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

Dallas Field Services Group
1100 Commerce Street, Room 441
Dallas, TX 75242

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

Appellant:	[appellant]
Agency classification:	Supervisory Information Technology Specialist (INFOSEC) GS-2210-12
Organization:	Security Division Information Technology Business Center US Army Garrison US Army Medical Department Center and School/ Ft. Sam Houston Department of the Army Fort Sam Houston, Texas
OPM decision:	Supervisory Information Technology Specialist (INFOSEC) GS-2210-12
OPM decision number:	C-2210-12-01

/s/ Judith L. Frenzel

Judith L. Frenzel
Classification Appeals Officer

July 28, 2003

Date

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

Decision sent to:

[appellant's name and address]

[servicing personnel office address]

Deputy Assistant Secretary
Civilian Personnel Policy/Civilian Personnel Director for Army
Department of the Army
Room 23681, Pentagon
Washington, DC 20310-0300

Director, U.S. Army Civilian Personnel Evaluation Agency
Department of the Army
Crystal Mall 4, Suite 918
1941 Jefferson Davis Highway
Arlington, VA 22202-4508

Chief, Position Management and Classification Branch
Office of the Assistant Secretary
Manpower and Reserve Affairs
Department of the Army
Attn: SAMR-CPP-MP
Hoffman Building II
200 Stovall Street, Suite 5N35
Alexandria, VA 22332-0340

Chief, Classification Appeals Adjudication Section
Civilian Personnel Management Service
Department of Defense
1400 Key Boulevard, Suite B-200
Arlington, VA 22209-5144

Introduction

On March 12, 2003, the Dallas Field Services Group, formerly the Dallas Oversight Division, of the U.S. Office of Personnel Management (OPM) accepted a classification appeal from [appellant], an employee in the Security Division, Information Technology Business Center, U.S. Army Garrison, [installation], Department of the Army, at [location]. His position is currently classified as Supervisory Information Technology Specialist (INFOSEC), GS-2210-12. He believes his position should be classified as Supervisory Information Technology Specialist (INFOSEC), GS-2210-13. The complete administrative report was received on April 4, 2003. We have accepted and decided this appeal under section 5112(b) of title 5, United States Code.

Background information

The appellant is assigned to position description (PD) number FR [number]. The appellant and his supervisor agree that this PD is a complete and accurate description of the duties. The appellant disputed the accuracy of several factor levels assigned to his PD and attempted to resolve the issue with his agency. He filed an appeal with the Department of Defense's Civilian Personnel Management Service. That decision, dated February 25, 2003, sustained the installation's classification of the position. With his appeal to OPM, the appellant provided a statement that the duties in his current PD are essentially accurate, except for the evaluation of Factors 1, 3, 4B, 5, and 6, using the General Schedule Supervisory Guide. The appellant believes that the addition of two contract employees to his division and the additional duties involved in supervising the additional personnel warrants upgrading his position to GS-13. He does not question the evaluation of his nonsupervisory work.

We conducted a telephone audit with the appellant on May 21, 2003, to supplement information provided by the appellant and the agency in the written record. On May 27, 2003, we interviewed his supervisor by telephone to clarify responsibilities and authorities assigned to the appellant's position. On June 16, 2003, we interviewed the site manager for [company name] which has the contract for Defense Information Technology Security Certification and Accreditation Process (DITSCAP**)** at [location]. We also discussed the pay setting for contract employees hired by [company name] with Information Technology Business Center's Contracting Officer's Representative and the Deputy Chief Operating Officer of Fed Source, part of the Department of Treasury.

General issues

The appellant questions the GS-11 grade level equivalency established by [location] for the two contract personnel working in his Division. He bases his objection on the fact that the contract employees are paid at rates equal to GS-12 and GS-13 under the General Schedule pay system. Our fact finding determined that the contract vendor determines pay rates, based on the Statement of Work (SOW) for the contract position and the Department of Labor's (DOL) published wage determinations. If the labor category for the work is not on the DOL list, then a market survey is done. The government agency then accepts or rejects the vendor's proposed pay rate for the SOW.

The General Schedule Supervisory Guide measures the difficulty and complexity of the basic work directed as a factor in evaluating the grade level for supervisory work. By law, the

difficulty of this work is measured by comparison with classification standards. Based on the statements of work for the contract workers, the installation determined the duties assigned to those positions is equivalent to that performed by the Federal staff as IT Specialists at the GS-11 grade level. The CPMS concurred with that determination in their appeal decision and, based on our analysis of the appeal record, we agree.

Position information

The appellant directs the work of the Security Division, one of seven divisions in the Information Technology Business Center (ITBC). The ITBC is responsible for providing a wide range of information and technology systems and services to the [name] installation, their outlying installations, tenant organizations and the Department of Defense (DOD) offices located in the support area. These include multi-media and photo imaging, TV production, visual productions, as well as voice, data, and telecommunications services. As Chief of the Security Division, the appellant is responsible for directing and managing the installation information systems security (ISS) of the computer network used by [name] installations, tenants, and DOD activities.

The appellant implements the Army ISS Program to provide protection for all automated information systems and ensures all systems and networks are accredited according to regulatory guidance. He develops and manages an installation ISS awareness program covering computer support, hardware, software, systems, procedures, data, telecommunications, personnel, physical environment, networks, and firmware. The appellant ensures that supported installation and tenant organizations have appointed Information Assurance Security Officers and that those officers and system administrators are trained in all aspects of ISS, including system audit functions, reviews for detection of system intrusions and abuse, secure operations, and reporting security incidents and technical vulnerabilities.

The appellant manages and maintains network anti-virus protection. He reviews security threat and vulnerability assessments and suggests cost-effective countermeasures. He reports security incidents and technical vulnerabilities to the Army Computer Emergency Response Team (ACERT) or the Regional Computer Emergency Response Team (RCERT) or other Army agencies as required. The appellant oversees investigations of possible security breaches, attempted intrusions, and unauthorized accesses to data and implements and maintains security software and fixes to operating systems to correct identified vulnerabilities. He develops local ISS policy, ensures that Army security policies are implemented, develops and manages the division's budget, and prepares budget projections to request funding for next five years.

The appellant carries out these responsibilities with the assistance of his subordinate staff that includes three GS-2210-11 Information Technology (IT) Specialists, one GS-2210-9 IT Specialist, and one Computer Assistant, GS-335-6. This staff is supplemented with two contract personnel. The PD and record material provide more detailed information on the duties and responsibilities of the position.

Series, title, and standard determination

The agency classified the appellant's position in the Information Technology Specialist Series, GS-2210, and titled it Supervisory Information Technology Specialist (INFOSEC), using the parenthetical specialty title to further identify the duties and responsibilities performed and the

specialized knowledge and skills needed. The appellant does not question the series of his position. We concur with the agency's determination. The position meets the criteria for coverage under the General Schedule Supervisory Guide (GSSG) and is appropriately evaluated by its use. We find the position is properly titled as Supervisory Information Technology Specialist (INFOSEC).

Grade determination

The GSSG uses a factor-point evaluation approach that uses six factors common to all supervisory positions. Each factor level in the standard describes the minimum characteristics needed to receive credit for the described level. Therefore, if a position fails to meet the criteria in a factor level in any significant aspect, it must be credited at a lower level. Conversely, the position may exceed those criteria in some aspects and still not be credited at a higher level. Each factor level has a corresponding point value. The total points are converted to a grade by use of the grade conversion chart in the standard.

The appellant disagrees with the agency's evaluation of Factors 1, 3, 4B, 5, and 6. Our evaluation will discuss all factors.

Factor 1, Program scope and effect

This factor assesses the general complexity, breadth, and impact of the program areas and work directed, including its organizational and geographic coverage. It also assesses the effect of the work both within and outside of the immediate organization. All work, for which the supervisor is both technically and administratively responsible, including work accomplished through subordinates, military personnel, and contractors is considered. To receive credit for a given level, the separate criteria specified for both scope and effect must be met at that factor level.

Subfactor 1a: Scope

Scope addresses complexity and breadth of the program or work directed, including the geographic and organizational coverage within the agency structure. It has two elements: (a) the program (or program segment) directed and (b) the work directed, the products produced, or the services delivered.

At Level 1-3 of this subfactor, the supervisor directs a program segment that performs technical, administrative, protective, investigative, or professional work. The program segment and work directed typically have coverage which encompasses a major metropolitan area, a State, or a small region of several States; or when most of an area's taxpayers or businesses are covered, coverage comparable to a small city. Providing complex administrative or technical or professional services directly affecting a large or complex multimission military installation also falls at this level.

At Level 1-4, the supervisor directs a segment of a professional, highly technical, or complex administrative program which involves the development of major aspects of key agency scientific, medical, legal, administrative, regulatory, policy development or comparable, highly technical programs; or that includes major, highly technical operations at the Government's largest, most complex industrial installations.

As at Level 1-3, the appellant directs an administrative staff involved with ensuring the security and integrity of the computer network serving [installation] and its two sub-installations. [installation] meets the criteria for a multimission installation as it includes a major medical center, two Army Command headquarters, a garrison, and service schools. The serviced population is between 5,000 and 6,000 users. The appellant's program direction meets the scope described in Level 1-3. It does not meet Level 1-4 as it does not involve the development of major aspects of key agency programs or include operations at the largest, most complex industrial installations.

Subfactor 1b: Effect

b. Effect - This element of Factor 1 addresses the impact of the work, the products, and/or the programs described under "Scope" on the mission, the agency, other agencies, the general public, or others.

At Level 1-2 of this subfactor, the services or products support and significantly affect installation, area office, or field office operations and objectives or comparable program segments; or provide services to a moderate, local or limited population of clients or users comparable to a major portion of a small city or rural county.

At Level 1-3, activities, functions, or services accomplished directly and significantly impact a wide range of agency activities, the work of other agencies, or the operations of outside interests (e.g., a segment of a regulated industry), or the general public. At the field activity level (involving large, complex, multimission organizations and/or very large serviced populations), the work directly involves or substantially impacts the provision of essential support operations to numerous, varied, and complex technical, professional, and administrative functions. One illustration given at this level describes directing administrative services (personnel, supply management, budget, facilities management or similar) which support and directly affect operations of a bureau or major military command headquarters; a large or complex multimission military installation; or an organization of comparable magnitude.

The appellant’s position does not meet Level 1-3 of this subfactor. The work directed by the appellant involves assuring only the security aspects of the information technology systems in place at the installation. This does not fully meet the broader degree of administrative service, e.g., the full range of personnel, budget, IT services, nor affect the wide range of activities described as typical at the 1-3 level. To assign a factor level, the criteria involving both scope and effect must be met. Although Scope meets the 1-3 level, Effect is credited at 1-2, therefore, the factor must be credited at Level 1-2.

Level 1-2 is assigned for 350 points.

Factor 2, Organizational setting

This factor considers the organizational situation of the supervisory position in relation to higher level management.

The appellant does not question the evaluation of Factor 2. At Level 2-1, the position is accountable to a position that is two or more reporting levels below the first SES, flag or general officer, or equivalent higher level position in the direct supervisory chain.

The appellant reports to the Deputy Director of the ITBC, a GS-2210-13, who functions as the alter ego to the Director. The ITBC Director reports to the Army Garrison Commander, an Army Colonel. We concur with the agency's evaluation.

We assign Level 2-1 for 100 points.

Factor 3, Supervisory and managerial authority exercised

This factor covers the delegated supervisory and managerial authorities which are exercised on a recurring basis. To be credited with a level under this factor, a position must meet the authorities and responsibilities to the extent described for the specific level.

In order to meet Level 3-2, a position must meet any one of the conditions described in paragraphs a, b, or c under this factor level. This position meets Level 3-2c. Supervisors at that level must carry out at least three of the first four, and a total of six or more of the 10 responsibilities listed at that level in the GSSG. The appellant carries out all 10 authorities and responsibilities.

In order to fully meet Factor Level 3-3, a position must meet the conditions described in paragraphs a or b, under this factor level.

Under Level 3-3a, the incumbent of a position must exercise the delegated managerial authority to set long range plans with goals and objectives; assure implementation of the plans by subordinate organizational units; determine which objectives require additional emphasis; and determine solutions to and resolve issues created by budget and staff requirements, including contracting out. In contrast, the appellant serves as a first-level supervisor whose organization does not involve the degree of delegated managerial authority or involve subordinate organizational units or subordinate supervisors as is envisioned of an organizational setting at Level 3-3a. The position is not credited with Level 3-3a.

At Level 3-3b, a supervisor must exercise all or nearly all of the supervisory responsibilities and authorities described at Level 3-2c, plus at least 8 of the 15 responsibilities listed under Level 3-b of the GSSG. As noted, the appellant's position exercises all 10 of the responsibilities described at Level 3-2c. Of the 15 responsibilities listed under Level 3-3b, the appellant's duties and responsibilities are compared below:

Responsibilities 1, 3, 5, 6, and 8 refer to situations where work is accomplished through subordinate supervisors, team leaders, or other similar personnel. Supervisors at this level exercise these responsibilities through *multiple* subordinate supervisors or team leaders. Further, the supervisor's organizational workload must be so large and its work so complex that it requires using two or more subordinate supervisors, team leaders, or comparable personnel to direct the work. The appellant is a first-level supervisor. There are two contract employees responsible for DITSCAP Security Administration, with one designated as a team leader. Information in the record does not show duties that would warrant designation as a team leader

under applicable classification standards. Furthermore, the appellant's organizational workload of seven staff years is not so large and its work is not so complex that it requires using two or more subordinate supervisors, team leaders, or comparable personnel to direct the work. The appellant's position is not credited for these responsibilities.

Responsibility 2 is credited because the appellant exercises significant responsibilities in dealing with officials of other units and in advising management officials of higher rank, i.e., managers at Directorate and Garrison levels. Responsibility 7 is credited in that his selections for subordinate nonsupervisory positions must receive concurrence by the ITBC Director or Deputy. Responsibility 12 is credited because the appellant determines the adequacy of the contractor work performed so payment to the contractor can be authorized.

Responsibilities 10, 13, and 14 may not be credited as the authority to make those decisions has not been delegated to the appellant's position. For (10), the appellant acts as the proposing official for serious disciplinary actions, but a higher level supervisor acts as the deciding official. Regarding contract personnel, the appellant brings issues to the attention of the SPI site manager or recommends actions and the SPI site manager makes final decisions on any disciplinary actions (including removal) against contract personnel. For (13) approval of expenses comparable to within-grade increases, extensive overtime, and employee travel must receive ITBC Deputy Director approval. For contract employees, the appellant must concur on changes in pay rates, but all changes must receive SPI site manager approval. For (14), the appellant stated during the interview that he did not recommend awards or changes in position classification.

Responsibility 4 is not credited because the appellant does not direct a program with multimillion-dollar resources. The size of the organization directed also precludes exercising responsibilities 9, 11, and 15 on a regular basis at the level intended by the Guide. i.e., hearing and resolving group grievances or serious employee complaints; making decisions on nonroutine, costly, or controversial training needs, e.g., management development, sabbaticals, etc.; and finding and implementing methods to reduce or eliminate barriers to production, promote team building, or improve business practices.

Summarizing the information above, the appellant performs only 3 of the 15 responsibilities listed under Level 3-3b. Because the appellant's position does not meet Level 3-3a, nor are 8 of the 15 responsibilities listed in Level 3-3b, Level 3-2 is assigned.

Level 3-2 is assigned and 450 points are credited.

Factor 4, Personal contacts

This is a two part factor that assesses the nature and purpose of personal contacts related to supervisory and managerial responsibilities. The contacts used to determine credit level under one subfactor must be the same used to determine credit under the other subfactor.

Subfactor 4A: Nature of contacts

This subfactor covers the organizational relationships, authority or influence level, setting, and preparation difficulty involved in the supervisor's work. To be credited, contacts must be direct and

recurring, contribute to the successful performance of the work, and have a demonstrable impact on the difficulty and responsibility of the position.

The appellant's contacts are properly evaluated at Level 4A-2. As discussed at that level of the Guide, contacts are with members of the business community, the general public, higher ranking managers, supervisors, and staff of program, administrative, or other work units and activities throughout the installation. These contacts sometimes require special preparation. The appellant's contacts are with others in the ITBC, with customers within the installation's computer network, and with security specialists of other Army activities. Other contacts include the ACERT, RCERT, and the Theater Network Operations Security Center. We concur with the agency's evaluation and the appellant does not disagree.

We assign Level 4A-2 and 50 points.

Subfactor 4B: Purpose of contacts

This subfactor includes the advisory, representational, negotiating, and commitment responsibilities related to the supervisor's contacts credited under the previous subfactor.

At Level 4B-2, the purpose of contacts is to ensure that information provided to outside parties is accurate and consistent, to plan and coordinate the work directed with that of others outside the subordinate organization, and/or to resolve differences of opinion among managers, supervisors, employees, contractors, or others.

At Level 4B-3, the purpose of contacts is to justify, defend, or negotiate in representing the project, program segment(s), or organizational unit(s) directed, in obtaining or committing resources, *and* in gaining compliance with established policies, regulations, or contracts. Contacts at this level usually involve active participation in conferences, meetings, hearings, or presentations involving problems or issues of considerable consequence or importance to the program or program segment(s) managed.

As at Level 4B-2, the purpose of the appellant's contacts is to plan and coordinate his division's work with that of other ITBC divisions and to advise others on the security and integrity requirements of the installation's computer network. During changes in network connectivity, the appellant negotiates with local Army and/or tenant organizations on the type of network hookups needed and the cost allocation of the hookups. According to the supervisor, the appellant also negotiates adjustments to suspense dates with headquarters when implementation or other issued suspenses are unreasonable due to the large number of installation workstations impacted by the suspense item.

Unlike Level 4B-3, the appellant's contacts do not *typically* require him to justify, defend, or negotiate his division's work, to obtain or commit resources, *and* to gain compliance. When an organization was unwilling to comply with security requirements to maintain their connectivity to the network, the appellant stated that these situations were quickly elevated to higher management levels.

We assign Level 4B-2 and 75 points.

Factor 5, Difficulty of typical work directed

This factor covers the difficulty and complexity of the basic work most typical of the organization directed, as well as other line, staff, or contracted work for which the supervisor has technical or oversight responsibility (either directly or through subordinate supervisors, team leaders, or others). The level credited for this factor normally must constitute at least 25 percent of the workload of the organization supervised. Excluded from consideration is: (1) work of lower level positions that primarily support the basic work of the unit, (2) work that is graded based upon the supervisory or leader guides, (3) work that is graded higher than normal because of extraordinary independence from supervision, and (4) work for which the supervisor does not have the responsibilities defined under Factor 3.

The appellant provides administrative and technical supervision of the work of three IT Specialists, GS-2210-11; one IT Specialist, GS-2210-9; and one Computer Assistant, GS-335-6. He also has oversight responsibility for two contract personnel whose work has been found equivalent to IT Specialist at the GS-11 grade level. We find that GS-11 is the highest level of work directed under the criteria defined in Factor 5.

Level 5-6 is credited for 800 points.

Factor 6, Other conditions

This factor measures the extent to which various conditions contribute to the difficulty and complexity of carrying out supervisory duties, authorities, and responsibilities. Conditions affecting work for which the supervisor is responsible may be considered if they increase the difficulty of carrying out assigned supervisory or managerial duties and authorities. These Special Situations are considered if the factor level initially credited is less than 6-4.

Level 6-4 of the guide addresses complications arising from the supervision of work comparable in difficulty to the GS-11 level *and* requiring substantial coordination and integration of a number of major assignments or projects.

Level 6-5 addresses complications arising from the supervision of work comparable in difficulty to the GS-12 level *and* requiring significant and extensive coordination and integration. At Level 6-5, the supervisor's coordination and integration occur at the overall organizational level rather than the installation level and involve policy formulation for a program rather than development of local (or installation) policy to implement or clarify program policy. None of the provisions of Level 6-5 apply to the appellant’s position.

Comparable to level 6-4, the appellant supervises administrative work at the GS-11 level. He is expected to coordinate and integrate the computer security program at the installation in several areas, including software, hardware, firmware, personnel databases, information systems, telecommunications, physical environment and networks. As at Level 6-4, he is expected to make recommendations and participate in determinations regarding security projects to be initiated, dropped or curtailed. The position does not involve supervision of GS-12 level work nor the significant recommendation and coordination of the level typical of Level 6-5.

We assign Level 6-4 and 1120 points.

Summary

Factor	*Level*	*Points*
1. Program scope and effect	1-2	350
2. Organizational setting	2-1	100
3. Supervisory & managerial authority exercised	3-2	450
4. Personal contacts		
A. Nature	4A2	50
B. Purpose	4B2	75
5. Difficulty of typical work directed	5-6	800
6. Other conditions	6-4	1,120
	Total	2,945

A total of 2945 points is credited. Using the grade conversion table in the GSSG standard, 2,945 points fall in the GS-12 range (2,755-3,150).

Decision

The position is properly classified as Supervisory Information Technology Specialist (INFOSEC), GS-2210-12.