

**CLASSIFICATION APPEAL DECISION
U.S. OFFICE OF PERSONNEL MANAGEMENT
CHICAGO OVERSIGHT DIVISION**

INCUMBENT: **[Appellant]**

POSITION NUMBER: 720650001

AGENCY CLASSIFICATION: Physical Security Specialist, GS-080-9

POSITION LOCATION: Department of the Navy
[Installation]
[Installation City and State]

OFFICE OF PERSONNEL
MANAGEMENT DECISION: **Physical Security Specialist, GS-080-9**

OPM DECISION NUMBER: C-0080-09-01

This appellate decision constitutes a certificate that is mandatory and binding on administrative, certifying, payroll, and accounting offices of the Government. It is the final administrative decision on the classification of the position, not subject to further appeal. It is subject to discretionary review only under the conditions and time limits specified in Part 511, Subpart F, of Title 5, U.S. Code of Federal Regulations.

/s/

FREDERICK J. BOLAND
CLASSIFICATION APPEALS OFFICER

12/5/96

DATE

Information Considered

- Appellant's letter of appeal, dated December 29, 1995, and earlier correspondence, with enclosures.
- Agency letter of February 7, 1996, and its enclosures.
- Appellant's letter of May 31, 1996, with enclosures, containing comments on the material submitted to this office by the agency.
- Copy of the official description of the appellant's position, number 720650001.
- Copy of the official description of the appellant's supervisor's position.
- Copy of the appellant's performance plan.
- Copy of the organization chart and statement of functions for the appellant's organization.
- Copy of the position evaluation statement reflecting the agency's application of published position classification standards in reaching its decision for the appellant's position.
- Telephone audits of the position with the appellant on July 18, 1996, and with his supervisor on July 23, 1996, and subsequent conversations with his supervisor on October 1 and 3, 1996.
- Work samples submitted by the appellant on July 19, 1996.
- Work samples submitted by the appellant's supervisor on October 1, 1996.

Evaluation Criteria

- *Security Administration, GS-080, Series* position classification standard, dated December 1987.

Introduction

The appellant contests his agency's decision in classifying his position. He is assigned to position number 720650001, classified on April 12, 1995, as Physical Security Specialist, GS-080-9. The position is located in the [activity], [City, State]. He requests upgrading of his position to Physical Security Specialist, GS-080-11. He agrees that his official position description accurately reflects his major duties, but believes his work warrants higher credit based upon the knowledge required by his position, the nature of the guidelines used and the judgement needed to apply them, the complexity of the work performed, and its scope and effect (Factors 1, 3, 4, and 5 of the position classification standard).

Job Information

[Installation] is the host site of various facilities of the five branches of the armed services. As of March 1996, [the Installation] had a Command Staff, 10 Directorates, 11 tenants, 9 on-site contractors, and more than 70 departments. The [Installation] site covers 63,000 square acres and has more than 3,200 structures. Of this number, approximately 2,500 are storage magazines, 300 are buildings housing personnel and other equipment, 200 buildings store equipment or are unoccupied, and 200 structures are bridges, trestles and sheds. [Installation] also has 39 ready service magazines, 20 open storage and test areas, 36 jeep trails, 15 perimeter trails, 154 entry/exits, 150 miles of railroad, and 80 miles of fencing. The [activity], in which the appellant's position is located, is responsible for information, personnel, and industrial security. However, other organizations at [Installation] also provide security support in specialized areas to certain tenants. For example, the [Branch] Security Specialists who specialize in high security locking devices used for shipboard nuclear weapons security. The [certain] Weapons and Arms, Ammunition, and Explosives Branch likewise has a security specialist. (Both Branches are part of the [Directorate].)

The appellant is one of four Security Specialists (one GS-10 and three GS-9's) in the [activity]. They report to the GS-12 Supervisory Security Specialist who, in turn, reports to the GS-13 Security Officer. Specialists in the [activity] work in different security functions, such as information, personnel, and physical security. The appellant is responsible for a portion of the physical security function. Other portions of this function, such as the MLSR program and the Lock and Key program, are handled by separate specialists.

The appellant's major duties include:

- serving as a knowledgeable source concerning physical security and providing assistance to management on physical security requirements;
- providing guidance concerning physical security measures, standard operating procedures, and contingency plans for emergency responses;
- reviewing and evaluating physical security regulations, instructions, and directives from higher authorities and making recommendations to the appropriate managers on implementation;
- ensuring compliance with requirements governing the safeguarding and transportation of arms, ammunition, and explosives (AA&E);
- serving on [Installation] and outside teams to review and evaluate policies and procedures concerning physical security affecting other Department of the Navy (DON) activities;
- rewriting [activity] instructions to implement new regulations, instructions, and directives;
- formulating and rewriting specialized computer programs and generating various reports; and,

- assuring compliance with applicable physical security requirements by reviewing drawings and designs of construction projects and by attending preconstruction and inspection conferences.

Analysis and Findings

Series and Title Determination

The appellant's duties fall within the type of work covered by the position classification standard for the *Security Administration, GS-080, Series*, which includes positions of which the primary duties are analytical, planning, advisory, operational, or evaluative work that has as its principal purpose the development and implementation of policies, procedures, standards, training, and methods for identifying and protecting information, personnel, property, facilities, operations, or material from unauthorized disclosure, misuse, theft, assault, vandalism, espionage, sabotage, or loss.

Physical Security Specialist is the prescribed title for non-supervisory positions in this series in which the work is primarily concerned with the physical protection of sensitive or classified information, personnel, facilities, installations, or other sensitive materials, resources, or processes against criminal, terrorist, or hostile intelligence activities.

Grade Determination

The GS-080 standard is in the Factor Evaluation System (FES) format. This system requires that credit levels assigned under each factor relate to only one set of duties and responsibilities. Under FES, work must be fully equivalent to the factor-level described in the standard to warrant credit at that level's point value. If work is not fully equivalent to the overall intent of a particular level described in the standard, a lower level and point value must be assigned, unless the deficiency is balanced by an equally important aspect of the work that meets a higher level.

Factor 1: Knowledge Required by the Position

This factor assesses the nature and extent of information or facts that employees must understand to do acceptable work (e.g., steps, procedures, practices, rules, policies, theories, principles, and concepts) and the nature and extent of the skills needed to apply those knowledges.

The appellant believes that his work meets the requirements for Level 1-7 credit. He states that he is the authoritative source for physical security program knowledge for all [Installation] departments, tenant activities, and contractor organizations supported by the local security office, that he must resolve issues involving conflicting regulations, and that he must possess a knowledge of other areas of security.

At Level 1-6, the appellant has already been credited with the knowledge and experience necessary to independently analyze and resolve common problems in at least one security function (e.g., information, personnel, or physical security). He is credited with such matters as:

- resolving well-defined questions or conditions using standardized approaches for the nature of materials or information to the protected and the readily determined cost-benefit relationships for security devices or equipment systems involved;
- participating in the development of local security implementing plans and instructions based on well-defined objectives and using fully established methods and procedures;
- inspecting facilities where security processes and methods are known, security programs are operated effectively, and there is no history of significant violations and deficiencies;
- advising facility security personnel on matters requiring judgment and interpretation of the intent of regulations and procedures; and,
- collecting information, interviewing workers, and observing physical conditions and related activities concerned with violations and compromises.

At Level 1-7 of the standard, employees use knowledge of a *wide range* of security concepts, principles, and practices to review independently, analyze, and resolve *difficult and complex* security problems. Employees working in narrower areas, like the appellant, who is responsible for a portion of a security function rather than a broad range of security matters, might demonstrate Level 1-7 knowledge by handling *correspondingly more complex* problems. Such work would require significant expertise and depth in physical security, e.g., knowledge of a great variety of *state-of-the-art* security equipment and devices in planning and implementing protective methods and security procedures.

A construction project that the appellant's supervisor cites as representative of the appellant's job demands required the appellant to specify multiple levels of security and the type and placement of security devices and equipment. For the project [the certain facility], the appellant mapped Electronic Surveillance System (ESS) zones, designating the placement of secure access switches, balance magnetic switches, infrared devices, transceivers, and transponders. He also designated security devices such as card readers, locks, panic hardware, entry buzzers, and electronic switches and their placement. These various devices contribute to the overall complexity of the facility's security system and include some modern technology, but fall short of the standard's great variety of state-of-the-art devices criterion. Absent, for example, are the most modern devices used in controlling access (e.g., voice recognition, retina scanning, thumbprint readers, metal detection, x-ray scanning, etc.), shielding and encrypting voice and data communications, and intensifying and enhancing images. Also absent is evidence of regular and continuing assignments involving the correspondingly more complex problems that accompany unusual physical security circumstances or conditions.

The appellant suggests that he makes an extensive range of recommendations, as required at Level 1-7, to department directors, project managers, engineers, and construction experts so that facilities will meet the requirements for specific security operations. He indicates that in doing so he must analyze the variables of each situation: what is being stored or transported, the threat level, the terrain, the weather conditions, whether it is long or short term storage, the categorization and classification of the material being stored and/or transported, and the personnel needing access to the equipment and facilities. However, he supports his claim by citing a range of physical security

concepts, rather than a wide range of security concepts, e.g., involving personnel and information security, rather than physical security alone.

He provides four specific examples to illustrate the level of analysis required in his work. The first example, *[program]*, contains general operating instructions for an automated procedure he developed with a computer programmer to handle the arrival, parking, and departure of trucks at the site. The second example contains procedures to operate the Closed Circuit Television System (CCTV). The third contains comments he supplied to the [Installation] on proposed revisions to security regulations. The fourth is a security checklist that he completed for the Defense Logistics Agency when doing a physical security review on the Defense Reutilization and Marketing Office (DRMO) at [City]. Each reflects commendable improvements, but no greater analysis than which he has already been credited, since virtually none required his resolution of difficult and complex security problems.

He suggests because he is recognized as a knowledgeable source of information regarding physical security requirements at [Installation], additional credit is warranted. Though he is an important resource regarding physical security requirements, the nature of problems raised by those seeking his advice and that he must personally resolve do not meet the difficulty and complexity requirements of Level 1-7, as explained above.

We evaluate this factor at Level 1-6 and credit 950 points.

Factor 2: Supervisory Controls

This factor covers the nature and extent of direct and indirect controls exercised by the supervisor, the employee's responsibility, and the review of completed work. Controls are exercised by the supervisor in the way assignments are made, instructions are given to the employee, priorities and deadlines are set, and objectives and boundaries are defined. Responsibility of the employee depends upon the extent to which the employee is expected to develop the sequence and timing of various aspects of the work, to modify or recommend modification of instructions, and to participate in establishing priorities and defining objectives. The degree of review of completed work depends upon the nature and extent of the review (e.g., close and detailed review of each phase of the assignment; detailed review of the finished assignment; spot check of finished work for accuracy; or review only for adherence to policy).

At Level 2-3, supervisors define the employees' scope of responsibilities and the objectives, priorities, and deadlines. Employees plan and carry out the steps involved in the assignments, handle deviations from established procedures, and resolve problems that arise in accordance with agency or local standards, previous training and experience, established practices, or other security controls appropriate to each assignment. Completed work is usually evaluated for technical soundness and appropriateness in relation to the nature and level of security required by the controlled materials or facility involved. During the course of assignments, supervisors do not usually review techniques used by employees in detail.

At Level 2-4, supervisors set the overall objectives and decide on the resources available. Employees consult with their supervisors in determining which projects to initiate, develop deadlines, and identify staff and other resources required to carry out assignments. Employees plan and carry out assignments, resolve most of the conflicts which arise, integrate and coordinate the work of others as necessary, and interpret policy. Employees keep their supervisors informed about progress, potential controversial matters, or developing security conditions or requirements with far-reaching implications. Completed work is reviewed for feasibility, compatibility with other security program requirements, or effectiveness in meeting objectives.

The appellant usually works independently with little or no technical supervision. He handles problems and deviations in work assignments using established security practices and methods found in the numerous regulations and guidelines issued by Navy, DOD, and various other military and civilian organizations. His work does not typically include difficult and complex security problems that require him to significantly deviate from established methods. He has ample experience in his specialization, which allows him to work with a great deal of independence when using standard physical security methods and devices and determining cost efficiency of such devices and systems. However, he lacks the greater responsibility that accompanies more difficult work assignments requiring a significantly higher level of knowledge. While he may work with greater independence than typical of Level 2-3, which is the highest level of independence and responsibility normally associated when using well precedented security approaches, it is without a significant increase in knowledge requirements or work complexity. Because Level 2-4 demands a corresponding increase in the difficulty of work to accompany the increased independence, it is inappropriate for the appellant's work.

We evaluate this factor at Level 2-3 and credit 275 points.

Factor 3: Guidelines

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

The appellant believes that he meets the requirements for Level 3-4 under this factor, because he uses numerous guidelines written by a number of Federal and private organizations. He states that these guides, which consist of publications, instructions, documents, and policy statements, are all general outlines of the concepts and methods for security programs and are always conflicting. He states that he must interpret the intent of the guidelines on every security project, goal, and program that he is involved with and comment on proposed security requirements.

He is already credited at Level 3-3 with using guidelines not always applicable to specific conditions and having gaps in requirements. He is credited with using judgement in interpreting, adapting, and applying such guidelines and independently resolving conflicts in guidelines. He is also credited with analyzing and developing security plans within the intent of available guidelines.

At Level 3-4 of the standard, guidelines are scarce or of limited use and often insufficient to accomplish specific objectives. They provide only a general outline of the concepts, methods and

goals of security programs. Employees at this level must deviate from traditional methods and develop new methods, criteria, or proposed new policies.

The guidelines and regulations used by the appellant are usually very specific. Due to this specificity, conflicts frequently arise; the appellant must then choose the most stringent guidelines for application or develop accommodating solutions and make recommendations to the project managers, directors, etc. He cites, for example, conflicting regulations for the storage of material issued by the Marine Corps, Air Force, and DOD. One set of regulations called for 5/8" steel bars on the windows; another called for 3/8" steel plates on the windows; and another required a chain link fence. In a situation such as this, the appellant typically recommends a security measure stringent enough to meet the most restrictive requirement. Such judgment and adaptation are fully credited at Level 3-3.

He also cites an atypical case involving the storage of [certain] equipment. He indicates [Installation] is the only site that stores [certain] equipment and that there are no regulations that cover its storage and safeguarding. Because the [certain] equipment is designated in Category IV, the appellant analyzed the requirements for other Category IV equipment and developed similar requirements for the [Installation] [certain] equipment storage. Though the judgment and analysis involved in this case exceeds Level 3-3, it is not characteristic of the appellant's regular and continuing assignments, which govern the assignment of credit levels.

Therefore, we evaluate this factor at Level 3-3 and credit 275 points.

Factor 4: Complexity

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

The appellant believes he meets the requirements for Level 4-4 of this factor because his assignments consist of a variety of duties and many different processes and methods in scientific and production operations, storage, shipping and receiving, maintenance and rework operations. He states that his assignments require constant coordination with the organizations on site and interpretation and analysis of regulations and requirements in numerous program areas. He also states that he coordinates the funding for project work where funding is shared by the organizations involved and advises the organizations involved on what part of the funding each organization is responsible for and, if desired, how to request that funding.

At Level 4-3 of the standard, employees perform various duties requiring the application of different and unrelated methods, practices, techniques, or criteria. Employees develop alternate security plans for a facility, describing options in levels of protection and costs involved for a Federal or private sector facility where the minimum protection requirement is well defined and accepted techniques are appropriate. Employees at this level compile, analyze, and summarize information related to the designated security requirements, develop plans for approaches to be taken, define the level of risk involved for each plan, develop costs for implementing each of several options, and recommend a

course of action to meet assignment objectives. Employees identify and analyze relationships among organizational needs and objectives, costs, requirements of security guides, and related information.

At Level 4-4 of the standard, 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 the alternatives and arrive at the decisions or recommendations. Security methods may require adjustment or modification of established approaches to accommodate local conditions or circumstances. Employees at this level typically assess situations complicated by unusual circumstances and conflicting or insufficient data, evidence, or testimony that must be analyzed to determine the applicability of established methods.

The appellant develops alternative physical security plans for projects or facilities located at the [Installation], describing options in levels of protection and the costs involved. Although regulations and requirements may conflict in projects involving more than one organization, the problems are well defined and established security techniques are adaptable. His recommendations concerning the implementation of security systems and alternatives are based on factual information such as available funding and regulatory requirements, as is consistent with Factor Level 4-3. His assignments do not typically involve unusual security circumstances or problems, as required at Level 4-4.

We evaluate this factor at Level 4-3 and credit 150 points.

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. Only the effect of properly performed work is to be considered.

The appellant believes that his work merits Level 5-4 because his work impacts a number of organizations at [Installation]. He indicates that he reviews and approves all facility and project blueprints to assure compliance with the security requirements and is presently involved with projects for a number of Federal agencies and private firms at [Installation]. He also claims that his work affects their budgets and programs.

The appellant cites two examples to support his position. He indicates that he substantially altered the security system at the [Installation] site by introducing Closed Circuit Television (CCTV) to [Installation] thereby providing another security system alternative. In some cases, the CCTV system has reduced the number of security guards needed to maintain surveillance on certain facilities for the Navy and the Marine Corps. The second example he cites involves the [certain equipment] project previously discussed and found uncharacteristic of his work assignments.

Scope

Level 5-3 of the standard credits work resolving conventional security problems, such as performing independent reviews and recommending actions based upon well-established criteria, methods, techniques, and procedures.

Level 5-4 of the standard requires that employees investigate and analyze a variety of unusual security problems, questions, or conditions, formulate projects or studies to alter existing security systems substantially, or establish criteria in an assigned area of specialization.

The appellant's work typically involves resolving conventional security problems, questions, and situations, interpreting, adapting, and applying established security criteria, and recommending actions involving established methods and procedures, which is consistent with Level 5-3. It does not typically involve investigating and analyzing a variety of unusual security problems (as previously noted under Factor 4) or comparable analytical difficulties that may be encountered in formulating projects or establishing criteria, as required at Level 5-4.

Effect

At Level 5-3, work products and assistance affect the effectiveness and efficiency of established security programs and contribute to the security effectiveness of newly introduced programs and facilities. The effect of the work is primarily local, although some programs may be part of multi-facility or nationwide program operations.

At Level 5-4, 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 in developing alternatives and options that are designed to meet requirements in a variety of physical and environmental circumstances.

As at Level 5-4, the appellant's work affects a wide range of agency activities at [Installation].

To receive credit for Level 5-4, its criteria must be met under both Scope and Effect. The appellant meets only Effect. Therefore, we evaluate this factor at Level 5-3 and credit 150 points.

Factor 6: Personal Contacts

This factor includes face-to-face contacts and telephone and radio dialogue with persons not in the supervisory chain. 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 (e.g., the degree to which the employee and those contacted recognize their relative roles and authorities). Above the lowest level, points should be credited under this factor only for contacts that are essential for successful performance of the work and that have a demonstrable impact on the difficulty and responsibility of the work performed.

The position has been credited with Level 6-3 and the appellant does not claim higher credit. The appellant's contacts are with individuals employed by other Federal agencies, Directorate directors

at [Installation], heads of tenant activities, private contractors, and Command, military, and other employees of the [activity].

At level 6-3 of the standard, moderately unstructured contacts take place 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, or congressional offices.

Contacts at Level 6-4 of the standard involve face-to-face or telephone contacts with Members of Congress and/or top Presidential advisors, or comparable levels of officials from foreign governments in highly unstructured settings.

We evaluate this factor at Level 6-3 and credit 60 points.

Factor 7: Purpose of Contacts

The purpose of personal contacts varies from factual exchange of information to situations involving significant or controversial issues and differing viewpoints, goals, or objectives. The personal contacts used as the basis for this factor must be the same as the contacts used for Factor 6.

The position has been credited with Level 7-2 and the appellant does not claim higher credit. The appellant contacts are for the purpose of conducting surveys, inspections, audits, giving or exchanging information, training employees and contractors about security, and making recommendations.

At Level 7-2 of the standard, contacts are made for the purpose of resolving issues and problems or for carrying out security plans and reviews to achieve mutually agreed upon security and program objectives.

At Level 7-3, the purpose of contacts is to persuade program managers and other decision-making officials, with widely different goals and interests, to follow a recommended course of action consistent with established security policies, objectives, and regulations.

We evaluate the factor at Level 7-2 and credit 50 points.

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 and physical exertion involved in the work.

This factor was evaluated at Level 8-1 and the appellant does not claim more credit.

Level 8-1 work is sedentary and presents no special physical demands, though there may be some walking, standing, bending, and carrying of light items. Level 8-2 work involves considerable walking, stooping, bending, climbing, etc., or long periods of standing or recurring lifting of moderately heavy items.

The appellant's work is mostly sedentary and free of special physical demands. Like Level 8-1, it involves some walking, standing, etc., but unlike Level 8-2, it does not *require* long periods of standing or the like. Occasional lifting of heavy objects when delivering or installing security devices is required, but rarely is recurring lifting ever required. The occasional need to lift moderately heavy objects does not warrant Level 8-2 credit, which is assigned to employees whose work regularly presents special physical demands.

We evaluate this factor at Level 8-1 and credit 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.

This factor was evaluated at Level 9-1 and the appellant does not claim higher credit.

Level 9-1 work is in an office setting. Level 9-2 work involves moderate safety risks or discomforts that require special precautions. The appellant's work is performed in an office-like setting and requires no special safety precautions. His work is generally performed in lighted, heated, and ventilated areas, although outdoor activities are necessary during surveys and inspections or physical security barriers and facilities used for storage of sensitive ordnance items, tools, equipment, and classified material.

We evaluate this factor at Level 9-1 and credit 5 points.

FACTOR LEVEL POINT SUMMARY

Factor	Level	Points
1	1-6	950
2	2-3	275
3	3-3	275
4	4-3	150
5	5-3	150
6	6-3	60
7	7-2	50
8	8-1	5
9	9-1	5
	Total:	1920

The table above summarizes our evaluation of the appellant's work. As shown on page 19 of the standard, a total of 1920 points falls within the GS-9 grade range (1855-2100).

Decision

The proper classification of the appellant's position is Physical Security Specialist, GS-080-9.