CERTIFICATE OF
A CLASSIFICATION APPEAL DECISION OF THE
OFFICE OF PERSONNEL MANAGEMENT
CHICAGO REGION

APPELLANT:	[appellant's name]
POSITION NUMBER:	[position description number]
AGENCY CLASSIFICATION:	Computer Specialist (Security), GM-334-13
POSITION LOCATION:	ADP and Communications Security Division Office of Command Security Defense Logistics Agency Columbus, Ohio
OFFICE OF PERSONNEL MANAGEMENT DECISION:	Computer Specialist, GS-334-13 Use of a parenthetical title is at the agency's discretion. PMRS (GM) determination is the responsibility of the employing agency
Decision Number:	C-0334-13-02

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 the Classification Appeals Office's review only under the conditions specified in 5 CFR 511.613 and within the time limits specified in 5 CFR 511.605. (Address provided in Appendix B of Federal Personnel Manual Chapter 511.)

_____
Steven R. Cohen
Regional Director

4/7/93
_____
Date

DECISION TRANSMITTED TO:

[appellant's name and address]

Mr. Al C. Ressler
Staff Director, Civilian Personnel
Defense Logistics Agency
Cameron Station
Alexandria, Virginia 22304-6025

Mr. Frank M. Scutch
Director, Office of Civilian Personnel
DLA Administrative Support Center
Defense Logistics Agency
Cameron Station
Alexandria, Virginia 22304-6130

INFORMATION CONSIDERED

- Appellant's letter of appeal, dated October 27, 1992, with attachments
- Copy of the official description of the appellant's position, number [position description number]
- Copy of the official description of the appellant's supervisor's position
- Copy of the appellant's performance standards
- Copy of the organization chart and statement of functions for the ADP and Communications Security Division, Office of Command Security, Defense Logistics Agency, Columbus, Ohio, in which the appellant's position is located
- Copy of the position evaluation statements that reflect the Defense Logistics Agency's application of published position classification standards in reaching its decision for the appellant's position
- Audit of the position by telephone with the appellant on February 25, March 3 and 18, 1993 and with appellant's supervisor on March 1, 1993
- Discussions about the appellant's position with a Defense Logistics Agency information systems project manager, a National Institute of Standards and Technology computer scientist, and a Department of Defense information system management specialist familiar with appellant's work

EVALUATION CRITERIA

- OPM position classification standard for the Computer Specialist, GS-334, Series, dated July 1991

INTRODUCTION

The appellant contests a decision made by the Defense Logistics Agency in classifying his position. The appellant is assigned to position number [position description number], classified by the Defense Logistics Agency on November 21, 1992, as Computer Specialist (Security), GS-334-13. The position is located in the ADP and Communications Security Division, Office of Command Security, Defense Logistics Agency, Columbus, Ohio. The appellant's duty station allows him to work directly with the agency's central system design organization there and places him nearby the different types of Defense Logistics Agency activities requiring his support such as Supply Centers, Service Centers, Depots, and Contract Management Districts.

The appellant requested that his position be classified as Computer Specialist (Security), GM-334-14, because of his responsibility for writing and interpreting security policy. He contends that his involvement with policy warrants greater credit under Factor 3, Guidelines, of the classification standard. He agrees that his position description accurately reflects his duties.

JOB INFORMATION

The appellant is one of three non-supervisory employees in his Division who specialize in computer security. The appellant evaluates the security of Defense Logistics Agency computer systems against fraud, unauthorized access, tampering, disruption, sabotage, etc., to their operating systems, telecommunications control programs, database management systems, and the like. Computer systems range from those at six large information processing centers to numerous local area networks and personal computers. This comprises about 14 centers, 60 mainframes, 400 minicomputers, 240 local area networks, and 40,000 personal computers. The Columbus Defense Construction Supply Center alone, for example, has about 20 local area networks.

He identifies system vulnerabilities and formulates security specifications and improvement plans for ADP managers and system designers. This ranges from the study of existing systems or proposed acquisitions to stress testing of systems by attempting unauthorized access or transactions. Major systems studied include, for example, the Mechanization of Contract Administration System, the Base Operations Supply System, the Standard Automated Materiel Management System, and the Defense Business Management System.

He evaluates new security management systems and technologies for their technical effectiveness, applicability, and cost. These range, for example, from supervisory software like the Resource Access Control Facility used on IBM mainframes to specialized extension software and hardware. Some of the technology involved is state-of-the-art, like smart cards, digital signatures, and public key encryption. He develops policies and procedures to strengthen system, telecommunications, and procedural security, determining what features should be present to provide the level of security desired. He keeps security officers and functional area experts (database owners) informed of security requirements and developments and advises them on security policy, risks, safeguards, and countermeasures.

The appellant's organization is in the process of centralization of Department of Defense ADP activities into the Defense Information Systems Agency. This reconfiguration may well affect the appellant's work. However, the Office of Personnel Management is required to adjudicate classification appeals on the basis of the current duties and responsibilities of appealed positions, rather than on the basis of as yet unimplemented arrangements of work.

ANALYSIS AND FINDINGS

Series and Title Determination

The appellant's work meets the definition of the Computer Specialist, GS-334, Series. This series encompasses work designing or testing computer systems where the primary need is for knowledge of information processing methodology or technology, computer capabilities, and processing techniques. This includes specialized functions such as evaluating, designing, installing, and monitoring computer security systems. *Computer Specialist* is the prescribed title for non-supervisory positions in the GS-334 series. The agency has exercised its discretion to add the parenthetical title *Security* to identify the specialty area of the position.

Grade Determination

The Computer Specialist position classification standard is in Factor Evaluation System format. This requires a factor-by-factor analysis of the position in light of the standard. Under the Factor Evaluation System, a position factor must be fully equivalent to the factor-level described in the standard to warrant credit at that level and the associated point value. If a position fails in any significant aspect to meet a particular factor-level description in the standard, the next lower level (and its point value) must be assigned, unless the deficiency is balanced by an equally important aspect that meets a level above the particular factor-level.

Factor 1: Knowledge Required by the Position

This factor measures 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.

Level 1-8 calls for mastery of a specialty area and the ability to apply experimental theories and new developments to problems that do not yield to accepted methods. Such expert knowledge might be demonstrated by leading or participating on task forces for resolving critical problems that demand innovative solutions, by advising top ADP and user management on new developments and advanced techniques in the specialty area, or by coordinating the development of ADP standards, guidelines, or policy.

Level 1-9 is not described in the Computer Specialist standard, as it occurs infrequently in positions in this occupation. The Primary Standard indicates that Level 1-9 requires mastery of a professional field to generate and develop new hypotheses and theories, or equivalent knowledge and skill.

The appellant is one of the Defense Logistics Agency's technical authorities on computer security. As such, he advises top-level design and operational specialists at Defense Logistics Agency design activities and information processing centers on the meaning of security policies and standards, how well their systems meet security requirements, and how to apply the latest technological advances in computer security.

He plays a key role in formulating policies and developing computer security criteria. He authored major sections of Defense Logistics Agency's computer security regulations, DLAR 5200.17. He was the Defense Logistics Agency's expert on a task force charged with updating the Department of Defense's Automated Information System Security Manual. He reviews and recommends changes to Federal computer security criteria proposed by the National Institute of Standards and Technology and the National Security Agency, commenting, e.g., on the contents of document integrity guidelines and the practicality of identification and authentication requirements. He examines security planning documents (accreditation plans) for highly complex systems with multiple security levels (e.g., Joint Computer Aided Acquisition and Logistics Support), to ensure the Defense Logistics Agency's security needs are met.

He pursues novel solutions to critical problems by incorporating state-of-the art technology into the Defense Logistics Agency's security systems. For example, he is exploring the use of electronic digital signatures, public key encryption, and smart cards as a means of ensuring document integrity under paperless systems. Prototypes of such advanced authentication technology are just now being applied.

The knowledge required for such work is equivalent to Level 1-8. It does not involve the development of new hypotheses and theories as found at Level 1-9.

We evaluate this factor at Level 1-8 and credit 1550 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 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 2-4, supervisors set overall objectives and employees independently plan and carry out assignments. Work is reviewed for its overall feasibility, compatibility, and effectiveness.

At Level 2-5, only administrative supervision is provided; assignments are broadly defined missions or functions, carried out independently, and are not subject to technical review but may be reviewed for fulfillment of objectives. At this level, employees decide which analytical and technical decisions form the basis for major program policy and operational decisions by top management. Employees who work at this level are regarded as the leading technical authority for the employing organization in a data processing specialization.

The appellant's supervisor gives him extensive latitude in interpreting and developing security policy and criteria (e.g., the appellant's independent development of major sections of the Defense Logistics Agency computer security regulation, DLAR 5200.17). As an agency expert in computer security, he makes extensive independent judgments concerning policy and criteria that are communicated to ADP managers and system designers without any technical review. His

advice and comments concerning proposed criteria, security plans, and adaptation of new technology are accepted as technically authoritative.

The appellant is one of several computer security technical authorities within the ADP and Communications Security Division. He is not, however, the leading technical authority in computer security for the Defense Logistics Agency. While he advises on analytical and technical issues that form the basis for major program policy and operational decisions, he does not decide these issues. For example, his advice on security matters for the Defense Logistics Agency Automated Information System Review Council, which is the deciding body regarding Defense Logistics Agency automation projects, is funneled through his supervisor and not given by the appellant directly. The appellant is one of several specialists who help his superiors run a security program and formulate its policy, but he is not ultimately responsible for the program.

Level 2-4 involves a high degree of independence and responsibility. Level 2-5 embodies a level of extraordinary independence and freedom from supervision which is typically accompanied by responsibility for a significant program or function. The appellant has full technical authority for the aspects of the security program he is assigned. His superiors, however, must review his work for compatibility with the broader program and otherwise exercise substantial program control. They are given the broad mission or function which makes them ultimately responsible for the security program. In turn they set the overall objectives and resources under which the appellant assists them in carrying out the mission or function. For these reasons, the appellant's position does not reach Level 2-5.

We evaluate this factor at Level 2-4 and credit 450 points.

Factor 3: Guidelines

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

At Level 3-5, guidelines, in the form of agency policy or legislation, are broadly stated, non-specific, and require extensive interpretation and definition. The major constraints derive from state-of-the-art technology. Judgment is required in developing ways to obtain data on and evaluate the significance of technological advances in a specialty area such as computer security and to interpret conflicting legislation and overall objectives. Employees at this level are generally recognized throughout the agency as experts in a specialty area.

The appellant's work is accomplished under broad and non-specific Government guidelines such as the Computer Security Act of 1987 and general guidelines in Office of Management and Budget Circulars, Department of Defense directives, National Institute of Standards and Technology publications, and National Security Agency requirements. He develops with other Defense Logistics Agency experts proposed agency-wide guidelines for ADP managers and security officers in the form of security regulations (DLAR 5200.17) and criteria. In so doing, he must resolve conflicting overall objectives between the Defense Logistics Agency's needs for secure and trustworthy systems versus its needs for efficient and economical access to a variety of information.

He developed proposed certification and accreditation criteria for establishing the trustworthiness of systems and extensively interprets agency guidance, giving it definition for information processing centers and database owners. He must balance agency security requirements with technological limitations, costs, and user efficiency. He represents the Defense Logistics Agency as a technical expert on inter-agency task forces and committees that formulate general program guidance for the Department of Defense.

The appellant's position description and performance standards emphasize his role in interpreting security policy for the agency. He is recognized as a technical authority throughout the Defense Logistics Agency in this aspect of his work. He participates on inter-agency task forces and committees that formulate Department of Defense security guidance which organizations are required to use. The judgment and ingenuity he must use in these situations, as well as in developing new applications such as that of advanced authentication technology, are equivalent to Level 3-5 of the standard.

We evaluate this factor at Level 3-5 and credit 650 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.

At Level 4-5, work involves a broad range of activities or substantial depth of analysis. Decisions about what to do are complicated by major areas of uncertainty in approach or methodology or by interpretation and evaluation due to such elements as continuing changes in program, technological developments, unknown phenomena, or conflicting requirements. Technical difficulty is exceptional and work requires originating new techniques, establishing criteria, or developing new information.

At Level 4-6, work involves continuing efforts to establish concepts, theories, or programs, or to resolve unyielding problems in broad functions and processes. Work at this level includes performance of exploratory studies to define issues and problems where precedents do not exist. Decisions require extensive probing and analysis to determine the nature and scope of problems.

The appellant's work involves the application of security measures to a broad range of highly complex systems that interact at operating system, telecommunications, application, and other levels. Substantial analysis is required, for example, to trace audit trails, identify data flow, ascertain risks, and establish safeguards. His work must be integrated with the efforts of system designers, ADP managers, security officers, and sometimes others outside the agency. He applies newly developed technology, like electronic digital signatures, smart cards, and public key encryption, to novel (e.g., paperless systems) or persistent (e.g., password systems) problems.

His development of the Universal Access Control System (which seeks to automate the authorization of user access through electronic routing, approval, updating, and notification), for example, exemplifies a novel method of addressing persistent problems. It would incorporate electronic digital signatures by adapting cutting edge technology to the Defense Logistics Agency's security systems, providing a faster and more economical process for managing a critical security problem.

Such work equates to Level 4-5, where employees face exceptional technical difficulties. His work does not, however, push the barriers of what is known in broad areas of automated data processing, as suggested by the next higher level.

We evaluate this factor at Level 4-5 and credit 325 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.

At Level 5-5, work involves isolating and defining unknown conditions, resolving critical problems, or developing new theories. The work affects the work of other experts or the development of major aspects of programs or missions. Developing guidance for ADP security techniques to be used throughout an organization is given as one example of this level.

At Level 5-6, work involves planning and conducting vital administrative or scientific projects that are essential to the missions of the agency. Such work establishes precedent and has a long-term effect on the agency's programs and often influences other agencies' programs.

The appellant's expertise is directed at resolving critical computer security problems throughout the Defense Logistics Agency. As part of this work, he develops guidance on security techniques that affects the approach taken by other computer experts throughout the agency in their system designs.

Such work equates to Level 5-5, but lacks the broader scope and effect outside the agency typical of Level 5-6.

We evaluate this factor at Level 5-5 and credit 325 points.

Factor 6: Personal Contacts
and
Factor 7: Purpose of Contacts

These factors cover face-to-face contacts and telephone and radio dialogue with persons not in the supervisory chain. Levels of personal contacts 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.) The purpose of personal contacts ranges from factual exchanges of information to situations involving significant or controversial issues and differing viewpoints, goals, or objectives. The combined levels for both factors are converted to a single point-value for both factors.

Personal Contacts

Level 3 contacts include, in addition to those within the agency, individuals or groups outside the agency in moderately unstructured settings. Level 4 contacts are with high-ranking officials outside the agency, including key officials and top scientific personnel of other agencies, private industry, etc., in highly unstructured settings.

The appellant's intra-agency contacts are with ADP administrators, design chiefs, system programmers, security officers, and user personnel. Contacts external to the agency include security software specialists at vendor and contractor firms, technical experts at the National Computer Security Center and other agencies, and security industry associations. Such contacts are typical of Level . They do not involve the regular contact with key personnel in highly unstructured settings described at Level 4.

Purpose of Contacts

Level c purposes are to persuade others to cooperate or to influence others to adopt particular methods and procedures; at Level c, there are problems in securing cooperation, as when others are skeptical or have serious technical reservations. Level d purposes are to justify, defend, or resolve highly controversial matters.

The purpose of appellant's contacts is to persuade others to adopt security procedures where they are reluctant to do so because of time, cost, inconvenience, etc. This equates to Level c. The appellant is not expected to justify, defend, or resolve highly controversial matters as found at Level d.

We evaluate these factors at Level 3-c and credit 180 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.

Level 8-1 work is sedentary and requires no special physical demands. Level 8-2 work involves considerable walking, stooping, bending, and climbing. The appellant's work is sedentary, and we therefore evaluate this factor at Level 8-1 and credit 5 points.

Factor 9: Work Environment

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

Level 9-1 work is in an office setting that does not require special safety precautions. Level 9-2 work involves moderate safety risks or discomfort which require special precautions. The appellant's work is performed in an office and requires no special safety precautions, and we therefore evaluate this factor at Level 9-1 and credit 5 points.

The table that follows is a summary of our evaluation of the appellant's position.

Factor	Level	Points
1	1-8	1550
2	2-4	450
3	3-5	650
4	4-5	325
5	5-5	325
6&7	3-c	180
8	8-1	5
9	9-1	5
TOTAL:		3490

The grade conversion table on page 11 of the position classification standard for the Computer Specialist, GS-334, Series, shows that 3490 points convert to grade GS-13.

DECISION

As explained in the foregoing, the proper classification of the appellant's position is Computer Specialist, GS-334-13. The agency is permitted but not required to add a parenthetical title. Determination as to whether the position should be GS or GM, i.e., subject to the Performance Management and Recognition System, is at the discretion of the employing agency.