist (Network), GS-2210-11, at Tracy Defense Depot, and a vacancy announcement for a Telecommunications Specialist, GS-391-12, at the Department of the Army, Fort Belvoir, Virginia. She stated that these positions include duties similar to hers.

By law, we must classify positions solely by comparing their current duties and responsibilities to OPM standards and guidelines (5 U.S.C. 5106, 5107, and 5112). Since comparison to standards is the exclusive method for classifying positions, we cannot compare the appellant's position to others as a basis for deciding her appeal. However, our review of the documents she submitted does not support her contention that these other positions are essentially similar to hers.

The GS-391-12 position at the Pentagon is described as being responsible for planning, developing, coordinating, and directing those aspects of the communications security (COMSEC) program related to information security for all supported agencies within the Pentagon. This includes such duties as developing plans and programs to manage and ensure the availability of COMSEC assets, preparing and issuing COMSEC manuals and instructions, preparing internal operating procedures and work standards for support personnel, inspecting daily COMSEC transaction records, serving as COMSEC custodian, evaluating customer needs and identifying and acquiring COMSEC hardware and software for cryptonets based on system/circuit requirements, providing technical assistance and problem resolution and overseeing the application of modifications, establishing cryptonets for Pentagon secure circuits/nets, and performing controlling authority duties for over one hundred cryptonets worldwide requiring continuous net surveys and problem solving regarding insecurities/compromises, cryptonet expansion and deletion, and other required maintenance.

This PD encompasses some duties that correspond to those performed by the appellant, specifically the COMSEC custodian function and some aspects of those duties associated with operational cryptonet control. However, these duties are performed within the context of a broader information security assignment than performed by the appellant. The work requires knowledge of cryptonet planning, data administration and control, and user hardware, software, communications, and other components of the operational environment to develop and modify information architectures based on technical requirements and system capabilities. In other words, the position requires in-depth technical knowledge of the characteristics and operational capabilities of telecommunications systems and devices, presumably to evaluate, select, and install hardware and software. The appellant's position requires only a familiarity with the items in her account in terms of their general purposes and compatibilities. In addition, this position has cryptonet control functions on a much greater scale than the appellant, with over one hundred cryptonets requiring continuous monitoring and problem solving. This position appears to serve as an overall COMSEC manager subsuming the more limited COMSEC custodian duties. Although positions at varying grade levels and in different series may share isolated duties, positions are classified based on the totality of their work. This GS-391-12 position, as depicted in the position description, includes work and knowledge requirements that are well beyond the scope of the appellant's position.

Similarly, the vacancy announcement for the GS-391-12 position at Fort Belvoir includes COMSEC custodian duties. However, the primary function of the position appears to be the development of communications security operating procedures. Beyond that, the description of duties in the vacancy announcement is too cursory for any further observations.

The GS-2210-11 position serves as a network administrator with such duties as defining network requirements, configuring and optimizing the network, establishing connectivity between remote sites; monitoring installation and maintenance of all networking equipment; studying the volume and distribution of network traffic; integrating network systems with existing or planned network infrastructure; creating network maps; configuring hubs, switchers, and routers; installing and testing hardware and software fixes and upgrades; and other related duties requiring knowledge of information technology and skill in network system design, development, installation, testing, and maintenance. The appellant offered no explanation for how she believes this GS-2210-11 position is similar to hers. There would appear to be no resemblance between her duties and those of this technical IT specialist position.

The appellant also believes that her position warrants a higher grade because, in part, it requires a high-level security clearance. However, the security clearance associated with a position does not have a direct bearing on the position's grade. The security clearance required for a position relates solely to the degree of access the employee has to classified information or material. This access may occur in any capacity, ranging from high-graded analytical work to low-graded clerical functions. The level of clearance required is independent of the position's grade. The grade of a position, on the other hand, is based on the difficulty and complexity of the work performed, regardless of whether or not that work is of a sensitive nature.

Position information

The appellant serves as a COMSEC custodian for an account containing over 2400 items of equipment, supplying COMSEC material to supported offices within the Department of

Defense (DoD). These COMSEC items consist of various types of encryption equipment designed to provide telecommunications security by converting information to a form unintelligible to unauthorized interceptors and by reconverting such information back to its original form for authorized recipients. Approximately half of the items in the appellant's account are keying materials classified at the Secret and Top Secret levels. The responsibility of a COMSEC custodian is to assume accountability for this equipment or material upon receipt and control its dissemination to authorized individuals. The duties of a COMSEC custodian are prescribed by the National Security Agency (NSA), which develops and issues requirements governing all Federal communications security equipment and operations. These duties encompass the receipt, custody, issuance, safeguarding, accounting, and destruction of COMSEC material and include: controlling and safeguarding all material charged to the COMSEC account and limiting access to individuals having the proper clearance and need-to-know; ensuring that the appropriate COMSEC material is readily available to authorized individuals, making shipping arrangements, properly packaging the material for shipment, and issuing the material on hand-receipt; examining all shipments received for signs of tampering; accounting for the location of every item of accountable COMSEC material in the account, maintaining records, and submitting required paperwork and reports to NSA; performing routine destruction or other disposition of COMSEC material as directed; and reporting any known or suspected compromises involving COMSEC material to NSA.

The appellant has certain ongoing control responsibilities for the COMSEC keying materials used to enable a DLA-based cryptonet. Her duties in this capacity have included procuring the keying material from NSA and maintaining an inventory to ensure availability; keeping a database to track the location, users, and linkages of the keys and their supersession dates; obtaining and distributing replacement keys as needed; and disseminating software updates. For evaluation purposes, these duties are functionally similar to the COMSEC custodian duties described above, although they have additional requirements associated with monitoring, storing, and accounting for the items.

This is intended only as a brief summary of the major duties performed by the appellant. The PD and other material submitted in conjunction with the appeal provide more detailed information on the appellant's duties and responsibilities, all of which were considered in this evaluation.

Series and title determination

The appellant's position has some common characteristics with the General Supply Series, GS-2001, to the extent that her work involves ordering and acquiring equipment. However, the primary knowledge requirements and focus of her position relate not to the supply processes involved in procuring the equipment but to the controls and accounting associated with safeguarding the equipment. This work is specifically referenced in the position classification standard for the Security Administration Series, GS-080, under its discussion of "specialized security assignments" as follows:

> In organizations housing classified communications centers, or organizations which store classified communications materials, security specialists are sometimes designated as cryptographic custodians (this function may also be

> assigned to subject-matter employees) or cryptographic security officers. The cryptographic security function involves developing, implementing, and monitoring security systems for the protection of controlled cryptographic cards, documents, ciphers, devices, communications centers, and equipment. This is often a collateral duty or, in major communications centers can be a full-time responsibility. Other than the special control documents used and the accounting records that must be maintained, much of this work involves physical security practices adjusted to cryptographic protection requirements.

Thus, although COMSEC custodians may be co-located with supply organizations for logistical purposes, the function itself is directly associated with the GS-080 occupation.

The appropriate title for GS-080 positions of this nature is Physical Security Specialist. The agency may supplement this prescribed title by adding a parenthetical title to further identify the duties and responsibilities involved, e.g., (COMSEC Custodian).

The appellant does not perform the type of work that would support classification of her position to the Telecommunications Series, GS-391. At the operating level, the GS-391 series includes technical and analytical work related to the planning, development, acquisition, testing, integration, installation, utilization, or modification of telecommunications systems, facilities, and services. At the staff level, it includes work involved with the planning, implementation, or management of telecommunications programs, systems, or services. In either case, telecommunications work requires an understanding of electronic communications concepts, principles, practices, policies, standards, and operational requirements, *and* a technical knowledge of the operational and performance characteristics of communications equipment, automated control and network management systems, transmission media, and the relationship among component parts of telecommunications systems. Telecommunications employees must be able to understand, evaluate, and translate the needs of communications users into requirements; relate user requirements to existing technology, system capabilities, available technology and services, terms and conditions of systems and service contracts, equipment and staffing requirements, costs and funding, and other supporting services required; and identify, direct, or coordinate the actions required to provide needed services.

The appellant's role as a COMSEC custodian is limited to acquiring and distributing specified telecommunications equipment and items for the supported customers. She is not required to have an in-depth knowledge of telecommunications technology in order to independently plan, develop, select, and install telecommunication systems and services. She has some limited knowledge of the operating characteristics of certain items of equipment, sufficient to perform minor maintenance and ensure compatibility among components; but this falls far short of the broad technical knowledge required by the GS-391 series.

Likewise, the appellant's position is not classifiable to the Information Technology Management Series, GS-2210. The GS-2210 series covers work involved with the development, administration, management, and delivery of information technology (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., computer systems analysis, applications software design, network system development. Computers have become a universal tool in the Federal workplace, and there are few occupations that do not involve either processing information or

transacting business electronically. However, the GS-2210 series is not intended for IT users but rather for IT workers; i.e., those employees who actually develop and maintain the IT systems used by other functional specialists. The appellant *uses* IT technology such as the Internet, but does not *design, develop, or administer* that technology.

It should be noted, in those cases where the COMSEC custodian function is a collateral duty of a position or constitutes only a portion of a broader assignment, the series of that position may be controlled by the other duties performed. Thus, some COMSEC custodian positions may be classified to the GS-391 series or to various other subject-matter series because those custodian functions comprise only part of the position's overall duties. In such a case, the position's grade may be based wholly on the other duties that constitute the primary purpose of the position.

Grade determination

The position was evaluated by application of the criteria contained in the position classification standard for the Security Administration Series, GS-080. This standard is written in the Factor Evaluation System (FES) format, under which factor levels and accompanying point values are to be assigned for each of the following nine factors, with the total then being converted to a grade level by use of the grade conversion table provided in the standard. The factor point values mark the lower end of the ranges for the indicated factor levels. For a position to warrant a given point value, it must be fully equivalent to the overall intent of the selected factor-level description. If the position fails in any significant aspect to meet a particular factor-level description, the point value for the next lower factor level must be assigned, unless the deficiency is balanced by an equally important aspect that meets a higher level.

Factor 1, Knowledge Required by the Position

This factor measures the nature and extent of information an employee must understand in order to do the work, and the skills needed to apply that knowledge.

The knowledge required by the appellant's position matches Level 1-6. At that level, work requires practical knowledge of the criteria, equipment, or techniques for at least one area of security specialization to perform limited independent work. The assignments require some application of judgment in the use of security knowledge and 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. The work at this level includes such duties as:

- Advising facility security personnel on matters involving clear-cut explanations of regulations and procedures.

- Determining eligibility for access to classified or sensitive information and granting personnel security clearances/accesses in the presence of minor derogatory information.

- Inspecting facilities where security processes and methods are known to the employee, security programs are operated effectively, and there is no history of significant violations and deficiencies.

This level describes work comparable to the duties performed by the appellant. It depicts fairly narrow security assignments where the work is well-defined, involves carrying out established processes, and requires considering and weighing factual information, such as cost, access restrictions, and equipment availability. At this level, the work requires knowledge of clear-cut regulations and procedures directly related to the security functions performed. The appellant's work shares these characteristics with the assignments examples cited above. Her duties are limited to certain well-defined functions related to acquiring and controlling COMSEC equipment. This work requires knowledge of the governing regulations and prescribed procedures associated with the handling of the equipment. In carrying out this work, the appellant must consider such clear-cut factual information as the cost of the items, equipment compatibility, and available upgrades.

The position does not meet Level 1-7. At that level, work requires knowledge of a wide range of security concepts, principles, and practices to review independently, analyze, and resolve difficult and complex security problems. Such work situations may involve, for example: overlapping and conflicting requirements within a single facility or for a geographic region; 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; 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; develop or implement procedures and practices to cover multiple security objectives; serve on inter-agency or inter-organization committees and groups to identify and resolve security issues; or to perform similar work. The work at this level requires knowledge of a broad range of security program relationships or significant expertise and depth in one of the highly specialized areas of security to perform security program planning, or knowledge of a great variety of state-of-the-art security equipment and devices to plan and implement protective methods and security procedures.

Whereas Level 1-6 represents well-defined, operating-level security work, Level 1-7 depicts broader assignments involved in planning and setting up security programs and operations. The work requires a more comprehensive knowledge of security program interrelationships and the application of policy direction to specific operating requirements. In other words, this level encompasses program development work rather than ongoing security operations. As a COMSEC custodian, the focus of the appellant's work is exclusively to carry out defined processes and procedures to acquire, distribute, control, and account for sensitive equipment. She does not plan, develop, and implement security systems, procedures, practices, or controls, but rather follows regulations and guidelines that prescribe all aspects of her work.

Level 1-6 is credited (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 level of supervision under which the appellant works is comparable to Level 2-3. At that level, the supervisor defines the scope of the employee's responsibility and the objectives, priorities, and deadlines, and provides assistance with unusual situations. The employee, having developed competence in the work, plans and carries out the steps involved, handles deviations from established procedures, and resolves problems that arise in accordance with established practices and controls. The work typically includes conflicting interrelationships between security and subject-matter requirements that must be investigated and solved by the employee. Completed work is usually reviewed for technical soundness and appropriateness in relation to the nature and level of security required by the controlled materials, information, or facility, but the techniques used are not reviewed in detail.

This fully represents the type and level of supervision under which the appellant works. The appellant is assigned continuing functions with the scope of her responsibility and the general priority of her assignments defined. Using her acquired competence and experience with the work, she carries out the multiple steps and processes involved independently, resolving problems that arise in accordance with established practices and controls. Completed work is reviewed for adherence to prescribed procedures for handling the controlled items and responsiveness to the client organizations.

The position does not meet Level 2-4. At that level, the supervisor sets the overall objectives and 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 work, 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. The employee keeps the supervisor informed of progress, potential controversies, and issues with far-reaching implications. Completed 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.

Factor 2 is designed to measure not only the degree of independence with which the employee operates but also the extent of responsibility inherent in the assignment. The level of responsibility exercised is directly related to the nature of the work being performed. Within this context, Level 2-4 presupposes the conduct of projects or other assignments where the employee determines how the work is to be accomplished and is responsible for resolving conflicts among participants and interpreting policy applicable to the work. In contrast, the appellant is responsible for the conduct of certain defined, recurring functions where the procedures to be followed and the parameters of the work are very well defined. The highly sensitive nature of the work does not allow for deviation from established processes or departure from mandated controls. The appellant is not authorized to resolve conflicts among customers or to interpret policy related to the work on her own initiative. Her work is highly structured and her role is clearly defined and limited by the security considerations inherent to the assignment.

Level 2-3 is credited (275 points).

Factor 3, Guidelines

This factor covers the nature of the guidelines used and the judgment needed to apply them.

The guidelines used by the appellant match Level 3-3. At that level, the guidelines available and regularly used in the work are in the form of agency policies and implementing directives, manuals, handbooks, and locally-developed supplements. The guidelines are not always applicable to specific conditions or 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 is expected to use judgment in interpreting, adapting, and applying these guidelines, such as instructions for the application of security alarm and detection equipment; variations in security clearance levels for portions of facilities; document control systems and storage facilities where there is overlap in the levels of security required and the number and clearance level of persons with access to the facility; and other conditions.

The appellant interprets and applies detailed security guidelines associated with the handling of COMSEC material, which are broadly comparable to the regulations that cover the handling of classified information as described at Level 3-3 above.

The position does not meet Level 3-4. At that level, guidelines regularly applied consist of broad security guidance, such as directives issued by national security agencies, general agency policy statements, interagency security program policy proposals requiring refinement and coordination, or other guides that are not specific on how they are to be defined, implemented, and monitored. 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 geographic regions. Departmental guidelines available at this level are purposely left open to local interpretation and allow for local variations within overall policy direction. The employee must deviate from traditional methods and develop new methods, criteria, or proposed new policies. Examples of work situations involving this level of guidelines include: preparation of implementing instructions for a region, major military command, or comparable level of organization based on general national level directives or policy statements; working with program officials to anticipate security requirements and prepare general operating instructions; interpreting and preparing implementing procedures and instructions at field levels based on general agency policy statements; or establishing and monitoring operating security programs to meet specific needs (e.g., for organizations covering a number of locations or a variety of security program situations involving classified information, facilities, devices, industrial or scientific processes, etc.)

This level covers the various types of work situations where an employee is responsible for developing implementing guidelines or operating instructions for use by others. The appellant has no responsibility of this nature.

Level 3-3 is credited (275 points).

Factor 4, Complexity

This factor covers the nature, number, variety, and intricacy of the tasks or processes in the work performed, the difficulty in identifying what needs to be done, and the difficulty and originality involved in performing the work.

The complexity of the appellant's work is comparable to Level 4-3. At that level, employees perform various duties requiring the application of different and unrelated methods or practices. Assignments characteristic of this level include: developing alternate security plans for a facility describing options in levels of protection and the costs involved; adjudicating security clearance requests; defining information storage requirements for mixes of classified information requiring separate controls; or developing security plans involving separate protective systems for communications and ADP facilities. The work requires consideration of program plans, applicable policies, regulations, and procedures, and alternate methods of implementing and monitoring security requirements. Recommendations concerning the implementation of specific security systems and alternatives are based on factual information such as funding available, minimum regulatory requirements, delegated authorities to local managers to accept different levels of risk, and others that define the range of acceptable security decisions, programs, or systems.

As at this level, the appellant performs a variety of duties requiring different and unrelated methods and practices, encompassing the acquisition, shipping, distribution, accounting, and ultimate destruction of controlled items. The work is comparable to "defining information storage requirements for mixes of classified information" in that she has to implement and monitor the differing security requirements associated with various types of equipment. It involves consideration of factual information such as cost, equipment compatibilities, linkages within a system, and mandated security restrictions and safeguards.

The position does not meet Level 4-4. At that level, assignments consist 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 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. Programs and projects may be funded by or under the cognizance of different organizations with differing security requirements or variations in funding ability. The implementation of established security policies and practices may have to be varied for a number of locations or situations or coordinated with other organizations and security systems to assure compatibility with existing systems. The employee typically assesses situations complicated by conflicting or insufficient data which must be analyzed to determine the applicability of established methods, the need to digress from normal methods and techniques, the need to waive security standards, or whether specific kinds of waivers can be justified.

This level involves work that requires and permits a much greater degree of independent judgment and action than is vested in the appellant's position. It describes assignments that involve analyzing work situations to determine the types of security measures that should be implemented from among a range of alternatives, or where standard security practices must be adjusted or waived to fit local circumstances. The nature of the appellant's work does not permit this type of latitude. Her work, although complicated, is largely prescribed because of the strict controls that are maintained over the items she handles. Thus, the level of judgment required by the work is considerably less than described at this level.

Level 4-3 is credited (150 points).

Factor 5, Scope and Effect

This factor covers the relationship between the nature of the work, and the effect of the work products or services both within and outside the organization.

The scope and effect of the appellant's work match Level 5-3. At that level, the work involves resolving a variety of conventional security problems or situations, such as monitoring established security systems and programs. The work affects the efficiency of established security operations and contributes to the effectiveness of newly introduced programs requiring security support. The effect of the work is primarily local, although some programs may be part of multi-facility or nationwide program operations with interlocking security requirements.

The appellant's work involves implementing and monitoring established systems for the acquisition and control of sensitive items of equipment. The work affects the efficiency with which this function is carried out; i.e., whether customers receive the requested items in a timely manner and whether prescribed controls are properly maintained. As at this level, the work affects supported client organizations at geographically dispersed facilities within DoD.

The position does not meet Level 5-4. At that level, the work involves investigating and analyzing a variety of unusual security problems, questions, or conditions, formulating projects or studies to substantially alter existing security systems, or establishing criteria in an assigned area of specialization. The work affects security system design, installation, and maintenance in a wide range of activities within the organization and/or in non-Government organizations. 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, public organizations, or private industrial firms.

The appellant's work does not involve investigating problems, formulating projects, or establishing criteria related to the design or installation of security systems. It involves carrying out established processes for the acquisition and control of sensitive items. Although the work has a similar geographic impact beyond the immediate installation, it has a lesser programmatic impact in that it does not result in any substantive additions or alterations to existing security systems or operations.

Level 5-3 is credited (150 points).

Factor 6, Personal Contacts

These factors include face-to-face and telephone contacts with persons not in the supervisory chain.

The appellant's personal contacts match Level 6-2, where contacts are with persons from outside the immediate employing office or organization but usually within the same Federal agency, where the roles and relative authorities of the persons contacted are explicit. Level 6-3 is not met, where contacts are with individuals from outside the agency who represent the security program interests of other Federal agencies, contractors, private business and financial interests, foreign governments, or congressional offices, where 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 included at this level are contacts with the staff of national security agencies when these contacts take place at formal security briefings, deliberations, conferences, or negotiations.

The appellant's primary contacts are with staff from within various DoD components. Although she has occasional contacts with NSA staff, these contacts are conducted within a much more limited capacity that expected at Level 6-3. Her dealings with NSA consist primarily of telephone contacts to request equipment rather than the formal briefings and negotiations described at that level.

Level 6-2 is credited (25 points).

Factor 7, Purpose of Contacts

The purpose of the appellant's contacts match Level 7-2, where 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. Level 7-3 is not met, where contacts are for such purposes as persuading program managers to follow a recommended course of action; to discuss and resolve derogatory information that may affect the ability to grant security clearances; or to present and defend controversial security policies and regulations at meetings and conferences with higher-level security officials or officials from other agencies.

As at Level 7-2, the purposes of the appellant's contacts are to carry out established, prescribed processes. Her work does not involve or permit persuasion or negotiation or presenting policy recommendations in formal settings.

Level 7-2 is credited (50 points).

Factor 8, Physical Demands

This factor covers the requirements and physical demands placed on the employee by the work situation.

The appellant's work is consistent with Level 8-1, where work is primarily sedentary and no special physical effort is required to perform the work. Level 8-2 is not met, where work requires regular and recurring physical exertion, such as when inspecting buildings or industrial facilities.

Level 8-1 is credited (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 appellant's work environment matches Level 9-1, where work is performed in an office-like setting.

Level 9-1 is credited (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

The total of 1885 points falls within the GS-9 range (1855-2100) on the grade conversion table provided in the standard.

Decision

The position is properly classified as Physical Security Specialist, GS-080-9.